DOC.
000233

CPL/AC

PREGÃO
050/2003

LOCAÇÃO DE EQUIPAMENTOS DE INFORMÁTICA INCLUINDO ASSISTÊNCIA TÉCNICA E TREINAMENTO

NEC DO BRASIL S/A – MANUAL VOLUME V

2003
PASTA 27

001

Nº 3702

Declarações

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 002
3702
Doc.

IBM BRASIL - INDÚSTRIA, MÁQUINAS E SERVIÇOS LTDA.
SCN Q. 4 Bl. B - 7º andar Centro Empresarial Varig
Brasília- DF Cep: 70.710-500
Telefone: (61) 329-2800 Fax: (61) 329 2850
C.N.P.J.: 33.372.251/0100-38 Insc. Es.: 07.333.522/002-44

DECLARAÇÃO

Brasília, 23 de Julho de 2.003

Á
EMPRESA BRASILEIRA DE CORREIOS E TELÉGRAFOS - ECT
Administração Central
SBN – Quadra 01, Bloco "A" – Sobreloja – Ed. Sede ECT
Brasília – D.F.

Ref.: EDITAL DO PREGÃO N.º 050/2003 – CPL/AC

Objeto: LOCAÇÃO DE EQUIPAMENTOS DE INFORMÁTICA, INCLUINDO A ASSISTÊNCIA TECNICA E TREINAMENTO DE PESSOAL

Prezados Senhores,

Declaramos para fins de comprovação junto ao edital em epigrafe que a Itautec Informática S.A. - Grupo Itautec Philco, inscrita no CNPJ sob o n.º 51.764.058/0001-42, sediada na Rua Santa Catarina, 1 - São Paulo - SP, está autorizada a comercializar, instalar, prestar serviços de manutenção e etc. nos produtos abaixo descritos:

TIPO DE PRODUTO	MARCA	MODELO
SERVIDOR INTEL TIPO 01	IBM	xSeries 440
SERVIDOR INTEL TIPO 02	IBM	xSeries 360
SERVIDOR INTEL TIPO 03	IBM	xSeries 235
SERVIDOR RISC TIPO 01	IBM	pSeries 690
SWITCH TIPO 01	Cisco	Catalyst 6513
SWITCH TIPO 02	Cisco	Catalyst 2950
SWITCH TIPO 03	IBM	2109-M12
SWITCH TIPO 04	Black Box	Afinity

Fls Nº 003
Nº 3702

16.633

SWITCH TIPO 05	Cisco	CVPN 3060
ROTEADOR TIPO 01	Cisco	Cisco 3745
ROTEADOR TIPO 02	Cisco	Cisco 1751-V
UNIDADE DE BACKUP ROBOTIZADO	IBM	LTO Ultrium 3584
SERV. DE SEGURANÇA LÓGICA TIPO1	Cisco	PIX - 535
SERV. DE SEGURANÇA LÓGICA TIPO2	Cisco	PIX - 525
SERV. P/ DETECÇÃO DE INTRUSÃO	Cisco	IDS - 4250
SERVIDOR RISC ADICIONAL	IBM	pSeries 630
Notebooks	IBM	ThinkPad G40

Brasília, 23 de Julho de 2003

Carmem Távora

Carmem Lúcia Távora Vieira
Gerente de Unidade de Negócios
IBM Brasil - Indústria, Máquinas e Serviços Ltda.

CPMI - CORREIOS
Fls. nº 004
Nº 3702

IBM BRASIL - INDÚSTRIA, MÁQUINAS E SERVIÇOS LTDA.
SCN Q. 4 Bl. B - 7° andar Centro Empresarial Varig
Brasília- DF Cep: 70.710-500
Telefone: (61) 329-2800 Fax: (61) 329 2850
C.N.P.J.: 33.372.251/0100-38 Insc. Es.: 07.333.522/002-44

16.62+
1-

DECLARAÇÃO

Brasília, 23 de Julho de 2.003

Á
EMPRESA BRASILEIRA DE CORREIOS E TELÉGRAFOS - ECT
Administração Central
SBN – Quadra 01, Bloco "A" – Sobreloja – Ed. Sede ECT
Brasília – D.F.

Ref.: EDITAL DO PREGÃO N.° 050/2003 – CPL/AC

Objeto: LOCAÇÃO DE EQUIPAMENTOS DE INFORMÁTICA, INCLUINDO A ASSISTÊNCIA TECNICA E TREINAMENTO DE PESSOAL

Prezados Senhores,

Declaramos para fins de comprovação junto ao edital em epigrafe que a ITEC S.A. - Grupo Itautec Philco, inscrita no CNPJ sob o n.° 96.452.347/0001-44, sediada na Av. Paulista, 1938 - 20° andar- São Paulo - SP, está autorizada a comercializar, instalar, prestar serviços de manutenção e etc. nos produtos abaixo descritos:

TIPO DE PRODUTO	MARCA	MODELO
SERVIDOR INTEL TIPO 01	IBM	xSeries 440
SERVIDOR INTEL TIPO 02	IBM	xSeries 360
SERVIDOR INTEL TIPO 03	IBM	xSeries 235

Brasília, 23 de Julho de 2003

Carmem Távora

Carmem Lúcia Távora Vieira
Gerente de Unidade de Negócios
IBM Brasil - Indústria, Máquinas e Serviços Ltda.

CPMI - CORREIOS
Fls. Nº 005
Nº 3702
Doc.

IBM BRASIL - INDÚSTRIA, MÁQUINAS E SERVIÇOS LTDA.
SCN Q. 4 Bl. B - 7° andar Centro Empresarial Varig
Brasília- DF Cep: 70.710-500
Telefone: (61) 329-2800 Fax: (61) 329 2850
C.N.P.J.: 33.372.251/0100-38 Insc. Es.: 07.333.522/002-44

16.036
L

DECLARAÇÃO

Brasília, 23 de Julho de 2.003

Á
EMPRESA BRASILEIRA DE CORREIOS E TELÉGRAFOS - ECT
Administração Central
SBN – Quadra 01, Bloco "A" – Sobreloja – Ed. Sede ECT
Brasília – D.F.

Ref.: EDITAL DO PREGÃO N.° 050/2003 – CPL/AC

Objeto: LOCAÇÃO DE EQUIPAMENTOS DE INFORMÁTICA, INCLUINDO A ASSISTÊNCIA TECNICA E TREINAMENTO DE PESSOAL

Prezados Senhores,

Declaramos para fins de comprovação junto ao Edital em epigrafe que os equipamentos cotados abaixo pela CPM S/A, inscrita no CNPJ sob o n° 65.599.953/0001-63, sediada na Rua General Fernando de Vasconcellos Cavalcanti de Albuquerque, 775 Granja Viana – Cotia – SP, são de linha de produção continuada e que nos comprometemos a fornecer peças de reposição pelo período mínimo de 60 (sessenta) meses.

Os equipamentos cotados são:

TIPO DE PRODUTO	MARCA	MODELO
SERVIDOR INTEL TIPO 01	IBM	xSeries 440
SERVIDOR INTEL TIPO 02	IBM	xSeries 360
SERVIDOR INTEL TIPO 03	IBM	xSeries 235
SERVIDOR RISC TIPO 01	IBM	pSeries 690
SWITCH TIPO 03	IBM	2109-M12
UNIDADE DE BACKUP ROBOTIZADO	IBM	LTO Ultrium 3584

006
Nº 3702

SERVIDOR RISC ADICIONAL	IBM	pSeries 630
Notebooks	IBM	ThinkPad G40

Brasília, 23 de Julho de 2003

Carmem Lúcia Távora Vieira
Gerente de Unidade de Negócios
IBM Brasil - Indústria, Máquinas e Serviços Ltda.

ROS nº 03/2006 - CN - CPMI - CORREIOS
Fls. Nº 007
Doc: 3702

16.681

DECLARAÇÃO

A empresa IBM Brasil Indústria, Máquinas e Serviços Ltda., CNPJ n.º 33.372.251/0001-56, na condição de fabricante, declara que " há compatibilidade e integração com as versões dos equipamentos existentes: Switches: Modelo 2109 - S16 fabricante IBM (OEM Brocade 2800 Silkworm), versão de microcódigo A2.4.1C; Storage Modelo 2105 - F20 (IBM) com dois microcódigos (2 dispositivos de armazenamento) 1.5.2.103 e 1.3.2.49; HBA`s Modelo Qlogic QLA 2200 - PCI Fibre Channel adpater, versão de microcódigo 8.0.8.1" , conforme item 3.3 SWITCH TIPO 3 (FC) subitem 5 - Compatibilidade e Integração do Anexo 01-b do Edital do Pregão n.º 050/2003-CPL/AC.

Brasília - DF, 23 de Julho de 2003.

Carmem Távora Vieira
RG. 1451032-88 SSP-CE
Gerente de Unidade de Negócios
IBM Brasil Indústria, Máquinas e Serviços Ltda.

008

Nº 3702

IBM BRASIL - INDÚSTRIA, MÁQUINAS E SERVIÇOS LTDA.
SCN Q. 4 Bl. B - 7º andar Centro Empresarial Varig
Brasília- DF Cep: 70.710-500
Telefone: (61) 329-2800 Fax: (61) 329 2850
C.N.P.J.: 33.372.251/0100-38 Insc. Es.: 07.333.522/002-44

16.683
2

DECLARAÇÃO

Brasília, 23 de Julho de 2.003

Á
EMPRESA BRASILEIRA DE CORREIOS E TELÉGRAFOS - ECT
Administração Central
SBN – Quadra 01, Bloco "A" – Sobreloja – Ed. Sede ECT
Brasília – D.F.

Ref.: EDITAL DO PREGÃO N.º 050/2003 – CPL/AC

Objeto: LOCAÇÃO DE EQUIPAMENTOS DE INFORMÁTICA, INCLUINDO A ASSISTÊNCIA TECNICA E TREINAMENTO DE PESSOAL

Prezados Senhores,

Declaramos para fins de comprovação junto ao Edital em epigrafe que os equipamentos cotados abaixo pela Itautec Informática S.A. - Grupo Itautec Philco, inscrita no CNPJ sob o nº 51.764.058/0001-42, sediada na Rua Santa Catarina, 1 - São Paulo - SP, são de linha de produção continuada e que nos comprometemos a fornecer peças de reposição pelo período mínimo de 60 (sessenta) meses.

Os equipamentos cotados são:

TIPO DE PRODUTO	MARCA	MODELO
SERVIDOR INTEL TIPO 01	IBM	xSeries 440
SERVIDOR INTEL TIPO 02	IBM	xSeries 360
SERVIDOR INTEL TIPO 03	IBM	xSeries 235
SERVIDOR RISC TIPO 01	IBM	pSeries 690
SWITCH TIPO 01	Cisco	Catalyst 6513
SWITCH TIPO 02	Cisco	Catalyst 2950
SWITCH TIPO 03	IBM	2109-M12

009
Nº 3702

16.682

SWITCH TIPO 04	Black Box	Afinity
SWITCH TIPO 05	Cisco	CVPN 3060
ROTEADOR TIPO 01	Cisco	Cisco 3745
ROTEADOR TIPO 02	Cisco	Cisco 1751-V
UNIDADE DE BACKUP ROBOTIZADO	IBM	LTO Ultrium 3584
SERV. DE SEGURANÇA LÓGICA TIPO1	Cisco	PIX - 535
SERV. DE SEGURANÇA LÓGICA TIPO2	Cisco	PIX - 525
SERV. P/ DETECÇÃO DE INTRUSÃO	Cisco	IDS - 4250
SERVIDOR RISC ADICIONAL	IBM	pSeries 630
Notebooks	IBM	ThinkPad G40

Brasília, 23 de Julho de 2003

Carmem Távora

Carmem Lúcia Távora Vieira
Gerente de Unidade de Negócios
IBM Brasil - Indústria, Máquinas e Serviços Ltda.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls: 010
Nº 3702
Doc:

IBM BRASIL - INDÚSTRIA, MÁQUINAS E SERVIÇOS LTDA.
SCN Q. 4 Bl. B - 7º andar Centro Empresarial Varig
Brasília- DF Cep: 70.710-500
Telefone: (61) 329-2800 Fax: (61) 329 2850
C.N.P.J.: 33.372.251/0100-38 Insc. Es.: 07.333.522/002-44

DECLARAÇÃO

Brasília, 23 de Julho de 2.003

Á
EMPRESA BRASILEIRA DE CORREIOS E TELÉGRAFOS - ECT
Administração Central
SBN – Quadra 01, Bloco "A" – Sobreloja – Ed. Sede ECT
Brasília – D.F.

Ref.: EDITAL DO PREGÃO N.° 050/2003 – CPL/AC

Objeto: LOCAÇÃO DE EQUIPAMENTOS DE INFORMÁTICA, INCLUINDO A ASSISTÊNCIA TECNICA E TREINAMENTO DE PESSOAL

Prezados Senhores,

Declaramos para fins de comprovação junto ao Edital em epigrafe que os equipamentos cotados abaixo pela ITEC S.A. - Grupo Itautec Philco, inscrita no CNPJ sob o nº 96.452.347/0001-44, sediada na Av. Paulista, 1938 - 20º andar- São Paulo - SP, são de linha de produção continuada e que nos comprometemos a fornecer peças de reposição pelo período mínimo de 60 (sessenta) meses.

Os equipamentos cotados são:

TIPO DE PRODUTO	MARCA	MODELO
SERVIDOR INTEL TIPO 01	IBM	xSeries 440
SERVIDOR INTEL TIPO 02	IBM	xSeries 360
SERVIDOR INTEL TIPO 03	IBM	xSeries 235

Brasília, 23 de Julho de 2003

Carmem Távora

Carmem Lúcia Távora Vieira
Gerente de Unidade de Negócios
IBM Brasil - Indústria, Máquinas e Serviços Ltda.

011

Nº 3702

IBM BRASIL - INDÚSTRIA, MÁQUINAS E SERVIÇOS LTDA.
SCN Q. 4 Bl. B - 7º andar Centro Empresarial Varig
Brasília- DF Cep: 70.710-500
Telefone: (61) 329-2800 Fax: (61) 329 2850
C.N.P.J.: 33.372.251/0100-38 Insc. Es.: 07.333.522/002-44

DECLARAÇÃO

Brasília, 23 de Julho de 2.003

Á
EMPRESA BRASILEIRA DE CORREIOS E TELÉGRAFOS - ECT
Administração Central
SBN – Quadra 01, Bloco "A" – Sobreloja – Ed. Sede ECT
Brasília – D.F.

Ref.: EDITAL DO PREGÃO N.º 050/2003 – CPL/AC

Objeto: LOCAÇÃO DE EQUIPAMENTOS DE INFORMÁTICA, INCLUINDO A ASSISTÊNCIA TECNICA E TREINAMENTO DE PESSOAL

Prezados Senhores,

Declaramos para fins de comprovação junto ao edital em epigrafe que a CPM S/A, inscrita no CNPJ sob o n.º 65.599.953/0001-63, sediada na Rua General Fernando de Vasconcellos Cavalcanti de Albuquerque, 775 Granja Viana – Cotia – SP, está autorizada a comercializar, instalar, prestar serviços de manutenção e etc. nos produtos abaixo descritos:

TIPO DE PRODUTO	MARCA	MODELO
SERVIDOR INTEL TIPO 01	IBM	xSeries 440
SERVIDOR INTEL TIPO 02	IBM	xSeries 360
SERVIDOR INTEL TIPO 03	IBM	xSeries 235
SERVIDOR RISC TIPO 01	IBM	pSeries 690
SWITCH TIPO 03	IBM	2109-M12
UNIDADE DE BACKUP ROBOTIZADO	IBM	LTO Ultrium 3584
SERVIDOR RISC ADICIONAL	IBM	pSeries 630

EDS nº 03/2005 - CN
CPMI CORREIOS
Fls Nº 012
Doc. 3702

1679

Notebooks	IBM	ThinkPad G40

Brasília, 23 de Julho de 2003

Carmem Lúcia Távora Vieira
Gerente de Unidade de Negócios
IBM Brasil - Indústria, Máquinas e Serviços Ltda.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 013
Nº 3702
Doc.

IBM

1675

DECLARAÇÃO

A empresa IBM Brasil Indústria, Máquinas e Serviços Ltda., CNPJ n.º 33.372.251/0001-56, na condição de fabricante, declara que "serão fornecidos 2 (dois) equipamentos servidores RISC para o CCD de Brasília, em alta disponibilidade, para abrigar os softwares gerenciadores das fitotecas e os softwares gerenciadores do backup e também serão fornecidos 2 (dois) servidores RISC para o CCD de São Paulo, em alta disponibilidade, para abrigar o software gerenciador da fitoteca e o software gerenciador do backup. A configuração dos servidores, **abaixo descrita**, possibilita que estejam dimensionados de tal forma que suportem o gerenciamento de 150 clientes de backup, individualmente", conforme item 5 - Unidade de Backup subitem 15 - Geral do Anexo 01-b do Edital do Pregão n.º 050/2003-CPL/AC.

CCD de São Paulo

ITSM – BACKUP

Dois servidores Risc em alta disponibilidade e Rack

Product	Description	Quantity
7028-6C4	ITSM SPM:pSeries 630 Model 6C4 Rack-mount Server	2
2633	CD-ROM Drive - 48X (Max) IDE	2
2848	POWER GXT135P Graphics Accelerator	2
3158	36.4 GB 10,000 RPM Ultra3 SCSI Disk Drive Assembly	4
3254	RIO Cable Support Brackets	2
4250	Connector Cable, 6-slot PCI Riser to Media Bays.	2
4254	SCSI Connector Cable	2
4452	2048MB (4x512MB) SDRAM DIMM Memory	2
4651	Rack Indicator, Rack #1	2
5127	2-way 1.45 GHz POWER4+ Processor Card	2
5701	IBM 10/10/1000 Base-TX Ethernet PCI-X Adapter	2
6158	20/40GB 4mm Internal Tape Drive	2
6230	Advanced SerialRAID Plus Adapter	2
6239	2 Gigabit Fibre Channel PCI-X Adapter	4
6273	Power Supply ,645 Watt AC, Hot-Swap, Base and Redundant	4
6557	Redundant Cooling	2
6568	Ultra3 SCSI 4-Pack Hot Swap Back Plane	2
9172	Power Specify, AC	2
9300	Lang.Group Spec.-US English	2
9556	6 Slot PCI Riser (Initial order only)	2
9581	RIO-2 Enablement Indicator	2

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 0014
Página 1 de 3
Nº Doc. 3702

9911	Power C.-All(Std.Rack P.C.)	2

16677

Product	Description	Quantity
7311-D20	I/O Drawer 1:Model D20 I/O Drawer	2
3147	Remote I/O Cable, 3.5M	4
4651	Rack Indicator, Rack #1	2
5701	IBM 10/10/1000 Base-TX Ethernet PCI-X Adapter	2
6006	SPCN 3m Cable: Drawer to Drawer	4
6239	2 Gigabit Fibre Channel PCI-X Adapter	2
6268	Power Supply, 435 Watt AC, Hot-swap, Base and Redundant	4
6417	RIO-2 Ports to I/O Planar Riser Card	2
9172	Power Specify, AC	2
9300	Lang Grp Spec.-US English	2
9911	Pwr Cord Spec.- All	2

Product	Description	Quantity
7014-T00	Rack 1:IBM RS/6000 Rack Model T00	1
6068	Front door (Black) for 1.8M(High Perforation) racks	1
6098	Side panel (black) for 1.8M or 2M racks	2
7176	Power Distribution Unit - Side Mount, Single Phase, L6-30 Connector	1
9176	Pwr Dist Unit Spec.1 Ph.L6-30	1
9300	Language Group US English	1
9800	Power Cord US/Canada	1

CCD de Brasília:

ITSM – BACKUP

Dois servidores Risc em alta disponibilidade e Rack

Product	Description	Quantity
7028-6C4	ITSM SPM:pSeries 630 Model 6C4 Rack-mount Server	2
2633	CD-ROM Drive - 48X (Max) IDE	2
2848	POWER GXT135P Graphics Accelerator	2
3158	36.4 GB 10,000 RPM Ultra3 SCSI Disk Drive Assembly	4
3254	RIO Cable Support Brackets	2
4250	Connector Cable, 6-slot PCI Riser to Media Bays.	2
4254	SCSI Connector Cable	2
4452	2048MB (4x512MB) SDRAM DIMM Memory	4
4651	Rack Indicator, Rack #1	2
5127	2-way 1.45 GHz POWER4+ Processor Card	4
5701	IBM 10/10/1000 Base-TX Ethernet PCI-X Adapter	2
6158	20/40GB 4mm Internal Tape Drive	2
6230	Advanced SerialRAID Plus Adapter	2
6239	2 Gigabit Fibre Channel PCI-X Adapter	6
6273	Power Supply ,645 Watt AC, Hot-Swap, Base and Redundant	4
6557	Redundant Cooling	2
6568	Ultra3 SCSI 4-Pack Hot Swap Back Plane	2

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 015
Doc. 3702

9172	Power Specify, AC	2
9300	Lang.Group Spec.-US English	2
9556	6 Slot PCI Riser (Initial order only)	2
9581	RIO-2 Enablement Indicator	2
9911	Power C.-All(Std.Rack P.C.)	2

Product	Description	Quantity
7311-D20	I/O Drawer 1:Model D20 I/O Drawer	2
3147	Remote I/O Cable, 3.5M	4
4651	Rack Indicator, Rack #1	2
5701	IBM 10/10/1000 Base-TX Ethernet PCI-X Adapter	2
6006	SPCN 3m Cable: Drawer to Drawer	4
6239	2 Gigabit Fibre Channel PCI-X Adapter	4
6268	Power Supply, 435 Watt AC, Hot-swap, Base and Redundant	4
6417	RIO-2 Ports to I/O Planar Riser Card	2
9172	Power Specify, AC	2
9300	Lang Grp Spec.-US English	2
9911	Pwr Cord Spec.- All	2

Product	Description	Quantity
7014-T00	7014-T00 : Rack 1:IBM RS/6000 Rack Model T00	1
6068	Front door (Black) for 1.8M(High Perforation) racks	1
6098	Side panel (black) for 1.8M or 2M racks	2
7176	Power Distribution Unit - Side Mount, Single Phase, L6-30 Connector	1
9176	Pwr Dist Unit Spec.1 Ph.L6-30	1
9300	Language Group US English	1
9800	Power Cord US/Canada	1

Brasília - DF, 24 de Julho de 2003.

Carmem Távora Vieira
RG. 1451032-88 SSP-CE
Gerente de Unidade de Negócios
IBM Brasil Indústria, Máquinas e Serviços Ltda.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 016
Doc 3702

IBM

16 675

DECLARAÇÃO

A empresa IBM Brasil Indústria, Máquinas e Serviços Ltda., CNPJ n.º 33.372.251/0001-56, na condição de fabricante, declara que "as licenças de software que desempenha as funções de um **GERENCIADOR DE FITOTECA E DE BACKUP** serão fornecidas considerando-se o número de unidades de backup solicitadas e o número total de servidores fornecidos", conforme item 5 - Unidade de Backup subitem 13 – Recursos de Software do Anexo 01-B do Edital do Pregão n.º 050/2003-CPL/AC.

Brasília - DF, 24 de Julho de 2003.

Carmem Távora

Carmem Távora Vieira
RG. 1451032-88 SSP-CE
Gerente de Unidade de Negócios
IBM Brasil Indústria, Máquinas e Serviços Ltda.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 017
Doc. 3702

IBM BRASIL - INDÚSTRIA, MÁQUINAS E SERVIÇOS LTDA.
SCN Q. 4 Bl. B - 7º andar Centro Empresarial Varig
Brasília- DF Cep: 70.710-500
Telefone: (61) 329-2800 Fax: (61) 329 2850
C.N.P.J.: 33.372.251/0100-38 Insc. Es.: 07.333.522/002-44

16.674
L

DECLARAÇÃO

Á
EMPRESA BRASILEIRA DE CORREIOS E TELÉGRAFOS
Administração Central
SBN - Quadra 01, Bloco 'A' - Sobreloja - Ed. Sede ECT
Brasília - DF

Ref.: EDITAL DO PREGÃO nº 050/2003 - CPL/AC

Objeto: LOCAÇÃO DE EQUIPAMENTOS DE INFORMÁTICA, INCLUINDO A ASSISTÊNCIA TÉCNICA E TREINAMENTO DE PESSOAL

A IBM Brasil - Indústria, Máquinas e Serviços Ltda., inscrita no CNPJ Nº 33.372.251/0001-56, com sede na Av. Pasteur, 138/146 - Rio de Janeiro, na qualidade de fabricante dos equipamentos descritos abaixo, declara para os devidos fins que os mesmos atendem na íntegra as disposições do Edital do Pregão ECT nº 050/2003 – CPL/AC.

Os itens descritos a seguir serão observados para todos os produtos que compõem a proposta técnica.

Requisito	Atributos Ofertados
2.1 – Comprovação de Performance para os Equipamentos da plataforma RISC	• Estão sendo ofertados equipamentos IBM pSeries p690 Turbo com 16 CPUS de 1.7 GHz. Este equipamento foi auditado pelo Standard Performance Corporation com 32 CPUs. Está sendo apresentada a comprovação por documentação adequada do valor de SPECjbb2000 auditado pelo Standard Performance Evaluation Corporation – SPEC (www.spec.org) para o equipamento cotado. • O equipamento cotado não foi auditado com o número de processadores proposto, desta forma estamos informando um cálculo estimado. O valor utilizado para estimativa de SPECjbb2000 foi obtido em equipamento auditado, com o mesmo tipo/série e tipo de CPU (modelo, clock e cache), do equipamento cotado, o que será comprovado por documentação adequada de auditoria.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 018
Doc. 3702

Requisito	Atributos Ofertados
	• A performance estimada, foi calculada com base na fórmula:SPECjbb2000 estimado = SPECjbb2000 auditado * (nº de CPU ofertadas / nº CPU auditada) • O benchmark de SPECjbb2000 utilizado é superior ao valor máximo especificado.
2.2 – Comprovação de Performance para os Equipamentos da plataforma INTEL	• Todos os equipamentos INTEL para os quais foram solicitados valor de performance baseado em tpm-C, possuem documentação comprobatória adequada do valor do tpm-C auditado pelo Transaction Processing Performance Council – TPC (www.tpc.org) para o equipamento cotado ou para equivalente, conforme documentação em anexo. • Para o servidor Intel Tipo 3 foi utilixzada a formula de performance estimada abaixo:Tpm-C estimado = tpm-C auditado * (no. De CPU ofertadas / no. CPU auditada)
2.3 – Requisitos Gerais	• Os equipamentos serão novos de fábrica e entregues acondicionados adequadamente em caixas fechadas, de forma a permitir completa segurança durante o transporte; • Serão fornecidos pela ITAUTEC, quando da entrega e instalação dos produtos, todos os cabos, acessórios, manuais e documentações completas, que são necessários ao pleno funcionamento dos equipamentos, softwares e periféricos; • Não serão consideradas para efeitos de somatório das quantidades mínimas exigidas, controladoras Fibre Channel e de Rede integradas na placa de sistema; • Serão aceitas, para efeito de somatório, Placas de Rede Ethernet com até 2 (duas) interfaces por placa, na montagem da configuração dos Servidores RISC Tipo 01; • A ECT solicitará o remanejamento de módulos de switch, interfaces de rede ou fibre channel entre os servidores fornecidos, a qualquer momento da vigência do Contrato, sem ônus adicionais.
2.4 – Garantia	• É de total responsabilidade da ITAUTEC, a garantia do pleno funcionamento e operabilidade dos produtos fornecidos, durante a vigência do Contrato.
2.5 – Alimentação Elétrica	• Todos os equipamentos Intel destinados ao CCD de Brasília operam em 220 (duzentos e vinte) volts. • Todos os equipamentos Intel destinados ao CCD de São Paulo operam em 220 (duzentos e vinte) volt, e através da instalação de equipamentos adicionais que realizam compatibilidade elétrica, conforme especificado no subitem 1.3.1.alínea "i" do ANEXO 1-A, estaremos atendendo este item.

16 673

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 019
Doc. 3702

Requisito	Atributos Ofertados
2.6 – Assistência técnica	• A ITAUTEC prestará os serviços assistência técnica nos locais de instalação dos equipamentos, nas cidades de Brasília/DF e São Paulo/SP; • Os serviços prestados devem englobar a substituição de peças e componentes defeituosos dos equipamentos, bem como a depuração e resolução de problemas relacionados ao AMBIENTE OPERACIONAL fornecido pela ITAUTEC.
2.7 – Recursos Mínimos de Particionamento para os Servidores RISC	• O Equipamento RISC Tipo 01 está sendo ofertado com, no mínimo, 8 (oito) partições físicas ou lógicas e são expansíveis a 16 (dezesseis) partições físicas ou lógicas. • O número especificado de partições é alcançado com a simples configuração de software fornecido para este fim, sem a necessidade de adição de nenhum hardware ou software adicionais. Estão sendo ofertadas 2 (duas) consoles em cada localidade, sendo que todas as consoles gerenciam todos os equipamentos em cada localidade; • As partições funcionarão de modo que cada uma execute sua própria imagem de sistema operacional e que a falha do sistema operacional de uma partição não interfira, em hipótese alguma, no funcionamento das demais partições; • Os equipamentos RISC Tipo 01 permitirão o remanejamento de recursos de CPU, Memória e I/O entre as partições; • Os equipamentos RISC Tipo 01 serão fornecidos com todos os recursos de hardware e software necessários à criação do número mínimo de partições especificadas para cada equipamento; • A ITAUTEC fornecerá notebooks, com no mínimo: Processador INTEL Pentium IV 2,0 GHz, 256MB de memória RAM, Placa de Rede e Placa de Faxmodem, para desempenhar a função de gerenciamento e suporte remoto dos servidores RISC. Fornecerão 4 (quatro) notebooks para o CCD de Brasília e 1 (um) notebook para o CCD de São Paulo.
2.8 – Recursos Mínimos	▪ Todos os servidores Intel fornecidos, inclusive os adicionais, possuem mecanismos de detecção de pré-falhas para os componentes vitais ao sistema : CPU, Memória e Discos; ▪ Através da instalação e implementação de um servidor adicional com o sw IBM Director, seus agentes e console de gerenciamento estará disponibilizada a gerência de pré-falhas, sendo disponibilizado um ambiente para cada localidade (CCD de Brasília e CCD de São Paulo)

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 020
Doc. 3702

Requisito	Atributos Ofertados
de Gerenciamento do Hardware requeridos para os Servidores INTEL	
2.9 – Recursos Mínimos de hardware e software para os Servidores INTEL	Todos os servidores INTEL ofertados adicionalmente, serão montados em RACK de 19", conforme o subitem 7, a serem fornecidos pela ITAUTEC; Os equipamentos Intel adicionais serão fornecidos com os seguintes recursos : • Sistema Operacional Microsoft Windows Server 2003 Standard Edition, instalado, licenciado e configurado para Rede Corporativa dos Correios; • 1 (uma) licença do agente 'Concord SystemEdge', devidamente instalado e configurado conforme orientação da equipe técnica dos Correios; • 1 (uma) licença de software agente de backup compatível com o gerenciador de fitoteca especificado no subitem 5.13, devidamente instalado e configurado conforme orientação da equipe técnica dos Correios; Estamos ofertando como servidores adicionais, equipamentos idênticos aos configurados para Intel Tipo 02 e 03. Todos os servidores adicionais possuem os seguintes componentes de hw : • Fontes de alimentação instaladas na configuração máxima do equipamento com recurso de troca sem interrupção (Hot Swap/Hot plug) e alimentação elétrica em 220V para as duas localidades, com frequência 60 (sessenta) Hertz; • As fontes de alimentação são redundantes por fontes internas independentes, com alimentação redundante, de tal forma que, em caso de falha de uma das fontes por defeito ou por falta de alimentação elétrica em um dos 02 (dois) circuitos, o equipamento conitunará funcionando sem prejuízo às aplicações. • Interfaces de rede padrão Ethernet PCI 10/100/1000 BaseT em conformidade com os padrões IEEE 802.3ab e 802.3u com possibilidade de gerenciamento SNMP; • As interfaces de rede conectarão os servidores a Rede do CCD utilizando cabeamento UTP CAT-6 e conectores RJ-45.
	• Os servidores Risc oferecidos adicionalmente serão montados em RACKS de 19". Os Racks serão fornecidos pela ITAUTEC. • A ITAUTEC está fornecendo e irá instalar e configurar, para todos

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 021
Doc. 3702

Requisito	Atributos Ofertados
2.10 – Recursos Mínimos de hardware e software para os servidores RISC adicionais	os servidores RISC cotados adicionalmente os seguintes softwares: • Sistema Operacional AIX 64Bits, será instalado e configurado para Rede dos Correios, e está sendo proposto com número ilimitado de usuários simultâneos; • Sistema de Arquivos JFS • Ferramenta que permita o backup e restore do sistema operacional (Image Backup) • 1 licença do agente "Concord SystemEdge", devidamente instalado e configurado conforme orientação da equipe técnica dos Correios. • 1 licença de software agente de backup compatível com o gerenciador de fitoteca especificado no subitem 5.13, devidamente instalado e configurado conforme orientação da equipe técnica dos correios. • A ITAUTEC está fornecendo e irá instalar, para todos os servidores RISC cotados adicionalmente, os seguintes componentes de hardware: • Fontes instaladas na configuração máxima do equipamento, com recurso de troca sem interrupção (HotSwappable/HotPluggable) e alimentação elétrica de acordo com a localidade onde serão instalados os equipamentos, conforme subitem 2.5, freqüência de 60 (sessenta)Hertz; • As fontes de alimentação propostas são redundantes por fontes internas independentes, com alimentação redundante, de tal forma que, em caso de falha de uma das fontes por defeito ou por falta de alimentação elétrica em um dos 2(dois) circuitos, o equipamento continue a funcionar sem prejuízo das aplicações; • As interfaces de rede serão padrão Ethernet PCI 10/100/1000 Base-T em conformidade com os padrões IEEE 802.3ab e 802.3u com possibilidade de gerenciamento SNMP; • As interfaces de rede irão conectar os servidores a Rede do CCD utilizando cabeamento UTP CAT-6 e conectores RJ45; ▪ 1 (uma) unidade de fita DDS4 interna. Está sendo prevista a entrega de 10 (dez) fitas DDS 3 e 2 (duas) fitas para limpeza.
2.11 – Comprovação dos Requisitos Exigidos	• No fornecimento da documentação técnica, é exigido que sejam fornecidos obrigatoriamente todos os informes, conforme descritos nos subitens que seguem: ▪ A documentação que acompanha o equipamento deve ser em língua portuguesa, espanhola ou inglesa, preferencialmente em língua portuguesa; ▪ A identificação do Fabricante, da Marca e do Modelo do produto. • Comprovação, conforme MODELO VIII do ANEXO 3, de todos

6.670

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 022
Doc. 3702

Requisito	Atributos Ofertados
	os atributos exigidos nesta planilha de Especificações, atestada pelo fornecimento do descrito em qualquer dos subitens que seguem ou pelo conjunto destes: • Prospecto técnico do modelo cotado, o qual deve ser preferencialmente no original ou fotocópia legível e completa, com grifo nas características técnicas a serem informadas; ▪ Cópia legível e atual da página Internet do Fabricante onde constem às especificações técnicas do modelo do produto cotado, com grifo nas características técnicas a serem informadas
2.12 – Organização da Documentação	• A ITAUTEC organizará toda a documentação dos equipamentos e softwares de forma que estejam reunidas e catalogadas, nos CCDs de Brasília e São Paulo, cópias da documentação técnica de cada tipo de equipamento ofertado, bem como cópias do CDs de instalação de cada software fornecido pela ITAUTEC; • A ITAUTEC entregará, sem ônus para a ECT , os CDs com toda atualização dos softwares fornecidos, durante a vigência do Contrato. Será entregue 1 (uma) cópia no CCD de Brasília e 1 (uma) cópia no CCD de São Paulo.
2.13 – Suporte Remoto	• A ITAUTEC disponibilizará todos os PRODUTOS necessários à implementação de uma estrutura de acesso remoto que permita a ITAUTEC acesso a rede corporativa da ECT , utilizando o Switch Tipo 5 a ser fornecido de acordo com o subitem 3.5.; • Esta estrutura de acesso remoto que será utilizado pela ITAUTEC possa prestar serviço de suporte remoto nas • Situações em que a ECT julgue necessária. A estrutura de acesso remoto seguirá estritamente as Normas de Segurança definidas pela ECT.
2.14 – Configuração das Ferramentas de Gerenciamento	• Durante o Treinamento de Gerenciamento, descrito no Subitem 1.9.2.3. do ANEXO 1-A, a ITAUTEC irá instalar e configurar os novos agentes 'Concord SystemEdge', integrando conforme os padrões da plataforma de Gerência já existente da ECT ; • A ITAUTEC configurará os agentes 'Concord SystemEdge' para, entre outras coisas, medir o tempo de resposta dos serviços de infra-estrutura, não se limitando a: DNS, HTTP, HTTPS, SMTP, POP3, FTP e TCP; • A ITAUTEC configurará os agentes 'ConcordSystemEdge' para que monitore o desempenho e falhas das aplicações Exchange, Oracle, MS SQL, APACHE e IIS; • A ITAUTEC habilitará o agente SNMP dos Roteadores, Switches

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 023
3702
Doc

Requisito	Atributos Ofertados
	e servidores fornecidos, conforme os padrões da ECT ; • A ITAUTEC configurará as ferramentas de gerenciamento existentes na ECT , não se limitando a: ▪ Integração de eventos no HP OpenView Operations; ▪ Criação e integração de regras inteligentes do Concord Live Health para envio de eventos ao HP OpenView Operations; ▪ Criação e geração de relatórios do Concord eHealth.

1. CONECTIVIDADE DA REDE

1.1. SWITCH TIPO 3 (FC)

OBJETIVO	
Conectividade com os Storage Existente e Backup Robotizado	
Requisito	**Atributos Ofertados**
1 – Recursos Básicos	Deverão ser disponibilizados equipamentos de SWITCH, com um mínimo de 64 portas Fibre Channel, operando a 2 Gbit/sec, que deverão ser interligados a rede SAN já existente na **CONTRATANTE**. Os equipamentos fornecidos deverão interligar todos os elementos relativos a Storage Area Network – SAN, definidos neste Edital, a saber: o SERVIDORES (INTEL e RISC) fornecidos; o STORAGE (IBM 2105 F20); o BACKUP fornecido. • Os switches deverão possuir, no mínimo, os seguintes recursos: o Possibilidade de configuração das portas de forma independente; o Portas "HOT-SWAPPABLE/HOT-PLUGGABLE"; o Modularidade. • Os **SWITCHES TIPO 3** deverão ser montados em RACKS de 19" de acordo com o **subitem 7,** a serem fornecidos pela **CONTRATADA**.
2 – Portas Ethernet	• Deverá possuir, no mínimo, 1 (uma) interface Fast-Ethernet 10/100 autosensing, com protocolo SNMP para gerência.
3 – Cabeamento	• Deverão ser disponibilizados e instalados, todos os recursos necessários ao cabeamento, incluindo os cabos, que deverão ser em Fibra Ótica Multi Mode com conectores LC.
4 – Recursos	• Os equipamentos deverão ser acompanhados de todos os recursos de hardware, software, cabos, manuais, etc necessários a sua total instalação, configuração, gerenciamento e utilização. • Deverá for fornecida pela **CONTRATADA** ferramenta que

ECT nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 024
Doc. 3702

Requisito	Atributos Ofertados
	implemente o gerenciamento da Rede SAN, contemplando todos os agentes e consoles necessários ao seu pleno funcionamento.Esta ferramenta deve: o Permitir descoberta automática dos elementos que compõe a SAN, baseado em protocolo SNMP ou agentes da própria ferramenta; o Permitir a visão lógica da topologia dos elementos que compões a SAN, de forma gráfica, incluindo as interconexões FC, switches, servidores e devices de storage em uma única console; o Ter a capacidade de apresentar detalhes sobre as conexões das portas FC; o Ter a capacidade de receber eventos provenientes dos elementos constantes na topologia SAN; o Possibilitar o envio dos eventos recebidos através de protocolo SNMP ou agentes próprios. • Deverão ser montados 2 (dois) ambientes de gerenciamento da Rede SAN, sendo 1 (um) no CCD de Brasília e 1 (um) no CCD de São Paulo. • A **CONTRATADA** deverá fornecer os servidores necessários para a implantação da gerência da rede SAN.
5 – Compatibilidade e Integração	• Os equipamentos deverão ser totalmente compatíveis e fornecer suporte total aos padrões FIBER CHANNEL. • Os equipamentos fornecidos deverão integrar-se aos equipamentos já existentes na **CONTRATANTE**, formando uma única rede SAN em cada localidade Brasília-DF e São Paulo-SP. • As versões dos equipamentos existentes são as seguintes: o Switches: Modelo IBM 2109-S16; Fabricante IBM (OEM Brocade 2800 SilkWorm), versão de microcódigo A2.4.1C; o Storage: Modelo 2105-F20 (IBM) com dois microcódigos (2 dispositivos de armazenamento): 1.5.2.103 e 1.3.2.49; o HBA´s: Modelo QLOGIC QLA 2200 - PCI Fibre Channel Adapter, versão de Microcódigo 8.0.8.1.
6 – Fonte de Alimentação	• Fontes instaladas na configuração máxima do equipamento, com recurso de troca sem interrupção (HOT-SWAPPABLE/HOTPLUGGABLE) e alimentação elétrica de acordo com a localidade onde serão instalados os equipamentos, conforme **subitem 2.5.**, freqüência de 60 (sessenta) Hertz; • As fontes de alimentação deverão ser redundantes por fontes internas independentes, com alimentação redundante, de tal forma que, em caso de falha de uma das fontes por defeito ou por falta de alimentação elétrica em um dos 2 (dois) circuitos, o equipamento continue a funcionar sem prejuízo das aplicações.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 025
Doc 3702

16.666
L

2. SERVIDORES CORPORATIVOS

2.1. SERVIDORES INTEL

2.1.1. SERVIDORES INTEL TIPO 1

OBJETIVO
Banco de Dados de Grande Porte e Correio Eletrônico Corporativo

Requisito	Atributos Ofertados
1 – CPU e Performance	• Servidor composto por processadores Intel, com 8 (oito) processadores INTEL XEON MP, com clock de 2,0 GHz, sem a formação de Cluster; • O equipamento possui performance 119.115 tpm-C, conforme especificado no Subitem 2.2.; • O equipamento será montado em RACK próprio do fabricante com 42U de altura.
2 – Barramento	• Barramento do sistema de 400 MHz.
3 – Memória Cache	• 2MB (dois Megabytes) por processador
4 – Memória RAM	• 8 GB (oito gigabytes) ECC SDRAM.
5 – Controladora e Unidade de Disco Rígido – Interno	▪ Capacidade em disco de 72 GB (líquidos) após implementado um arranjo em RAID 1 por hardware utilizando discos com tempo médio de acesso igual a 4,9 ms e velocidade de rotação de 10.000 RPM. ▪ Controladora de discos padrão Ultra 3 / Ultra 160 SCSI, com suporte a troca de discos defeituosos sem interrupção no funcionamento do equipamento. ▪ Controladoras de disco instalada em slot PCI-X.
6 – Interface de VIDEO	• Padrão SVGA, PCI 32 Bits, com 8 Mbytes.
7 – Unidade de CD/DVD-ROM	• 1 (uma) unidade interna, tecnologia IDE, com velocidade de 24X CD-ROM.
8 – Controladora de I/O (por equipamento)	• Serão disponibilizadas controladoras FIBER CHANNEL, operando a 2Gb/s, para acesso à Rede SAN, com disponibilidade para 2 (dois) canais; • Serão disponibilizadas 3 (três) interfaces de rede padrão Ethernet PCI 10/100/1000 Base-T em conformidade com os padrões IEEE 802.3ab e

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 026
Doc. 3702

Requisito	Atributos Ofertados
	802.3u, com possibilidade de gerenciamento SNMP.; • As interfaces de rede conectarão os servidores a Rede do CCD utilizando cabeament UTP CAT-6 e conectores RJ-45.
9 – Ambiente Operacional	• Os Servidores INTEL TIPO 1 serão fornecidos com o seguinte ambiente operacional para cada equipamento: ▪ Microsoft Windows Server 2003 Enterprise Edition, com número ilimitado de usuários simultâneos, instalado, licenciado e configurado para Rede Corporativa dos Correios; ▪ 1 (uma) licença do agente 'Concord SystemEdge', devidamente instalado e configurado conforme orientação da equipe técnica dos Correios; ▪ 1 (uma) licença de software agente de backup compatível com o software gerenciador de fitoteca especificado no Subitem 5.13 que permita backup LAN FREE, devidamente instalado e configurado conforme orientação da equipe técnica dos Correios; • Deve ser fornecido, na modalidade de licenciamento por CPU, para uso perpétuo, o SGBD MICROSOFT SQL SERVER 2000 ENTERPRISE EDITION para 7 (sete) servidores INTEL TIPO 1. O SGBD será instalado e configurado em Cluster pela Itautec, utilizando o recurso de cluster do sistema operacional, de acordo com a configuração definida pela ECT .
10 – Fonte de Alimentação	• Instalada na configuração máxima do equipamento; • Suporte ao recurso de troca sem interrupção (HOT-SWAPPABLE/HOT-PLUGGABLE); • Possui alimentação elétrica de 220V em cada localidade onde serão instalados os equipamentos, conforme subitem 2.5., freqüência de 60 (sessenta) Hertz; • As fontes de alimentação são redundantes por fontes internas independentes, com alimentação redundante, de tal forma que, em caso de falha de uma das fontes por defeito ou por falta de alimentação elétrica em um dos 2 (dois) circuitos, o equipamento continue a funcionar sem prejuízo das aplicações.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 027
Doc. 3702

2.1.2. SERVIDORES INTEL TIPO 2

OBJETIVO
Banco de Dados de Médio Porte e Aplicações Corporativas

Requisito	Atributos Ofertados
1 – CPU e Performance	• Servidor composto por processadores Intel, com no mínimo 4 (quatro) processadores INTEL XEON MP, com clock mínimo de 2,0 GHz, sem a formação de Cluster; • O equipamento deve apresentar performance mínima de 50.000 tpm-C, conforme especificado no Subitem 2.2.; • O equipamento deve ser montado em RACK próprio do fabricante com, no mínimo, 40U de altura.
2 – Barramento	• Barramento do sistema de, no mínimo, 400 MHz.
3 – Memória Cache	• 2MB (dois Megabytes) por processador.
4 – Memória RAM	• 4 GB (quatro gigabytes) ECC SDRAM ou tecnologia superior,instalada.
5 – Controladora e Unidade de Disco Rígido – Interno	• Capacidade em disco de, no mínimo, 72 GB (líquidos) após implementado um arranjo em RAID 1 por hardware utilizando discos com tempo médio de acesso menor ou igual a 6 ms e velocidade de rotação mínima de 10.000 RPM. • Controladora de discos padrão Ultra 3 SCSI ou superior , com funcionalidade que permita a troca de discos ou periféricos defeituosos sem interrupção no funcionamento do equipamento. • São aceitas controladoras de disco instaladas na placa de sistema.
6 – Interface de VIDEO	• Padrão SVGA, PCI 32 Bits ou superior, com 8 Mbytes no mínimo.
7 – Unidade de CD/DVD-ROM	• 1 (uma) unidade interna, tecnologia IDE ou SCSI, com velocidade mínima de 24X CD-ROM ou 4X DVD-ROM.
8 – Controladora de I/O	• Devem ser disponibilizadas controladoras FIBER CHANNEL, operando a 2Gb/s, para acesso à Rede SAN, com disponibilidade mínima para 2 (dois) canais;

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 028
Doc 3702

1663

Requisito	Atributos Ofertados
(por equipamento)	• Devem ser disponibilizadas 2 (duas) interfaces de rede padrão Ethernet PCI 10/100/1000 Base-T em conformidade com os padrões IEEE 802.3ab e 802.3u, com possibilidade de gerenciamento SNMP; • As interfaces de rede devem conectar os servidores a Rede do CCD utilizando cabeamento UTP CAT-6 e conectores RJ-45.
9 – Ambiente Operacional	Os Servidores INTEL TIPO 2 devem ser fornecidos com o seguinte ambiente operacional para cada equipamento: ▪ Microsoft Windows Server 2003 Enterprise Edition, com número ilimitado de usuários simultâneos, instalado, licenciado e configurado para Rede Corporativa dos Correios; ▪ 1 (uma) licença do agente 'Concord SystemEdge', devidamente instalado e configurado conforme orientação da equipe técnica dos Correios; ▪ 1 (uma) licença de software agente de backup compatível com o gerenciador de fitoteca especificado no subitem 5.13, devidamente instalado e configurado conforme orientação da equipe técnica dos Correios.
10 – Fonte de Alimentação	• Instalada na configuração máxima do equipamento; • Recurso de troca sem interrupção (HOT-SWAPPABLE/HOT-PLUGGABLE); • Possuirá alimentação elétrica de acordo com a localidade onde instalarão os equipamentos, conforme subitem 2.5., freqüência de 60 (sessenta) Hertz; • As fontes de alimentação devem ser redundantes por fontes internas independentes, com alimentação redundante, de tal forma que, em caso de falha de uma das fontes por defeito ou por falta de alimentação elétrica em um dos 2 (dois) circuitos, o equipamento continue a funcionar sem prejuízo das aplicações.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 029
Doc 3702

16.662
i-

2.1.3. SERVIDORES INTEL TIPO 3

OBJETIVO
Banco de Dados de Pequeno Porte, Servidores de Aplicação e Serviços de Rede

Requisito	Atributos Ofertados
1 – CPU e Performance	• Servidor composto por processadores Intel, com no mínimo 2 (dois) processadores INTEL XEON, com clock mínimo de 2,4 GHz; • O equipamento deve apresentar performance mínima de 30.000 tpm-C, conforme especificado no Subitem 2.2.; • O equipamento deve ser montado em RACK próprio do fabricante com, no mínimo, 40U de altura.
2 – Barramento	• Barramento do sistema de, no mínimo, 533 MHz.
3 – Memória Cache	• 512kB por processador.
4 – Memória RAM	• 1,5GB (um gigabyte e meio) ECC SDRAM ou tecnologia superior, instalada.
5 – Controladora e Unidade de Disco Rígido– Interno	• Capacidade em disco de, no mínimo, 72 GB (líquidos) após implementado um arranjo em RAID 1 por hardware utilizando discos com tempo médio de acesso menor ou igual a 6 ms e velocidade de rotação mínima de 10.000 RPM. • Controladora de discos padrão Ultra 3 SCSI ou superior , com funcionalidade que permita a troca de discos ou periféricos defeituosos sem interrupção no funcionamento do equipamento. • São aceitas controladoras de disco instaladas na placa de sistema.
6 – Interface de VIDEO	• Padrão SVGA, PCI 32 Bits ou superior, com 8 Mbytes no mínimo.
7 – Unidade de CD/DVD-ROM	• 1 (uma) unidade interna, tecnologia IDE ou SCSI, com velocidade mínima de 24X CD-ROM ou 4X DVD-ROM.
8 – Controladora de I/O (por equipamento)	• Devem ser disponibilizadas 2 (duas) interfaces de rede padrão Ethernet PCI 10/100/1000 Base-T em conformidade com os padrões IEEE 802.3ab e 802.3u, com possibilidade de gerenciamento SNMP.;

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 030
Doc 3702

Requisito	Atributos Ofertados
	• As interfaces de rede devem conectar os servidores a Rede do CCD utilizando cabeamento UTP CAT-6 e conectores RJ-45.
9 – Ambiente Operacional	• Os Servidores INTEL TIPO 3 devem ser fornecidos com o seguinte ambiente operacional para cada equipamento: ▪ Microsoft Windows Server 2003 Standard Edition, com número ilimitado de usuários simultâneos, instalado, licenciado e configurado para Rede Corporativa dos Correios; ▪ 1 (uma) licença do agente 'Concord SystemEdge', devidamente instalado e configurado conforme orientação da equipe técnica dos Correios; ▪ 1 (uma) licença de software agente de backup compatível com o gerenciador de fitoteca especificado no subitem 5.13, devidamente instalado e configurado conforme orientação da equipe técnica dos Correios.
10 – Fonte de Alimentação	• Instalada na configuração máxima do equipamento; • Recurso de troca sem interrupção (HOT-SWAPPABLE/HOT-PLUGGABLE); • Possuirá alimentação elétrica de acordo com a localidade onde instalarão os equipamentos, conforme subitem 2.5., freqüência de 60 (sessenta) Hertz; • As fontes de alimentação devem ser redundantes por fontes internas independentes, com alimentação redundante, de tal forma que, em caso de falha de uma das fontes por defeito ou por falta de alimentação elétrica em um dos 2 (dois) circuitos, o equipamento continue a funcionar sem prejuízo das aplicações.

2.2. SERVIDORES RISC

2.2.1 SERVIDORES RISC TIPO 1

OBJETIVO
Banco de Dados e aplicações corporativas.

Requisito	Atributos Ofertados
1 – CPU e Performance	Servidor composto por 16 processadores RISC Power4+ 1.7GHz que apresenta performance mínima de 276.740 SPECjbb2000, com possibilidade de expansão a 553.480 SPECjbb2000

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 031
Doc 3702

Requisito	Atributos Ofertados
2 – Memória RAM	64 Gbytes, instalada, com possibilidade de expansão para, no mínimo, 512 Gbytes, com disponibilidade de recursos para verificação de erro
3 – Suporte à Arquitetura	SMP – Symetric Multi Processing

4 – Fonte de Alimentação	• Estão sendo propostas 2 fontes, número suficiente para suportar a operação do equipamento na configuração máxima especificada:
	  • As fontes possuem recurso de troca sem interrupção (Hot-Swappable/Hot Pluggable)
	  • A alimentação elétrica estará disponível de acordo com a tensão da localidade onde serão instalados os equipamentos e a freqüência de alimentação é de 60 (sessenta) Hertz;
	  • As fontes de alimentação são redundantes por fontes internas independentes, com alimentação redundante, de tal forma que, em caso de falha de uma das fontes por defeito ou por falta de alimentação elétrica eum um dos dois (2) circuitos, o equipamento continue a funcionar sem prejuízo das aplicações.

5 – Controladoras e Disco Rígido	• Estão sendo propostas 16 discos de 36GB, com funcionalidade de troca sem interrupção, com tempo médio de acesso menor ou igual a 6ms e com velocidade de rotação mínima de 10.000 RPM. • Estão sendo propostas 8 controladoras de disco PCI Ultra3 SCSI não incorporadas na placa de sistema
6 – Controladora de I/O	• Estão sendo propostas 16 controladoras Fiber Channel operando a 2Gb/s, para acesso de alta velocidade a unidades de STORAGE e BACKUP. • Estão sendo propostas 16 (dezesseis) interfaces de rede padrão Ethernet PCI 10/100/1000 Base-T em conformidade com os padrões IEEE 802.3ab e 802.3u, com possibilidade de gerenciamento SNMP. • As interfaces de rede irão conectar os servidores a Rede do CCD utilizando cabeamento UTP CAT-6 e conectores RJ-45.
7 – Unidade de CD/DVD-ROM e Backup	• Está sendo proposta 1 (uma) unidade de CD-ROM e 1 (uma) unidade de leitora/gravadora de Fita DAT DDS-4 • O Servidor possui capacidade de remanejar a unidade de fita e a unidade de CD-ROM para qualquer uma das partições implementadas, pela simples configuração de software, sem a interrupção das aplicações em execução. • A unidade de CD-ROM possui velocidade de 32x. A unidade leitora/gravadora de fita atende ao padrão DDS 4 • Está prevista a entrega de 10 (dez) fitas novas, padrão DDS 3 e 2 (duas) fitas para limpeza para cada unidade leitora/gravadora de fitas.

16.660

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 032
Doc. 3702

16.699
L

Requisito	Atributos Ofertados
8 – Ambiente Operacional	• Os servidores RISC Tipo 1 estão sendo fornecidos com o seguinte ambiente operacional, licenciado para cada uma das 8 (oito) partições do equipamento: • Sistema operacional AIX 5.2, 64 Bits, instalado e configurado para Rede dos Correios, com número ilimitado de usuários simultâneos; • Sistema de arquivos JFS (Journaled File System) proposto está disponível dentro do sistema operacional AIX 5.2 • Está sendo proposto o Network Install Manager incluído no sistema operacional AIX 5.2. Esta ferramenta permite o backup e restore do sistema operacional (IMAGE BACKUP) pela rede TCP/IP • Está sendo proposta uma licença do agente "Concord SystemEdge" devidamente instalado e configurado conforme orientação da equipe técnica dos Correios; • Está sendo proposta uma licença de software agente de backup que permite backup LAN FREE compatível com o gerenciador de fitoteca especificado no subitem 5.13 devidamente instalado e configurado conforme orientação da equipe técnica dos Correios. • O sistema operacional AIX 5.2 e o servidor p690 (7040-681) são produzidos pelo mesmo Fabricante – IBM; • Estão sendo fornecidas licenças do compilador C para 6 (seis) servidores RISC TIPO1. A versão fornecida do compilador está homologada para o AIX 5.2. As licenças foram dimensionadas considerando-se o número de processadores fornecidos em cada equipamento. O compilador C é compatível com o padrão ANSI C. • Estão sendo fornecidas e instaladas as licenças do software HACMP 4.5 que permite a criação do ambiente clusterizado entre os equipamentos fornecidos. • Estão sendo fornecidas 11 (onze) licenças de HACMP (uma por máquina), que permitem a formação de 16 clusters por equipamento. Essas licenças permitem a criação de até 88 clusters para o ambiente. Dessa forma a ECT pode configurar os seguintes ambientes: • 14 (quatorze) clusters com 2 (dois) nós para o CCD de Brasília/DF; • 6 (seis) clusters com 2 (dois) nós para o CCD de São Paulo/SP

3. UNIDADE DE BACKUP

OBJETIVO
Backup Corporativo

RQS nº 03/2005 - CN
CPMI – CORREIOS
Fls Nº 033
Doc 3702

Requisito	Atributos Ofertados
1 – Descrição	• Serão fornecidos 2 (dois) sistemas automatizados de armazenamento de dados em cartuchos padrão `LTO Ultrium 2`, incorporando controladora robotizada, gabinete e software de gerenciamento. Sendo 1(um) sistema para o CCD de Brasília-DF e 1 (um) sistema para o CCD de São Paulo-SP
2 – Capacidade da Biblioteca	• Para o CCD de Brasília, o equipamento possui capacidade de armazenamento e recuperação de dados para a tecnologia'LTO ULTRIUM 2' de, com 60 TB (sessenta Terabytes), sem compressão (nativo); • Para o CCD de São Paulo, o equipamento possui capacidade de armazenamento e recuperação de dados para a tecnologia'LTO ULTRIUM 2' de, com 40 TB (quarenta Terabytes), sem compressão (nativo); • Não será considerada para efeito de cálculo da capacidade solicitada tecnologia de compactação e/ou compressão.
3 – Capacidade dos Cartuchos	• O Cartucho 'LTO Ultrium 2' possui capacidade de 200 GBytes (sem compressão).
4 – Compatibilidade	• O hardware é compatível com o padrão 'LTO Ultrium', permiti a leitura de cartuchos, neste padrão, instalados na fitoteca atualmente instalada nos Correios ('3583-L72 IBM LTO Ultrium').
5 – Quantidade de SLOTS	• Na fitoteca ofertada para o CCD de Brasília possui 300 Slots (60 TB/ 200GB) • Na fitoteca ofetada para o CCD de São Paulo possui 200 Slots (40TB/ 200GB)
6 – Quantidade de Cartuchos	• Para o CCD de Brasília está sendo fornecido 600 cartuchos (300*2) • Para o CCD de São Paulo está sendo fornecido 400 cartuchos (200*2)
7 – THROUGHPUT por drive	• Os drives apresentam performance nominal de 35MB/segundo para gravação, sem compactação, utilizando cartuchos padrão 'LTO Ultrium 2'

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 034
Doc. 3702

Requisito	Atributos Ofertados
8 – Número de DRIVES	• Para o CCD de Brasília, o equipamento possui no 20 (vinte) drives, atingindo o THROUGHPUT nominal de 600 (seiscentos) MB/segundo, utilizando tecnologia de gravação linear, que permite operação simultânea de todos os drives. • Para o CCD de São Paulo, o equipamento possui no 12 (Doze) drives, atingindo o THROUGHPUT nominal de 360 (Trezentos e sessenta) MB/segundo, utilizando tecnologia de gravação linear, que permite operação simultânea de todos os drives.
9 – Conectividade	• Fibre Channel, operando a 2 Gbit/sec, entre os servidores e a unidade de backup.
10 – Recursos de Hardware	• Possui capacidade de manutenção/substituição de cartuchos, sem interrupção dos processos de BACKUP ou RESTORE em curso; • Possui 1 (uma) porta de Comunicação para diagnóstico. • Sistema de leitura de cógido de barras; • Os rótulos dos cartuchos - LABEL, deverão seguir padrão definido pela ECT.
11 – Retirada das Fitas	• Os equipamentos e Softwares fornecidos permiti a realização da cópia dos dados armazenados nos cartuchos em cartuchos novos.; • Os equipamentos e softwares fornecidos permite que a CONTRATANTE realize a retirada dos cartuchos duplicados sem que esta operação interrompa os demais porcessos de BACKUP ou RESTORE em curso.
12 – Recursos Necessários	• O equipamento possui recurso automático para limpeza de todos os drives, utilizando processo transparente de operação; • Será fornecida 1(uma) fita de limpeza para cada drive de leitura/gravação.
13 – Recursos de Software	• Serão fornecidas e instaladas nos servidores descritos no subitem 5.15. licenças de software que desempenhe as funções de um GERENCIADOR DE FITA E DE BACKUP;

RQS nº 03/2005 CN
CPMI CORREIOS
Fls Nº 035
Doc 3702

16.656

Requisito	Atributos Ofertados
	• As licenças serão fornecidas considerando-se o número de unidades de backup solicitadas e o número total de servidores fornecidos; • Os PRODUTOS de backup fornecidos realizam o BACKUP On-Line do SGBD ORACLE que será instalado em, pelo menos, 10 (dez) partições dos servidores RISC Tipo 01; • Os PRODUTOS de backup fornecidos realizam o Backup/Restore da base de dados do MS Exchange Server 2000 que será instalado em, pelo menos, 8 (oito) Servidores INTEL Tipo 01.
14 – Fonte de Alimentação Interna	• O n. de fontes instaladas é suficiente para suportar a operação do equipamento na configuração máxima especificada; • Possui alimentação elétrica de acordo com a localidade onde serão instalados os equipamentos, conforme subitem 2.5, freqüência de 60 (sessenta) Hertz; • As fontes de alimentação são redundantes por fontes internas independentes, com alimentação redundante, de tal forma que, em caso de falha de uma das fontes por defeito ou por falta de alimentação elétrica em um dos 2 (dois) circuitos, o equipamento continue a funcionar sem prejuízo das aplicações;
15 – Geral	• Serão fornecidos 2 (dois) servidores RISC para o CCD de Brasília, em alta disponibilidade, para abrigar os softwares gerenciadores das fitotecas e os softwares gerenciadores do backup; • Serão fornecidos 2 (dois) servidores RISC para o CCD de São Paulo, em alta disponibilidade, para abrigar o software gerenciador da fitoteca e o software gerenciador do backup; • Os servidores devem estar dimensionados de tal forma que suportem o gerenciamento de, no mínimo, 150 clientes de backup, individualmente.

4. RACK PARA EQUIPAMENTOS

Requisito	Atributos Ofertados
1 – Estrutura	• Todos os equipamentos fornecidos, que não tenham RACK próprio do fabricante, serão instalados em estruturas de RACK, com as seguintes características: ▪ RACK do tipo fechado, em aço, com 19" de largura e profundidade de 103cm, para fixação dos dispositivos ofertados; ▪ Altura de 42U; ▪ Permite a instalação de todos os equipamentos com largura padrão de 19"

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 036
Doc. 3702

16.655

Requisito	Atributos Ofertados
Física	(dezenove polegadas); ▪ Sistema de ventilação através de portas perfuradas; ▪ colunas de segundo plano (aproximadamente 10 cm); ▪ sistema de chave e fechadura; laterais e traseira removíveis; guias de roteamento verticais e horizontais (organizadores de cabos).
2 – Estrutura Funcional	• Os RACKS serão interligados à rede elétrica através de tomadas tripolares, a serem instaladas pela Itautec quando realizar a adequação da estrutura elétrica das Salas de Segurança Físicas, conforme subitem 1.3.1. alínea i. do ANEXO 1-A do Edital; • A Itautec instalará 32 (trinta e duas) réguas de tomadas no suíte de Racks no CCD de Brasília, e outras 27 (vinte e sete), no CCD de São Paulo, considerando cada circuito elétrico existente na Sala de Segurança Física, com tomadas universais em número suficiente para total de elementos instalados no RACK. As réguas possuem pinagem compatível com as tomadas dos equipamentos instalados no RACK. • OBS.: As PDUs deverão ter suas tomadas removidas e substituídas por tomadas padrão ABNT.
3 – Gerais	• A quantidade de RACKS dimesionada pela Itautec é de 8 para o CCD de Brasília e 5 para o CCD de São Paulo e deverá ser aprovado pela ECT, levando-se em conta a atual distribuição dos equipamentos nas Salas de Segurança Física e os critérios de padronização do layout definidos pela ECT.

São Paulo, 23 de julho de 2003

Carmem Lúcia Távora Vieira
Gerente de Unidade de Negócios
IBM Brasil - Indústria, Máquina e Serviços Ltda.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 037
Doc. 3702

16 6541

Segurança Tipo 1 doc 1

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 038
Doc 3702

Cisco Systems

16.653
L

Data Sheet

Cisco PIX **535** Security Appliance

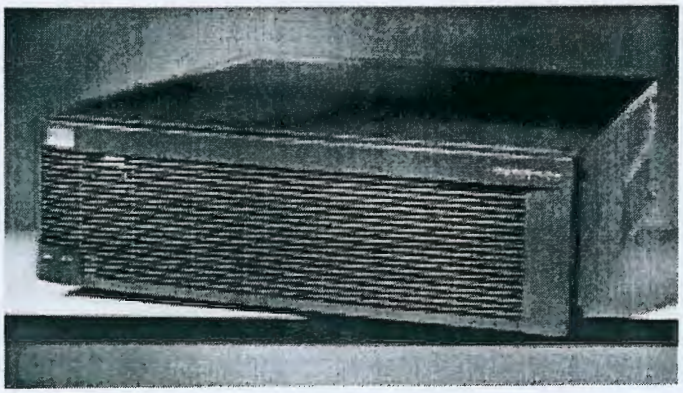
The Cisco PIX® 535 Security Appliance delivers enterprise-class security for enterprise and service provider networks in a high performance, purpose-built appliance. Its highly modular three-rack unit (3RU) design supports up to ten 10/100 Fast Ethernet interfaces or nine Gigabit Ethernet interfaces as well as redundant power supplies, making it an ideal choice for businesses requiring the highest levels of performance, port density, reliability, and investment protection. Part of the world-leading Cisco PIX Security Appliance Series, the Cisco PIX 535 Security Appliance provides a wide range of rich integrated security services, hardware VPN acceleration capabilities, and powerful remote management capabilities in a highly scalable, high-performance solution.

Enterprise-Class Security for Large Enterprise and Service Provider Networks

The Cisco PIX 535 Security Appliance delivers a multilayered defense for enterprise and service provider networks through rich, integrated security services including stateful inspection firewalling, protocol and application inspection, virtual private networking (VPN) in-line intrusion protection, and rich multimedia and voice security in a single device. The state-of-the-art Cisco Adaptive Security Algorithm (ASA) provides rich stateful inspection firewall services, tracking the state of all authorized network communications and preventing unauthorized network access.

Enterprise networks benefit from an additional layer of security via intelligent, "application-aware" security services that examine packet streams at Layers 4–7, using inspection engines specialized for many of today's popular applications. Administrators can also easily create custom security policies for firewall traffic by using the flexible access control methods and the more than 100 predefined applications, services, and protocols that Cisco PIX Security Appliances provide.

Figure 1
Cisco PIX 535 Security Appliance



Market-Leading Voice-over-IP Security Services Protect Next-Generation Converged Networks

Cisco PIX Security Appliances provide market-leading protection for a wide range of voice-over-IP (VoIP) and multimedia standards, allowing businesses to securely take advantage of the many benefits that converged data, voice, and video networks deliver. By combining VPN with the rich

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Reg'd 07/25/06
File No. 039
№ Doc 3702

16.652

stateful inspection firewall services that Cisco PIX Security Appliances provide for these converged networking standards, businesses can securely extend voice and multimedia services to home office and remote office environments for additional cost savings, improved productivity, and competitive advantage.

Flexible VPN Services Extend Networks Economically to Remote Networks and Mobile Users

Businesses can securely extend their networks across low-cost Internet connections to mobile users, business partners, and remote offices worldwide using the full-featured VPN capabilities provided by the Cisco PIX 535 Security Appliance. Solutions range from standards-based site-to-site VPN leveraging the Internet Key Exchange (IKE) and IP security (IPsec) VPN standards, to the innovative Cisco Easy VPN capabilities found in Cisco PIX Security Appliances and other Cisco security solutions—such as Cisco IOS® routers and Cisco VPN 3000 Series Concentrators. Easy VPN delivers a uniquely scalable, cost-effective, and easy-to-manage remote-access VPN architecture that eliminates the operational costs associated with maintaining remote-device configurations typically required by traditional VPN solutions. Cisco PIX Security Appliances encrypt data using 56-bit Data Encryption Standard (DES), 168-bit Triple DES (3DES), or up to 256-bit Advanced Encryption Standard (AES) encryption. Certain Cisco PIX 535 Security Appliance models have integrated hardware VPN acceleration capabilities, delivering highly scalable, high performance VPN services.

Integrated Intrusion Protection Guards Against Popular Internet Threats

The integrated in-line intrusion-protection capabilities of the Cisco PIX 535 Security Appliance can protect enterprise networks from many popular forms of attacks, including Denial-of-Service (DoS) attacks and malformed packet attacks. Using a wealth of advanced intrusion-protection features, including DNSGuard, FloodGuard, FragGuard, MailGuard, IPVerify and TCP intercept, in addition to looking for more than 55 different attack "signatures," Cisco PIX Security Appliances keep a vigilant watch for attacks, can optionally block them, and can notify administrators about them in real time.

Award-Winning Resiliency Provides Maximum Business Uptime

Select models of Cisco PIX 535 Security Appliances provide stateful failover capabilities that ensure resilient network protection for enterprise network environments. Employing a cost-effective, active-standby, high-availability architecture, Cisco PIX Security Appliances that are configured as a failover pair continuously synchronize their connection state and device configuration data. Synchronization can take place over a high-speed LAN connection, providing another layer of protection through the ability to geographically separate the failover pair. In the event of a system or network failure, network sessions are automatically transitioned between appliances, with complete transparency to users.

Robust Remote-Management Solutions Lower Total Cost of Ownership

The Cisco PIX 535 Security Appliance is a reliable, easy-to-maintain platform that provides a wide variety of methods for configuring, monitoring, and troubleshooting. Management solutions range from centralized, policy-based management tools to integrated, Web-based management to support for remote monitoring protocols such as Simple Network Management Protocol (SNMP) and syslog.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0402
Doc. 3702

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

16.651

Administrators can easily manage large numbers of remote Cisco PIX Security Appliances using CiscoWorks VPN/Security Management Solution (VMS). This suite consists of numerous modules including Management Center for Firewalls, Auto Update Server Software and Security Monitor. This powerful combination provides a highly scalable, next-generation, three-tier management solution that includes the following features:

- Comprehensive configuration and software image management
- Device hierarchy with "Smart Rules"-based configuration inheritance
- Customizable administrative roles and access privileges
- Comprehensive enterprise change management and auditing
- "Touchless" software image management for remote Cisco PIX Security Appliances
- Support for dynamically addressed appliances

Additional integrated event management and inventory solutions are also available as part of the CiscoWorks VMS network management suite.

The integrated Cisco PIX Device Manager provides an intuitive, Web-based management interface for remotely configuring, monitoring, and troubleshooting a Cisco PIX 535 Security Appliance—without requiring any software (other than a standard Web browser) to be installed on an administrator's computer. A setup wizard is provided for easy installation into any network environment.

Alternatively, through methods including Telnet and Secure Shell (SSH), or out of band through a console port, administrators can remotely configure, monitor, and troubleshoot Cisco PIX Security Appliances using a command-line interface (CLI).

Table 1 Key Product Features and Benefits

Key Features	Benefit
Enterprise-Class Security	
True security appliance	• Uses a proprietary, hardened operating system that eliminates security risks associated with general purpose operating systems • Cisco quality and no moving parts provide a highly reliable security platform
Stateful inspection firewall	• Provides perimeter network security to prevent unauthorized network access • Uses state-of-the-art Cisco ASA for robust stateful inspection firewall services • Provides flexible access-control capabilities for over 100 predefined applications, services and protocols, with the ability to define custom applications and services • Includes numerous application-aware inspection engines that secure advanced networking protocols such as H.323 Version 4, Session Initiation Protocol (SIP), Cisco Skinny Client Control Protocol (SCCP), Real-Time Streaming Protocol (RTSP), Internet Locator Service (ILS), and more • Includes content filtering for Java and ActiveX applets
Easy VPN Server	• Provides remote access VPN concentrator services for a wide variety of Cisco software or hardware-based VPN clients • Pushes VPN policy dynamically to Cisco Easy VPN Remote-enabled solutions upon connection, ensuring the latest corporate security policies are enforced • Extends VPN reach into environments using Network Address Translation (NAT) or Port Address Translation (PAT), via support of Internet Engineering Task Force (IETF) UDP-based draft standard for NAT traversal

BOS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 041
Doc 3702

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

16.65C
L.

Table 1 Key Product Features and Benefits

Key Features	Benefit
Site-to-site VPN	• Supports IKE and IPsec VPN standards • Ensures data privacy/integrity and strong authentication to remote networks and remote users over the Internet • Supports 56-bit DES, 168-bit 3DES and up to 256-bit AES data encryption to ensure data privacy
Intrusion protection	• Provides protection from over 55 different types of popular network-based attacks ranging from malformed packet attacks to DoS attacks • Integrates with Cisco Network Intrusion Detection System (IDS) sensors for the ability to dynamically block/shun hostile network nodes via the firewall
AAA support	• Integrates with popular authentication, authorization, and accounting services via TACACS+ and RADIUS support • Provides tight integration with Cisco Secure Access Control Server (ACS)
X.509 certificate and CRL support	• Supports SCEP-based enrollment with leading X.509 solutions from Baltimore, Entrust, Microsoft, and VeriSign
Integration with leading third-party solutions	• Supports the broad range of Cisco AVVID (Architecture for Voice, Video and Integrated Data) partner solutions that provide URL filtering, content filtering, virus protection, scalable remote management, and more
Robust Network Services/Integration	
Virtual LAN (VLAN)-based virtual interfaces	• Provides increased flexibility when defining security policies and eases overall integration into switched network environments by supporting the creation of logical interfaces based on IEEE 802.1q VLAN tags, and the creation of security policies based on these virtual interfaces • Supports multiple virtual interfaces on a single physical interface through VLAN trunking • Supports multiple VLAN trunks per Cisco PIX Security Appliances • Supports up to 24 VLANs on Cisco PIX 535 Security Appliances
Open Shortest Path First (OSPF) dynamic routing	• Provides comprehensive OSPF dynamic routing services using technology based on world-renowned Cisco IOS Software • Offers improved network reliability through fast route convergence and secure, efficient route distribution • Delivers a secure routing solution in environments using NAT through tight integration with Cisco PIX Security Appliance NAT services • Supports MD5-based OSPF authentication, in addition to plaintext OSPF authentication, to prevent route spoofing and various routing-based DoS attacks • Provides route redistribution between OSPF processes, including OSPF, static, and connected routes • Supports load balancing across equal-cost multipath routes
DHCP server	• Provides DHCP Server services one or more interfaces for devices to obtain IP addresses dynamically • Includes extensions for support of Cisco IP Phones and Cisco SoftPhone IP telephony solutions
DHCP relay	• Forwards DHCP requests from internal devices to an administrator-specified DHCP server, enabling centralized distribution, tracking, and maintenance of IP addresses
NAT/PAT support	• Provides rich dynamic/static NAT and PAT capabilities

ECT nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 042
3702
Doc

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

16.649
L

Table 1 Key Product Features and Benefits

Key Features	Benefit
Rich Management Capabilities	
CiscoWorks VPN/ Security Management Solution (CiscoWorks VMS)	• Comprehensive management suite for large scale deployments • Integrates policy management, software maintenance, and security monitoring
PIX Device Manager (PDM)	• Intuitive, Web-based GUI enables simple, secure remote management of Cisco PIX Security Appliances • Provides wide range of informative, real-time, and historical reports which give critical insight into usage trends, performance baselines, and security events
Auto Update	• Provides "touchless" secure remote management of Cisco PIX Security Appliance configuration and software images via a unique push/pull management model • Next-generation secure XML/HTTPS management interface can be leveraged by Cisco and third-party management applications for remote Cisco PIX Security Appliance configuration management, inventory, software image management/deployment and monitoring • Integrates seamlessly with Management Center for Firewalls and Auto Update Server for robust, scalable remote management of up to 1000 Cisco PIX Security Appliances (per management server)
Cisco PIX CLI	• Allows customers to use existing PIX CLI knowledge for easy installation and management without additional training • Accessible through variety of methods including console port, Telnet and SSH
Command-level authorization	• Enables businesses to create up to 16 customizable administrative roles/profiles for accessing Cisco PIX Security Appliances (for example, monitoring only, read-only access to configuration, VPN administrator, firewall/NAT administrator, and so on) • Leverages either the internal administrator database or outside sources via TACACS+, such as Cisco Secure ACS
SNMP and syslog support	• Provide remote monitoring and logging capabilities, with integration into Cisco and third-party management applications
Highly Flexible Expansion Capabilities	
Fast Ethernet and Gigabit Ethernet expansion options	• Supports easy installation of additional network interfaces via four 66-Mhz/64-bit and 5 33-MHz/32-bit PCI expansion slots • Supports expansion cards including single-port Fast Ethernet card, 4-port Fast Ethernet card, and single-port Gigabit Ethernet card
Hardware VPN acceleration options	• Delivers high speed VPN services via support of VPN Accelerator Card (VAC) and VPN Accelerator Card+ (VAC+)

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 043
3702
Doc.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

16 648

License Options

The Cisco PIX 535 Security Appliance is available in three primary models that provide different levels of interface density, failover capabilities, and VPN throughput.

Restricted Software License

The Cisco PIX 535 "Restricted" (PIX 535-R) model provides an excellent value for organizations looking for robust Cisco PIX Security Appliance services with gigabit firewall throughput, high interface density, maximum investment protection, and moderate VPN throughput requirements. It includes 512 MB of RAM and support for up to eight 10/100 Fast Ethernet or eight Gigabit Ethernet interfaces.

Unrestricted Software License

The PIX 535 "Unrestricted" (PIX 535-UR) model extends the capabilities of the family with support for stateful failover, additional LAN interfaces, and increased VPN throughput via integrated hardware-based VPN acceleration. It includes an integrated VAC or VAC+ hardware VPN accelerator, 1 GB of RAM, and support for up to ten 10/100 Fast Ethernet or nine Gigabit Ethernet interfaces. The Cisco PIX 535-UR also adds the ability to share state information with a hot-standby Cisco PIX Security Appliance for resilient network protection.

Failover Software License

The Cisco PIX 535 "Failover" (PIX 535-FO) model is designed for use in conjunction with a PIX 535-UR, providing a cost-effective, high-availability solution. It operates in hot-standby mode acting as a complete redundant system that maintains current session state information. With the same hardware configuration as the Cisco PIX 535-UR, it delivers the ultimate in high availability for a fraction of the price.

Performance Summary

Cleartext throughput: 1.7 Gbps

Concurrent connections: 500,000

168-bit 3DES IPsec VPN throughput: Up to 440 Mbps with VAC+ or 100 Mbps with VAC

128-bit AES IPsec VPN throughput: Up to 535 Mbps with VAC+

256-bit AES IPsec VPN throughput: Up to 440 Mbps with VAC+

Simultaneous VPN tunnels: 2000

Technical Specifications

Processor: 1-GHz Intel Pentium III Processor

Random access memory: 512 MB or 1 GB of SDRAM

Flash memory: 16 MB

Cache: 256 KB level 2 at 1-GHz

System buses: Two 64-bit, 66 MHz PCI, one 32-bit, 33-MHz PCI

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 044
Doc. 3702

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

16.647
L

Environmental Operating Ranges

Operating

Temperature: –25° to 131°F (–5° to 55°C)

Relative Humidity: 5% to 95%, noncondensing

Altitude: 0 to 9843 ft (3000 m)

Shock: 1.14 m/sec (45 in./sec) 1/2 sine input

Vibration: 0.41 Grms2 (3–500 Hz) random input

Acoustic Noise: 65 dBa maximum

Nonoperating

Temperature: –13° to 158°F (–25° to 70°C)

Relative Humidity: 5% to 95%, noncondensing

Altitude: 0 to 15,000 ft (4570 m)

Shock: 30 G

Vibration: 0.41 Grms2 (3–500 Hz) random input

Power

Input (per power supply)

Range Line Voltage: 100V to 240V AC or 48V DC

Nominal Line Voltage: 100V to 240V AC or 48V DC

Current: 4–2 Amps

Frequency: 50 to 60 Hz, single phase

Power: 220W (dual hot swap power supply capable)

Output

Steady State: 135W

Maximum Peak: 220W

Maximum Heat Dissipation: 750 BTU/hr, full power usage (220W)

Physical Specifications

Dimensions and Weight Specifications

Form factor: 3 RU, standard 19-in. rack mountable

Dimensions (H x W x D): 5.25 x 17.5 x 18.25 in. (13.33 x 44.45 x 46.36 cm)

Weight (one power supply): 32 lb (14.5 kg)

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 045
Doc. 3702

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

16.646
C

Expansion

Four 64-bit/66-MHz PCI slots

Five 32-bit/33-MHz PCI slots

Six 168-pin DIMM RAM slots, supporting up to 1 GB PC133 DRAM

Interfaces

Console Port: RS-232 (RJ-45) 9600 baud

Failover Port: RS-232 (DB-15) 115 Kbps (Cisco specified cable required)

Two integrated 10/100 Fast Ethernet ports, auto-negotiate (half/full duplex), RJ-45

Regulatory and Standards Compliance

Safety

UL 1950, CSA C22.2 No. 950, EN 60950, IEC 60950, AS/NZS3260, TS001, IEC60825, EN 60825, 21CFR1040

Electro Magnetic Compatibility (EMC)

FCC Part 15 (CFR 47) Class A, ICES 003 Class A with UTP, EN55022 Class A with UTP, CISPR 22 Class A with UTP, AS/NZ 3548 Class A with UTP, VCCI Class A with UTP, EN55024, EN50082-1 (1997), CE marking, EN55022 Class B with FTP, Cispr 22 Class B with FTP, AS/NZ 3548 Class B with FTP, VCCI Class B with FTP

Product Ordering Information

PIX-535	PIX 535 chassis only
PIX-535-R-BUN	PIX 535 restricted bundle (chassis, restricted software, 2 10/100 ports, 512 MB RAM)
PIX-535-UR-BUN	PIX 535 unrestricted bundle (chassis, unrestricted software, 2 10/100 ports, 1 GB RAM, VAC or VAC+)
PIX-535-FO-BUN	PIX 535 failover bundle (chassis, failover software, 2 10/100 ports, 1 GB RAM, VAC or VAC+)
PIX-535-HW=	PIX 535 rack mount kit, console cable, failover serial cable
PIX-FO=	PIX failover serial cable
PIX-4FE	4-port 10/100 Fast Ethernet PCI expansion card
PIX-1FE	Single-port 10/100 Fast Ethernet PCI expansion card
PIX-1GE-66	Single-port Gigabit Ethernet 64-bit/66-MHz PCI expansion card, Multimode (SX) SC connector
PIX-VPN-ACCEL	3DES IPsec hardware VAC
PIX-VAC-PLUS	3DES/AES IPsec hardware VAC+
PIX-VPN-3DES	168-bit 3DES and up to 256-bit AES encryption software license

CPMI - CORREIOS
Fls Nº 046
Doc 3702

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

16.665

PIX-VPN-3DES=	168-bit 3DES and up to 256-bit AES encryption software license
PIX-VPN-DES	56-bit DES encryption software license
PIX-VPN-DES=	56-bit DES encryption software license

Support Services

Support services are available from Cisco and Cisco partners. Cisco SMARTnet service augments customer support resources, and provides anywhere, anytime access to technical resources (both online and by telephone), the ability to download updated system software, and hardware advance replacement.

Support Ordering Information

CON-SNT-PIX535	SMARTnet 8x5xNBD service for PIX 535 chassis only
CON-SNT-PIX535R	SMARTnet 8x5xNBD service for PIX 535-R bundle
CON-SNT-PIX535UR	SMARTnet 8x5xNBD service for PIX 535-UR bundle
CON-SNT-PIX535FO	SMARTnet 8x5xNBD service for PIX 535-FO bundle
CON-SNTE-PIX535	SMARTnet 8x5x4 service for PIX 535 chassis only
CON-SNTE-PIX535R	SMARTnet 8x5x4 service for PIX 535-R bundle
CON-SNTE-PIX535UR	SMARTnet 8x5x4 service for PIX 535-UR bundle
CON-SNTE-PIX535FO	SMARTnet 8x5x4 service for PIX 535-FO bundle
CON-SNTP-PIX535	SMARTnet 24x7x4 service for PIX 535 chassis only
CON-SNTP-PIX535R	SMARTnet 24x7x4 service for PIX 535-R bundle
CON-SNTP-PIX535UR	SMARTnet 24x7x4 service for PIX 535-UR bundle
CON-SNTP-PIX535FO	SMARTnet 24x7x4 service for PIX 535-FO bundle
CON-S2P-PIX535	SMARTnet 24x7x2 service for PIX 535-R chassis only
CON-S2P-PIX535R	SMARTnet 24x7x2 service for PIX 535-R bundle
CON-S2P-PIX535UR	SMARTnet 24x7x2 service for PIX 535-UR bundle
CON-S2P-PIX535FO	SMARTnet 24x7x2 service for PIX 535-FO bundle
CON-OS-PIX535	SMARTnet On-Site 8x5xNBD service for PIX 535 chassis only
CON-OS-PIX535R	SMARTnet On-Site 8x5xNBD service for PIX 535-R bundle
CON-OS-PIX535UR	SMARTnet On-Site 8x5xNBD service for PIX 535-UR bundle
CON-OS-PIX535FO	SMARTnet On-Site 8x5xNBD service for PIX 535-FO bundle
CON-OSE-PIX535	SMARTnet On-Site 8x5x4 service for PIX 535 chassis only
CON-OSE-PIX535R	SMARTnet On-Site 8x5x4 service for PIX 535-R bundle
CON-OSE-PIX535UR	SMARTnet On-Site 8x5x4 service for PIX 535-UR bundle

IRQS nº 05/2005 - CN
CPMI - CORREIOS
Fls Nº 047
3702

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

CON-OSE-PIX535FO	SMARTnet On-Site 8x5x4 service for PIX 535-FO bundle
CON-OSP-PIX535	SMARTnet On-Site 24x7x4 service for PIX 535 chassis only
CON-OSP-PIX535R	SMARTnet On-Site 24x7x4 service for PIX 535-R bundle
CON-OSP-PIX535UR	SMARTnet On-Site 24x7x4 service for PIX 535-UR bundle
CON-OSP-PIX535FO	SMARTnet On-Site 24x7x4 service for PIX 535-FO bundle

16.144
2

Additional Information

For more information, please visit the following links:

Cisco PIX Security Appliance Series:

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

Cisco PIX Device Manager:

http://www.cisco.com/warp/public/cc/pd/fw/sqfw500/prodlit/pixd3_ds.pdf

Cisco Secure ACS:

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

CiscoWorks VMS, Management Center for Firewalls, Auto Update Server Software and Security Monitor:

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

SAFE Blueprint from Cisco:

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

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the **Cisco Web site at www.cisco.com/go/offices**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. CCIP, CCSP, the Cisco Arrow logo, the Cisco *Powered* Network mark, Cisco Unity, Follow Me Browsing, FormShare, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, Fast Step, GigaStack, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, MGX, MICA, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, ScriptShare, SlideCast, SMARTnet, StrataView Plus, Stratm, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0304R)

RD/LW3946 04/03

RQS nº 03/2005 - CN
CPMI - CORREIOS
Nº 3702 Doc 048

Segurança Tipo 1 doc 2

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 049
3702
Doc.

Cisco Systems

16-642

Data Sheet

Cisco **PIX** Firewall Version 6.2

The world-leading Cisco PIX® Firewall Series of purpose-built security appliances provides robust, enterprise-class security services, including stateful inspection firewalling, virtual private networking (VPN), intrusion protection, and much more—in cost-effective, easy-to-deploy solutions. Ranging from compact, plug-and-play desktop firewalls for small/home offices to carrier-class gigabit firewalls for the most demanding enterprise and service-provider environments, Cisco PIX Firewalls provide robust security, performance, and reliability for network environments of all sizes.

Advanced Firewall Technologies Provide Enterprise-Class Network Security

Cisco PIX Firewalls deliver a broad range of advanced firewall services that protect enterprise networks from the threats lurking on the Internet and in today's network environments. The state-of-the-art Cisco Adaptive Security Algorithm (ASA) provides rich stateful inspection firewall services, tracking the state of all authorized network communications and preventing unauthorized network access. Cisco PIX Firewalls deliver an additional layer of security through intelligent, "application-aware" security services that examine packet streams at Layers 4 through 7, using inspection engines specialized for many of today's popular applications. Administrators can easily create custom security policies that will be enforced on network traffic traversing the firewall by leveraging more than 100 pre-defined applications, services, and protocols within Cisco PIX Firewalls, and the flexible access control capabilities that Cisco PIX Firewalls provide. Access to network resources can also be strongly authenticated via the Cisco PIX Firewall's seamless integration with enterprise databases, either directly using TACACS+/RADIUS or indirectly via Cisco Secure Access Control Server (ACS). In addition to these services, Cisco PIX Firewalls provide extensive logging, URL filtering, content filtering, and more in concert with Cisco AVVID (Architecture for Voice, Video and Integrated Data) partner solutions.

Market-Leading Voice-over-IP Security Services Protect Next-Generation Converged Networks

Cisco PIX Firewalls continue to provide market-leading protection for numerous voice-over-IP (VoIP) standards and other multimedia standards, including H.323, Session Initiation Protocol (SIP), Skinny, Real-Time Transport Protocol (RTP), Real-Time Streaming Protocol (RTSP), and Real-Time Transport Control Protocol (RTCP). This allows businesses to securely take advantage of the many benefits that converged data and voice networks provide, such as significant total cost of ownership (TCO) savings and the competitive advantages and improved productivity gained through the power of fully integrated voice, video, and data networks. By combining VPN with the rich

Fls. Nº 050
Nº Dec 3702

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

16.641

stateful inspection firewall services that Cisco PIX Firewalls provide for these converged networking standards, businesses can easily extend voice and multimedia services to remote/satellite offices for additional bandwidth and cost savings.

Site-to-Site VPNs Extend Networks Economically to Remote Sites and Business Partners

Using the standards-based site-to-site VPN capabilities within Cisco PIX Firewalls, businesses can securely extend their network across low-cost Internet connections to business partners and remote/satellite offices worldwide. Built upon the Internet Key Exchange (IKE) and IP Security (IPSec) VPN standards, Cisco PIX Firewalls encrypt data using 56-bit Data Encryption Standard (DES) or advanced 168-bit Triple DES (3DES) encryption, ensuring that malicious individuals cannot see sensitive business data as it safely travels across the Internet. Cisco PIX Firewalls can also participate in X.509-based Public Key Infrastructures (PKI) and provide easy, automated certificate enrollment by taking advantage of the Simplified Certificate Enrollment Protocol (SCEP)—another Internet standard Cisco helped to pioneer. Certain Cisco PIX Firewall models also provide integrated hardware VPN acceleration, providing up to 100 Mbps of 3DES throughput and support for up to 2000 IKE security associations.

Easy VPN Enables Highly Scalable, Easy-to-Manage VPN Deployments

The innovative Easy VPN capabilities found in Cisco PIX Firewalls and other Cisco solutions—such as Cisco IOS® Software-based routers and Cisco VPN 3000 Series Concentrators—deliver a uniquely scalable, cost-effective, and easy-to-manage remote-access VPN architecture. Built upon the foundation of dynamic policy distribution and effortless provisioning, Easy VPN eliminates the operational costs associated with maintaining remote-device configurations typically required by traditional VPN solutions. Easy VPN enables Cisco customers to enjoy the numerous benefits that VPNs provide—increased employee productivity by taking advantage of high-speed broadband connectivity, and significantly reduced operational costs by eliminating expenses associated with legacy dialup architectures—without the problems commonly found with other remote-access VPN solutions.

Cisco PIX Firewalls provide robust, remote-access VPN concentrator services that enable enterprises to securely extend their network to traveling employees, teleworkers, and remote offices for "anytime, anywhere access" to vital corporate network resources. Acting as an Easy VPN Server, Cisco PIX Firewalls support the wide range of Cisco software- and hardware-based Easy VPN Remote products. By dynamically pushing VPN security policies to Easy VPN-enabled users as they connect, Cisco PIX Firewalls ensure that the latest VPN security policy is consistently enforced for all remote-access users.

Certain models of Cisco PIX Firewalls can also act as "hardware VPN clients" using the new Easy VPN Remote features in Cisco PIX Firewall OS, transparently providing secure access to a corporate network for all devices protected by a Cisco PIX Firewall in a remote network. This dramatically simplifies the initial deployment and ongoing management of VPNs deployed to remote offices and teleworker environments by eliminating the need to install and maintain VPN client software on the individual devices protected by a remote Cisco PIX Firewall. Advanced client-side resiliency features ensure maximum VPN uptime by providing automatic failover to backup Easy VPN Servers in the event of a network or service failure.

RQS nº 03/2005 - CN
CPMI - CORREIOS
051
Fls Nº
3702
Doc

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Integrated Intrusion Protection Guards from Popular Internet Threats

The integrated intrusion-protection capabilities in Cisco PIX Firewalls protect today's networks from many popular forms of attacks, including Denial-of-Service (DoS) attacks and malformed packet attacks. Using a wealth of advanced intrusion-protection features, including DNSGuard, FloodGuard, FragGuard, MailGuard, and TCP intercept, in addition to looking for more than 55 different attack "signatures," Cisco PIX Firewalls keep a vigilant watch for attacks, can optionally block them, and can notify administrators about them in real time. Additionally, Cisco PIX Firewalls support virtual packet reassembly, searching for attacks that are hidden over a series of fragmented packets. Strong integration with Cisco Intrusion Detection Systems (IDS) sensors enables Cisco PIX Firewalls to automatically shun (block) network nodes identified as being hostile by Cisco IDS sensors.

Enterprise-Class Resiliency Provides Maximum Business Uptime

Cisco PIX Firewalls provide award-winning stateful failover capabilities (on select models) that ensure resilient network protection for enterprise network environments. Employing a cost-effective, active-standby high-availability architecture, Cisco PIX Firewalls configured as a failover pair continuously synchronize connection state information and device configuration data between one another. Performing this synchronization over a high-speed LAN connection provides the added benefit of being able to geographically separate failover pair members, thus providing a further layer of protection. In the rare event of a system or network failure, network sessions are automatically transitioned between firewalls seamlessly, and with complete transparency to network users.

Robust Remote-Management Solutions Lower Total Cost of Ownership

Cisco PIX Firewalls deliver a wealth of remote-management methods for configuration, monitoring, and troubleshooting. Management solutions range from an integrated, Web-based management application to highly scalable multi-firewall management tools to support for remote-monitoring protocols such as Simple Network Management Protocol (SNMP) and syslog. Cisco PIX Firewalls additionally provide up to 16 levels of customizable administrative roles, so that enterprises can grant administrators and operations personnel the appropriate level of permissions they need for each firewall they manage (for example, monitoring only, read-only access to the configuration, VPN configuration only, firewall configuration only, etc.). Cisco PIX Firewalls now also support Auto Update, a revolutionary secure remote-management capability that ensures firewalls configurations and software images are kept up-to-date.

Cisco PIX Device Manager (PDM), integrated with Cisco PIX Firewalls, provides administrators an intuitive, Web-based management interface for remotely configuring and monitoring a single Cisco PIX Firewall, without requiring any software (other than a standard Web browser) to be installed on an administrator's computer. Administrators can also remotely configure, monitor, and troubleshoot Cisco PIX Firewalls using a command-line interface (CLI) through various methods, including Telnet and Secure Shell (SSH) Protocol, or out-of-band via a console port.

Administrators can easily manage a large number of remote Cisco PIX Firewalls using either the new combination of the CiscoWorks Management Center for Cisco PIX Firewalls and Auto Update Server, or Cisco Secure Policy Manager (CSPM)—all available within the Cisco VPN Security Management Solution (VMS) network management suite. The CiscoWorks Management Center for Cisco PIX Firewalls is a highly scalable, next-generation, three-tier management solution for Cisco PIX Firewalls that includes features such as hierarchical grouping of managed firewalls, "Smart Rules" configuration inheritance, customizable administrative roles and access privileges,

Fls Nº 052
Doc. 3702

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

workflow-based enterprise change management, comprehensive support for Cisco PIX Firewall's new Auto Update capabilities, and support for dynamically addressed firewalls. Cisco Secure Policy Manager Release 3.0 is a policy-based centralized management solution for Cisco PIX Firewalls that includes a task-based interface, an interactive network topology map, policy wizards, and policy import capabilities. Additional integrated event management and inventory solutions are also available as part of the Cisco VMS network management suite.

New Features Found in Cisco PIX Firewall Release 6.2

Cisco PIX Firewall Release 6.2 provides a wealth of new innovative features, which are detailed below:

Table 1 New Features and Benefits

New Features	Benefits
Enterprise-Class Security	
LAN-based failover	• Extends failover functionality and enables geographic separation of Cisco PIX Firewalls in a failover pair by allowing failover information to be shared over a dedicated LAN connection (instead of a serial cable) between failover pairs
Bidirectional Network Address Translation (NAT)	• Enhances rich NAT functionality in Cisco PIX Firewalls to support environments with overlapping private address ranges
Turbo access control lists (ACLs)	• Provides significantly enhanced performance and deterministic search times for ACL processing; especially useful in environments where extensive ACLs are deployed
N2H2 URL filtering	• Integrates with N2H2 Sentian™ products—leading Internet filtering solutions—to provide robust employee Web access control and monitoring
Enhanced small-packet performance	• Delivers up to 48 percent more firewall performance for 64- to 512-byte packets than previous Cisco PIX Firewall OS releases, due to further optimization of small-packet processing
Management	
Auto Update	• Provides highly scalable, secure remote management of PIX Firewalls with a unique push/pull management model • Next-generation secure XML/HTTPS interface can be leveraged by Cisco and third-party management applications for remote firewall configuration management, inventory, software image management/deployment and monitoring • Supports dynamically addressed firewalls in addition to firewalls with static IP addresses • Integrates seamlessly with CiscoWorks Management Center for Cisco PIX Firewalls and Auto Update Server for robust, scalable remote management of up to 1000 PIX Firewalls
Object grouping	• Enables administrators to group network objects (such as devices, networks, and services) into logical groups to greatly simplify access control rule definition and maintenance

RQS nº 03/2005 - CN
CPMI - CORREIOS
053
Fls Nº
Doc. 3702

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Table 1 New Features and Benefits

New Features	Benefits
Command-level authorization	• Enables businesses to create up to 16 customizable administrative roles and profiles for accessing Cisco PIX Firewalls (for example, monitoring only, read-only access to configuration, VPN administrator, firewall administrator, etc.) • Uses either the internal Cisco PIX Firewall administrator database or outside sources via TACACS+, such as Cisco Secure ACS
Dynamic ACLs via Cisco Secure ACS	• Supports dynamic downloading and enforcement of ACLs on a per-user basis, upon user authentication with the firewall
Network Time Protocol (NTP) v3 client	• Provides convenient method for synchronizing the clock on Cisco PIX Firewalls with other devices on a network
CPU monitoring via SNMP v2	• Extends SNMP-based remote firewall health monitoring to include the ability to monitor CPU utilization
Software and configuration updates via HTTP and HTTPS	• Adds support for downloading Cisco PIX Firewall OS and Cisco PIX Device Manager software, as well as configuration updates via HTTP or HTTPS • Provides ability to deliver configuration and software updates over authenticated, encrypted network connection
HTTPS-based CLI access	• Delivers flexible, secure interface for interactive and easily scriptable access to Cisco PIX Firewall CLI via standard HTTPS requests
Packet capture	• Gives administrators new, powerful troubleshooting capabilities by providing robust packet-capturing facilities on each interface of the firewall • Supports several methods of accessing captured packets, including via the console, secure Web access or a file exported to a Trivial File Transfer Protocol (TFTP) server
Small Office/Home Office	
Easy VPN Remote (hardware VPN client)	• Enables dramatically simplified VPN rollouts to small office, teleworker, and remote/branch-office environments, allowing Cisco PIX 501, 506, and 506E Firewalls to act as hardware VPN clients, and eliminating the provisioning complexities of traditional site-to-site VPN deployments • Downloads VPN policy dynamically from an Easy VPN Server upon connection, ensuring the latest corporate security policies are enforced • Provides robust client-side VPN resiliency with support for up to ten Easy VPN servers with automatic failover, in addition to Dead Peer Detection (DPD) support • Enables the network behind a Cisco PIX Firewall to appear as a single user to the VPN headend when using Easy VPN Remote Client Mode • Provides site-to-site VPN-like functionality without requiring any additional provisioning when using Easy VPN Remote Network Extension Mode • Supports both split and non-split tunneling environments • Provides intelligent, transparent Domain Name System (DNS) proxy capabilities for access to both corporate and public DNS servers
PPP over Ethernet (PPPoE) support	• Ensures compatibility with networks that require PPPoE support, such as xDSL and cable modem broadband environments

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 054
Doc 3702

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

16.654

Table 1 New Features and Benefits

New Features	Benefits
Voice-over-IP (VoIP)/Multimedia	
Multicast support	• Supports wide range of multicast applications by introducing support for Internet Group Management Protocol (IGMP) v2 and stub multicast routing, including NAT and Port Address Translation (PAT) and the ability to build access control lists for multicast traffic
PAT for H.323 and SIP	• Extends market-leading VoIP support and enables SIP and H.323 to work in PAT environments, typically found in home offices and remote offices
DHCP server support for Cisco IP phones	• Simplifies remote Cisco IP Phone deployments by providing Cisco CallManager contact information via DHCP options 66 and 150 to Cisco IP phones for automated bootstrapping
Internet Locator Service (ILS) Fixup	• Adds support for ILS, a popular directory service used by applications such as Microsoft NetMeeting, SiteServer and Active Directory, for registration and location of network entities/endpoints

Technical Specifications

VPN Client Compatibility

Cisco PIX Firewalls support a wide variety of software- and hardware-based VPN clients, including:

Software IPSec VPN clients	Cisco Secure VPN Client Release 1.1 Cisco VPN 3000 Concentrator Client, Release 2.5 and higher Cisco VPN Client for Microsoft Windows, Release 3.0 and higher Cisco VPN Client for Linux, Release 3.5 and higher Cisco VPN Client for Solaris, Release 3.5 and higher Cisco VPN Client for Mac OS X, Release 3.5 and higher
Hardware IPSec VPN clients	Cisco VPN 3002 Hardware Client, Release 3.0 and higher Cisco IOS Software Easy VPN Remote, Release 12.2(8)YJ Cisco PIX Firewall Easy VPN Remote, Release 6.2 and higher
Layer 2 Tunneling Protocol (L2TP)/IPSec VPN clients	Microsoft Windows 2000
Point-to-Point Tunneling Protocol (PPTP) VPN clients	Microsoft Windows 95 Microsoft Windows 98 Microsoft Windows NT 4.0 Microsoft Windows 2000

RQS nº 03/2005 - CN
CPMI CORREIOS
Fls Nº 055
Doc 3702

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Easy VPN Server Compatibility

Cisco PIX Firewalls can now act as hardware-based VPN clients, taking advantage of the new Easy VPN Remote capabilities in Cisco PIX Firewall OS. The following Easy VPN Server platforms are supported for this deployment scenario:

Cisco IOS Routers	Release 12.2(8)T and higher
Cisco PIX Firewalls	Release 6.0(1) and higher
Cisco VPN 3000 Concentrators	Release 3.1 and higher

Cisco Site-to-Site VPN Compatibility

In addition to supporting interoperability with many third-party VPN products, Cisco PIX Firewalls interoperate with the following Cisco VPN products for site-to-site VPN connectivity:

Cisco IOS Routers	Release 12.1(6)T and higher
Cisco PIX Firewalls	Release 5.1(1) and higher
Cisco VPN 3000 Concentrators	Release 2.5.2 and higher

Cryptographic Standards Supported

Cisco PIX Firewalls support numerous cryptographic standards and related third-party products and services, including the following:

Asymmetric (public key) encryption algorithms	RSA (Rivest, Shamir, Adelman) public/private key pairs, 512 bits to 2048 bits
Symmetric encryption algorithms	DES: 56 bits 3DES: 168 bits RC4: 40, 56, 64, and 128 bits
Perfect Forward Secrecy (Diffie-Hellman key negotiation)	Group 1: 768-bits Group 2: 1024-bits
Hash algorithms	MD5: 128-bits SHA-1: 160-bits
X.509 certificate authorities	Baltimore UniCERT Entrust Authority Microsoft Windows 2000 Certificate Services VeriSign OnSite
X.509 certificate enrollment protocols	SCEP

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 056
Doc. 3702

16.635
L

System Requirements

Platforms supported	Cisco PIX 501 Firewall Cisco PIX 506 Firewall Cisco PIX 506E Firewall Cisco PIX 515 Firewall Cisco PIX 515E Firewall Cisco PIX 520 Firewall Cisco PIX 525 Firewall Cisco PIX 535 Firewall
RAM, minimum	32 MB, except Cisco PIX 501 which requires 16 MB
Flash memory, minimum	16 MB, except Cisco PIX 501/506/506E which require 8 MB
Expansion cards supported	Single-port 10/100 Fast Ethernet card Four-port 10/100 Fast Ethernet card Single-port Gigabit Ethernet, multimode (SX) SC, card VPN Acceleration Card (VAC)

Product Ordering Information

PIX-SW-UPGRADE=	Cisco PIX software one-time upgrade for customers without a current SMARTnet™ support contract

Support Services

Support services are available from Cisco partners as well as from Cisco. The Cisco SMARTnet service augments customer support resources. It provides 24x7x 365 access to technical resources (both online and via telephone), the ability to download updated system software, and hardware advance replacement.

RQS nº 03/2005 - CN
CPMI - CORREIOS
0057
Doc. 3702

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Additional Information

For more information, please visit the following links:

Cisco PIX Firewall:

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

Cisco PIX Device Manager:

http://www.cisco.com/warp/public/cc/pd/fw/sqfw500/prodlit/pixdm_ds.pdf

Cisco Secure ACS:

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

Cisco Secure Policy Manager:

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

Cisco VPN Security Management Solution (VMS), CiscoWorks Management Center for Cisco PIX Firewalls and Auto Update Server:

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

Cisco SAFE Blueprint:

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

To download the latest Cisco PIX Firewall OS and Cisco PIX Device Manager software (with a valid Cisco.com login), visit:

http://www.cisco.com/cgi-bin/tablebuild.pl/pix

ROS nº 05/2005 - CN
CPMI - CORREIOS
0058
Doc. 3702

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

16.633

CISCO SYSTEMS

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 317 7777
Fax: +65 317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the

Cisco Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland
Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland
Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

All contents are Copyright © 1992–2002, Cisco Systems, Inc. All rights reserved. Cisco, Cisco IOS, Cisco Systems, the Cisco Systems logo, PIX, and SMARTnet are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0208R)

BD/LW3946 12/02

ROS 03/2005
Fls Nº 059
Doc 3702

16.632

Segurança Tipo 1 doc 3

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 060
Nº 3702
Doc

Cisco Systems

16.631

Data Sheet

CiscoWorks **Management Center** for Firewalls, Version 1.2

Introduction

The CiscoWorks Management Center for Firewalls and Auto Update Server Software are the functional components, within the CiscoWorks VPN/ Security Solution (VMS), that provide unprecedented manageability for the Cisco Firewall product line. The Management Center for Firewalls features the "look and feel" of the Cisco PIX Device Manager (PDM) but offers centralized management scalability of up to 1,000 Cisco Firewalls.

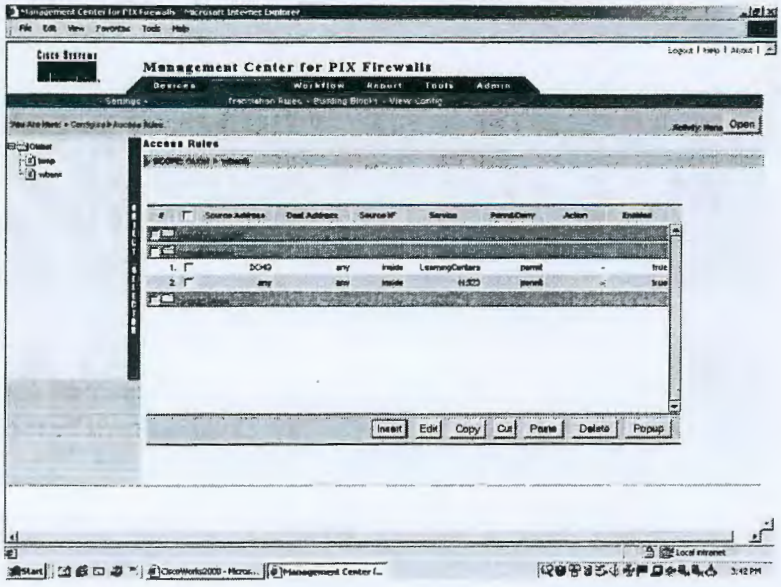
This management center component of CiscoWorks VMS, is an integral part of the SAFE blueprint, and combines Web-based tools for configuring, monitoring, and troubleshooting the following:

- VPNs
- Firewalls
- Network intrusion detection systems (IDS)
- Host-based IDS

CiscoWorks VMS addresses the needs of both small- and large-scale VPN and security deployments, and enables organizations to protect productivity gains and reduce operating costs.

Cisco protects the productivity of your enterprise with an integrated security management solution. Unlike pointer security products from multiple vendors that leave vulnerable gaps with different GUIs, CiscoWorks VMS provides a comprehensive solution that ties separate security and VPN technologies into a single, whole secure network.

Figure 1
CiscoWorks Management Center for PIX Firewalls



New Features

Management Center for Firewalls version 1.2 is the follow-on version of the Management Center for PIX Firewalls version 1.1. This module has been renamed to reflect the additional support for the Firwall Services Module (FWSM). Managment Center for Firewalls version 1.2 adds support for the following new features:

- Cisco PIX 6.3
- Single ckick to deploy configurations (No activity and job management)
- Object groups
- Dual NAT

RQS nº 03/2005 - CN
CPMI - CORREIOS
061
Fls Nº
Doc 3702

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

16.63
L

- Solaris
- VLANs
- Syslog per access-list
- Single Auto Update Server (AUS) set up for an entire group of Cisco PIX
- NAT 0 ACL
- Cut and paste of building blocks

Intended Use

The Management Center for Firewalls provides SAFE coverage and centralized management of access rules, Network Address Translation (NAT), intrusion detection, and VPN on Cisco Firewalls. It supports centralized management of virtually any Cisco Firewall security network including remote access; demilitarized zone (DMZ); small office/home office (SOHO); voice, storage, and wireless networks; Internet security; and management security provider scenarios.

Features and Benefits

The Management Center for Firewalls provides unique and robust scalability with these industry-first features:

- Smart Rules hierarchy and inheritance
- User-defined device and customer groups including nesting
- Global role-based access (RBAC) with administrative privileges per device and customer groups with CiscoWorks products and Cisco Secure Access Control Server (ACS)
- Mandatory and default device settings inheritance
- Workflow deployment to device, directory or Auto Update Server
- Look and feel of Cisco PIX Device Manager (PDM) but with scalability to 1,000 Cisco Firewalls
- Web GUI
- Integration of market-leading management features from other CiscoWorks products
- Complete SAFE coverage for centralized management of Cisco PIX and Firewall Services Module including access control, virtual private networks (VPN), intrusion detection systems (IDS), and authentication, authorization, and accounting (AAA)
- Reduction in total configuration time
- Reduction in manual configuration errors
- Automatic update of remote firewall configurations and operating systems
- Automatic and periodic verification of remote firewall configurations

Smart Rules

Smart Rules is an innovate feature that allows common information, including access rules and settings, to be inherited for all firewalls in a device or customer group. Smart Rules allows a user to define common rules once, reducing configuration time and resulting in fewer administrative errors. Furthermore, Smart Rules offers higher device scalability. A user can configure a common rule (such as allowing all HTTP traffic) once, and then apply this global rule to all firewalls. Smart Rules can also be defined on a device or customer group.

RQS nº 03/2005 - CN
CPMI CORREIOS
0062
3702
Doc

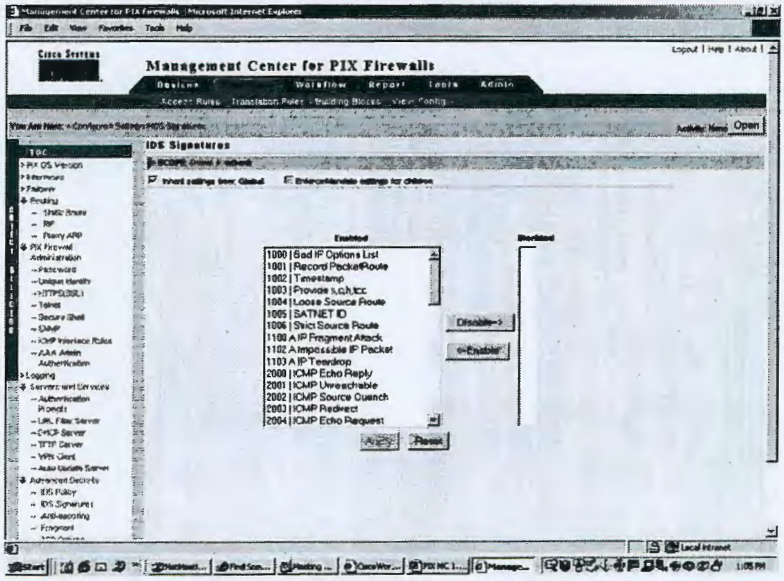
All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

16629

Granular Administrative Privileges for Customer/Device Groups

The CiscoWorks Management Center for Firewalls allows devices to be separated by geography, customer, device type, or any other mechanism the user wants. The Management Center for Firewalls supports multiple administrators. Administrative privileges can be defined on a device or customer group. Basic administrative privileges include the five roles defined in the CiscoWorks desktop. Administrative privileges can also be defined within Cisco Secure Access Control Server (ACS) to allow very granular administrative privileges so that a customer can view their own firewall configurations but not those of another customer.

Global/Group Device Settings



The CiscoWorks Management Center for Firewalls supports an extensive list of device settings including Failover, Routing, SNMP, ICMP, AAA, DHCP, TFTP, VPN Client, IDS, and IP Anti-spoofing. All of these settings can be defined globally and inherited by all applicable firewalls. Any of these settings can also be defined on a device or customer group for unprecedented scalability. Powerful feature settings, including IDS signatures, can now be defined for all applicable firewalls with just a few mouse clicks.

Benefits of Cisco PDM, Cisco.com, and CiscoWorks

Other competitive products simply distribute all configuration changes to all devices. Like other CiscoWorks products, the Management Center for Firewalls supports flexible configuration deployment to either a device, file directory, or Auto Update Server. The Management Center for Firewalls features the "look and feel" of the single-firewall Cisco PDM. It also offers the usability of Cisco PDM combined with the scalability of centralized management for up to 1,000 Cisco Firewalls.

RQS nº 03/2005 - CN
CPMI CORREIOS
Fls Nº 063
Doc: 3702

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

The Management Center for Firewalls incorporates an easy-to-use Web GUI and secure configuration and distribution with Secure Socket Layer (SSL) and secure digital certificates. The Management Center for Firewalls also supports key scalability features from CiscoWorks LAN Management Solution (LMS) and Routed WAN Management Solution (RWAN) that facilitate LAN and WAN deployments of more than 20,000 devices. Key CiscoWorks features supported by the Management Center for Firewalls include an approval flow, device list from CiscoWorks Resource Manager Essentials (RME), rollback, and activity and job management.

Device Support

- The Management Center for Firewalls supports the following Cisco Firewall platforms: Cisco PIX 501, 506, 506E, 515, 515E, 525, 535; and the Cisco Firewall Services Module (FWSM)
- The Management Center for Firewalls supports versions 6.0, 6.1, and 6.2 of the Cisco PIX Operating System, and FWSM versions 1.1(x).

The Management Center for Firewalls will import the configuration of existing Cisco Firewall version 6.0 deployments. The Management Center for Firewalls also features an outbound conduit to an access list conversion tool that enables conversion of existing access configurations to access lists.

System Requirements

The Management Center server software is currently supported on Windows 2000 only. For comprehensive hardware and operating requirements, see the CiscoWorks VMS Overview at http://www.cisco.com/go/vms.

Ordering Information

The Management Center for Firewalls is available exclusively as part of CiscoWorks VPN/Security Management Solution (VMS). For details on ordering, refer to the CiscoWorks VMS Product Bulletin at http://www.cisco.com/go/vms.

For More Information

Please reference http://www.cisco.com/go/vms for more information about CiscoWorks VMS, or email ciscoworks@cisco.com.

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 317 7777
Fax: +65 317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the

Cisco Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland
Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland
Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

All contents are Copyright © 1992–2002, Cisco Systems, Inc. All rights reserved. Cisco, Cisco IOS, Cisco Systems, the Cisco Systems logo, and PIX are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries. All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0208R)

202970/ETMG 9/02

Fls Nº 064
Nº Doc. 3702

Segurança Tipo 1 doc 4

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0365
3702
Doc.

Cisco Systems

16.646

Data Sheet

Monitoring Center for **Security**, Version 1.2

Introduction

The Monitoring Center for Security is a tool to capture, store, view, correlate and report on events from:

- Cisco Network IDS
- Cisco Switch IDS
- Cisco IDS Network Module for routers
- Management Center for Cisco Security Agents
- Cisco PIX Firewalls
- Cisco Firewall Services Modules
- Cisco IOS Routers

The Monitoring Center for Security will increase the accuracy of threat detection and lower the operational costs for event monitoring, and will increase your administrator's productivity. The software delivers event correlation to identify attacks that are not easily recognizable from a single event, a flexible notification scheme and automated responses to critical events. By taking advantage of user-defined event correlation rules, the operator can:

- Monitor attacks against specific, high visibility hosts (for example, a web server).
- Monitor the traffic for patterns of attacks
- Correlate IDS information from multiple security devices (e.g., firewalls, network IDS, host IDS)
- Receive early notification of emerging threats
- Trigger an automated response, as a corrective action against an attack
- Reduce the number of false positives

The Monitoring Center for Security is a component of the CiscoWorks VPN/ Security Management Solution (VMS). VMS is an integral part of the SAFE blueprint and combines web-based tools for configuring, monitoring and troubleshooting:

- Virtual Private Networks (VPN)
- Firewalls
- Network Intrusion Detection Systems (IDS)
- Host-based IDS

CiscoWorks VMS addresses the needs of both small- and large-scale VPN and security deployments by protecting productivity gains and reducing operating costs fororganizations.

Intended Use

The Monitoring Center for Security will benefit those organizations experiencing information overload, resulting from:

- Too many security consoles
- Too many security events to monitor
- Difficulty in viewing the big security picture

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 066
Doc. 3702

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

16.625

New Features

The Monitoring Center for Security includes support for additional event types. The operator can now monitor events from the Management Center for Cisco Security Agents, version 4.0 and also monitor events from the Cisco Intrusion Detection System (IDS) software version 4.1. The Management Center for Cisco Security Agents 4.0 will receive events from agents and then forward these events to the Monitoring Center for Security version 1.2. As a result, the Monitoring Center for Security provides a broad, unified view of security messages.

Support for IDS 4.1 allows the operator to monitor network IDS sensors that communicate using the Remote Data Exchange Protocol (RDEP). With the RDEP protocol the operator can subscribe to specific IDS event types and better control which events are received.

Enhancements in the event viewer include performance improvements for event deletions and an addition of a new interface graphing capability. The user can also preserve their preferred column ordering in the event viewer.

Enhancements for reporting include the ability to save generated reports to the database and to a file for more flexible storage options. Furthermore, new summary information has been added to reports to help with analysis. Cisco has added more reports for firewalls and Cisco Security Agents.

Enhancements in the notification system include an increase in the number of active events rules from 5 to 10. Event rules help identify critical events and automate a response so that the operator does not need to monitor a screen over long periods. The operator can also import Cisco IDS Sensor configurations from a remote Management Center for IDS Sensors server to save time.

The Monitoring Center for Security, version 1.1 is now supported on Solaris 8. This software does not have some of the features that are available in the Monitoring Center for Security version 1.2, which is available only on Windows 2000 currently. Examples of features not supported on the Solaris platform include:

- No support for events from the Management Center for Cisco Security Agents, version 4.0
- No support for events from the Cisco IDS Network Module for routers
- No support for events form IDS version 4.1 (however, IDS 4.0 is supported)
- No additional reports for firewall and Cisco Security Agents
- No support for saving the preferences of column ordering in the event viewer

Features and Benefits

Comprehensive reporting options for finding information

- Web-based wizard for creating flexible security reports
- On-demand and scheduled reports
- Reports by top incidents, by IP address, by time, by signature, by event, etc.
- Send notifications of reports by email

Web-based event viewer with features to easily locate attacks

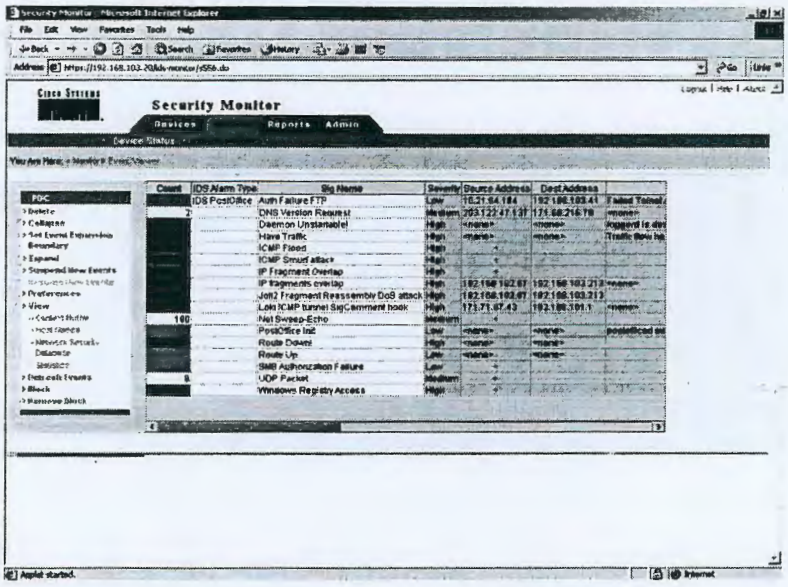
- Easily "slice and dice" data by moving event field columns and sifting through thousands of events in seconds. The Event Viewer can read both real-time and historical events from the database.

RQS nº 03/2005 - CN
CPMI - CORREIOS
FLS Nº 067
3702
Doc.

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

16.624

Figure 1
Design based on award winning event viewer.



Perform event correlation to detect an emerging threat

- Create user-defined rules for establishing relationships between events (correlate by type of event, by time, across sensors, across source addresses, etc.). This helps to identify attacks, which may not be apparent from a single event.
- The user can define thresholds and time periods when a rule should be triggered
- If a rule is triggered, the user can be notified via email and fine-tune what information from the suspicious packet is forwarded with the email. Alternatively, the user can automatically execute a script as a corrective response.

Database Management

- The Monitoring Center for Security provides a relational database that is used for storage of event data. Various database management functions such as archiving and purging can easily be performed without database administration skills within the Monitoring Center for Security using the web interface.

RQS nº 03/2005 CN
CPMI CORREIOS
Fls Nº 068
Nº Doc. 3702

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Devices Supported for Monitoring

Platform	Software Version Supported
Cisco Network IDS sensors	IDS 3.0, 3.1, 4.0 and 4.1
Cisco Switch IDS (IDSM) sensors	IDSM 3.0(5), 4.0 and 4.1
Cisco IDS Network Module for Cisco Routers	IDS 4.1
Cisco PIX Firewall	Cisco PIX Firewall OS 6.0(x), 6.1(x), 6.2(x), 6.3.1
Cisco Firewall Services Modules	1.1
Cisco IOS Router for IDS messages (with IOS Firewall toolkit)	12.2x mainline and later
Cisco Security Agents (forwarded by Management Center for Cisco Security Agents, version 4.0)	4.0
Cisco IDS Host Console (forwarded by the Cisco IDS Host Console, version 2.5)	2.5

System Requirements

For comprehensive hardware and operating requirements see the VMS Overview.

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

Ordering Information

The Monitoring Center for Security is a featured component of CiscoWorks VMS. For ordering details click on the VMS Product Bulletin found at:

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

For More Information

Please reference http://www.cisco.com/go/vms or email ciscoworks@cisco.com

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 317 7777
Fax: +65 317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the **Cisco Web site at www.cisco.com/go/offices**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

All contents are Copyright © 1992–2002, Cisco Systems, Inc. All rights reserved. Cisco, Cisco IOS, Cisco Systems, the Cisco Systems logo, and PIX are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries. All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0208R)

202970/ETMG 9/02

069
Doc: 3702

1662
2

Segurança Tipo 1 doc 5

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 070
Doc 3702

15.621

Configuring Building Blocks

Building Blocks allow you to optimize your configuration. Objects such as hosts, protocols, or services can be grouped, allowing you to issue a single command to every item in the group by using the name of the group.

The Building Blocks feature is used to associate names that can be used in place of corresponding data values in settings and rules. This facilitates ease of maintenance.

For example, an access rule might have a source address of 1.2.3.4. As an alternative, you can use building blocks to create a network object named fred-pc with the address 1.2.3.4. You can then create an access rule with the source address as fred-pc.

Using Building Blocks, you identify objects that will be used on your network, that are configured separately. For example, you can identify the servers used for AAA authentication. The protocols used to connect to those servers, however, are configured in Settings. This design facilitates network updates, as building blocks are defined only once and in one location.

Important Notes About Building Blocks

- You can edit only those objects defined at the current scope.
- Building blocks do not have a one-to-one association.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 071
Doc. 3702

- When an object is selected in the directory tree, all elements defined at the same level and above are applied.
- If you select an object by name and that name is defined at multiple scopes, the version defined nearest the current scope is selected. (See the "Configuring Network Objects" section on page 6-2 for examples using network objects.)

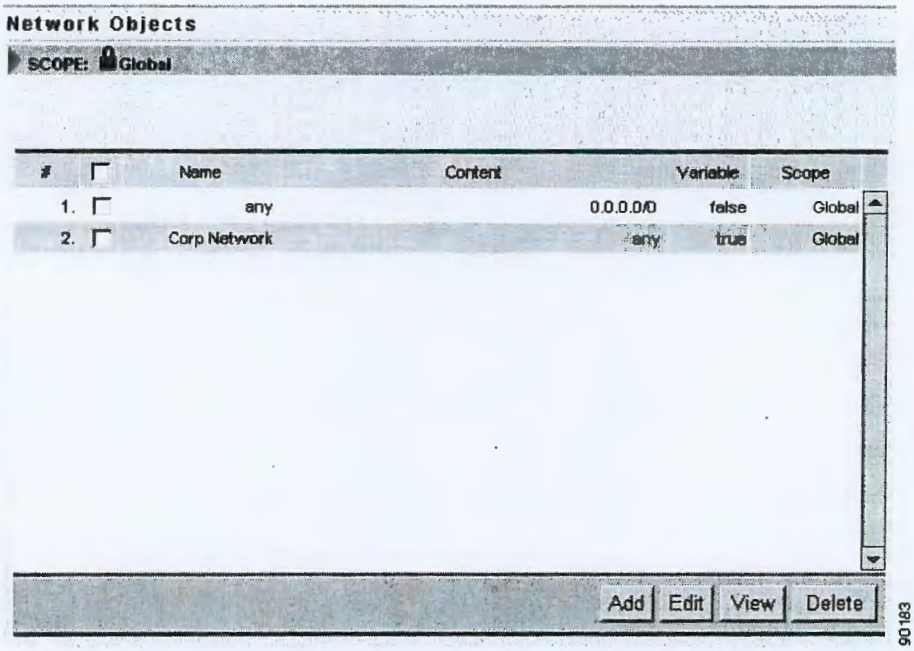
Configuring Network Objects

The Network Objects feature allows you to group a set of network addresses represented by an IP network (name, IP address, IP mask). This information provides the basic identification information for that network. Firewall MC uses the name and IP address–netmask pair to resolve references to the network in the source and destination conditions of access rules and in translation rules. Firewall MC uses the interface value to apply access and translation rules that refer the network to the correct interface. The interface delivers network packets to the network, thus enforcing the rules that refer to that network.

The following examples will help you to better understand how network objects can be used. Let's say you want to create the network object *Corp Network* at the Global scope, but different IP addresses will be used depending on the group being addressed. As a result, you can use a variable, which allows different values to be set for a building block for different devices or groups. The values are substituted into the same rule as applied to those different devices and groups (Figure 6-1).

RQS nº 03/2005 CN
CPMI - CORREIOS
Fls Nº 072
3702
Doc

Figure 6-1 Example 1—Network Object "Corp Network" Defined at the Global Scope with Variable

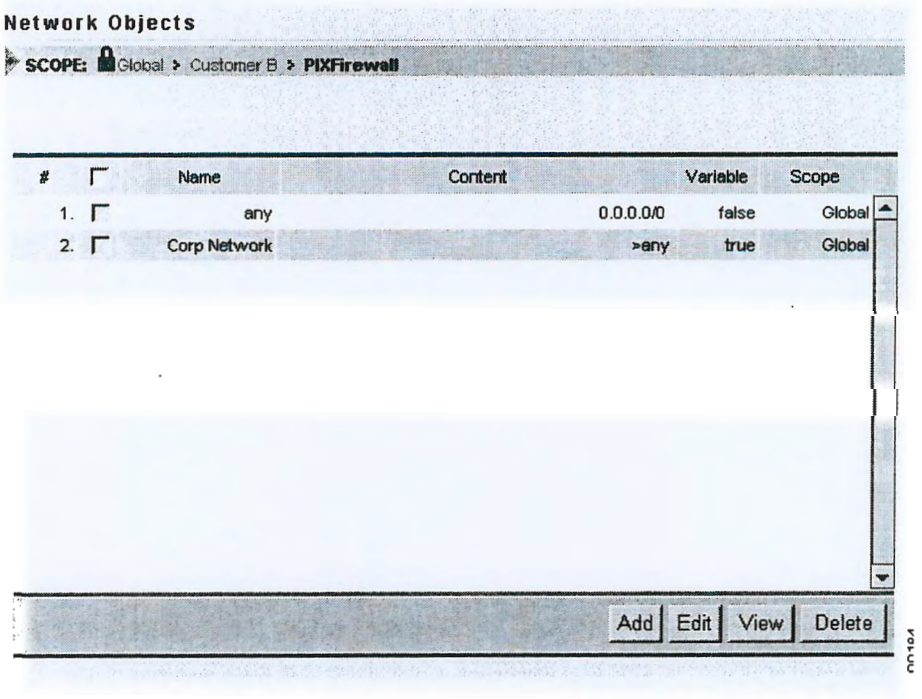


To access the Network Object feature, select **Configuration > Building Blocks > Network Objects**. The Network Objects table defaults to the Global scope. You complete the wizard to define the network object. When you are returned to the Network Objects table, *Corp Network* is shown in the table.

If you select the device *PIX Firewall* using the object selector, then view the Network Objects table for that scope, *Corp Network* is shown as created at the Global scope with the variable setting enabled. (The variable is set to true.) Notice that the check box is grayed-out, which means you cannot make changes at the device level (Figure 6-2).

RQS nº 03/2005 - CN
CPMI CORREIOS
Fls Nº 073
3702
Doc.

Figure 6-2 Example 1—Network Object "Corp Network" Shown at the Device Scope

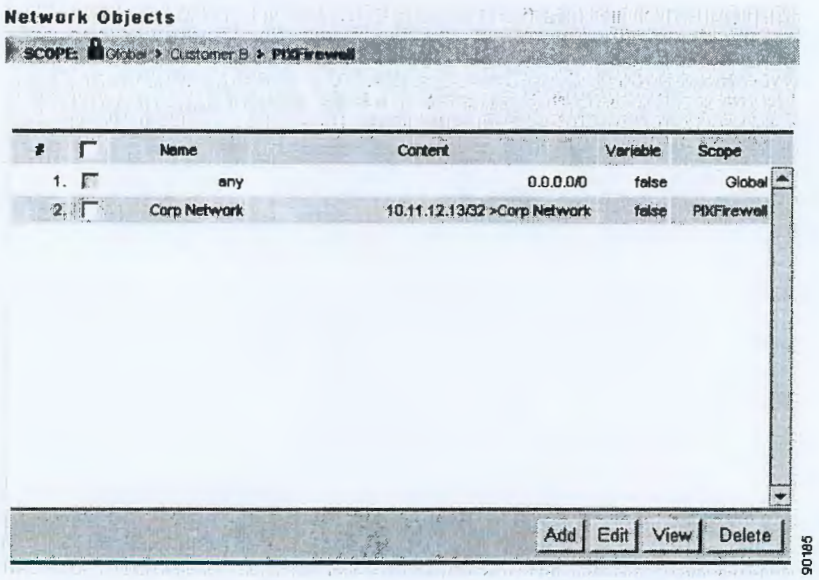


When you define *Corp Network* at the *PIX Firewall* scope, the new network object replaces the one defined at the Global scope and assigns an IP address to it (Figure 6-3). *Corp Network* can now be edited at the device scope; it is no longer shown as a variable. (The variable is set to false.)

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 074
3702
Doc.

16.617
L

Figure 6-3 Example 1—Network Object "Corp Network" Defined at the Device Scope



To create a mandatory access rule at the Global scope, you can use *Corp Network* as the source address.

If you view the access rules table for the Mandatory Global scope and the Default PIX Firewall scope, you will see the same access rule in each table. When the configuration file for the PIX Firewall is generated, the access rule uses the network object *Corp Network* and the IP address defined at the device level. This is displayed in the configuration file as

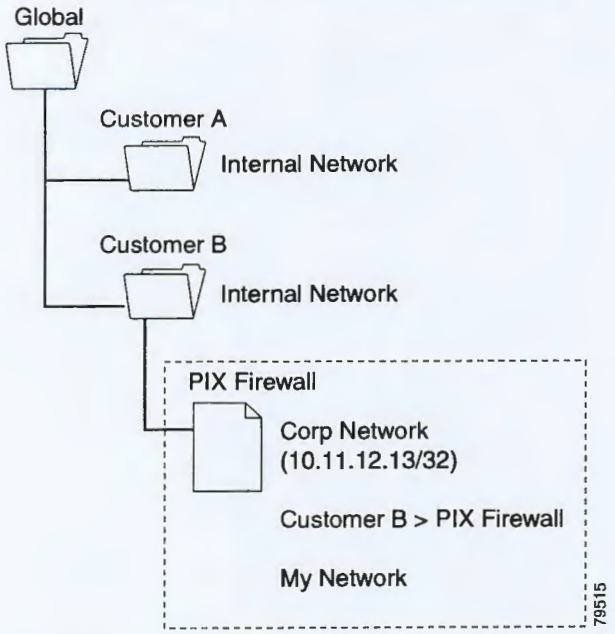
```
: acl_mdc_inside_access Access List

access-list acl_mdc_inside_access permit tcp 10.11.12.13
255.255.255.255 any
```

In conclusion, the network object defined at the Global scope using a variable must be redefined at the device scope with the same name, which then allows it to be used by access rules or translation rules.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 075
Doc 3702

Now consider another example. If you select an object by name and that name is defined at multiple scopes, the version defined nearest the current scope is selected. For this example, assume a service provider has two customers: *Customer A* and *Customer B* (Figure 6-4).

Figure 6-4 Example 2—Network Object Diagram



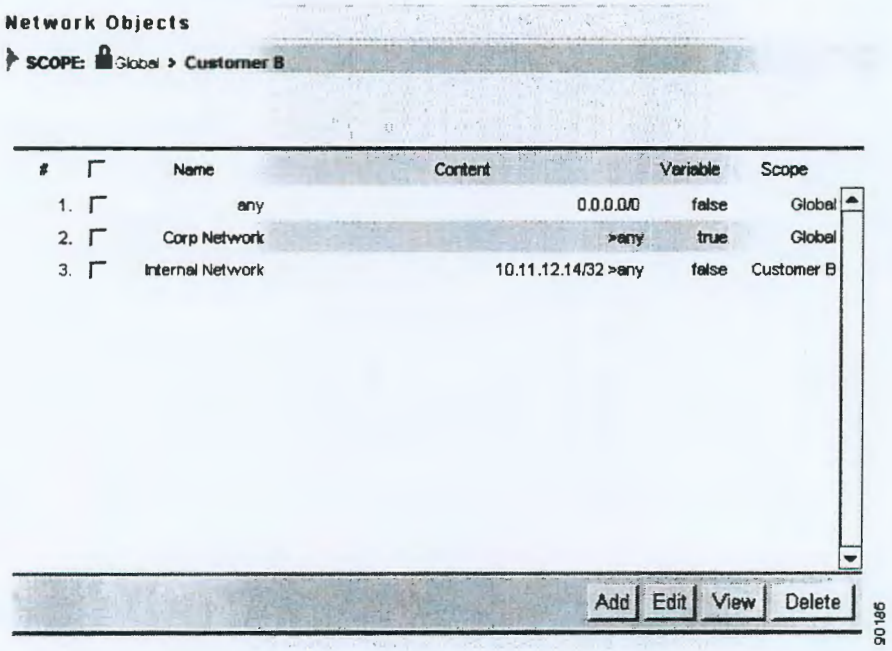
Customers A and B have the network object *Internal Network* defined. Customer B uses a device named *PIX Firewall*. Because *PIX Firewall* is closer to Customer B than Customer A in the navigation tree, the device will use the network object *Internal Network* defined at the *Customer B* scope. When you view the Network Objects table at the device scope, the object name is shown as Customer B>Internal Network.

The Network Object tables used to configure this example are shown in Figure 6-5 through Figure 6-7.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 076
Doc 3702

16.615

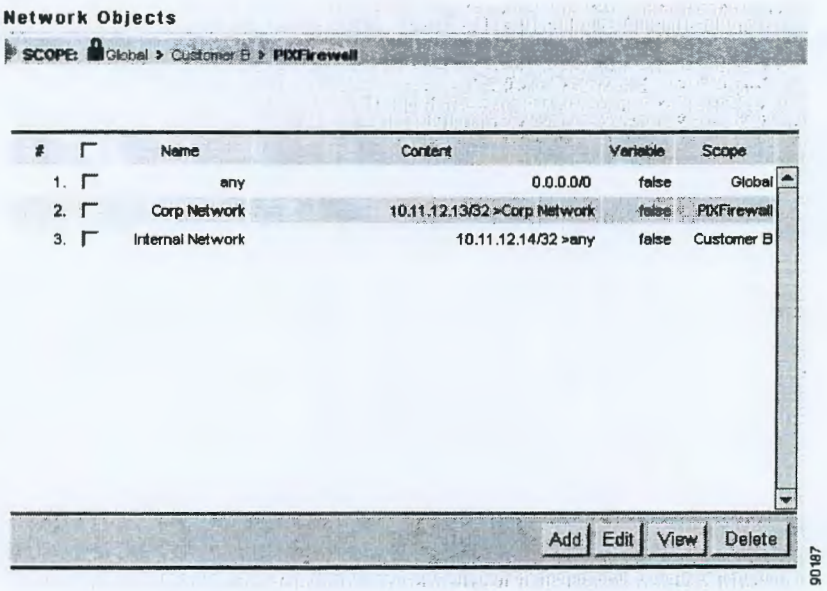
Figure 6-5 Example 2—Network Object "Internal Network" Defined at the Customer B Scope



To access the table in Figure 6-5, you select **Configuration > Building Blocks > Network Objects**. Using the object selector, you select *Customer B*.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 077
3702
Doc

Figure 6-6 Example 2—Network Object "Internal Network" Shown at the Device Scope



To access the table in Figure 6-6, you select **Configuration>Building Blocks> Network Objects**. Using the object selector, you select *PIX Firewall*.

After you have defined the network object at the device scope, the table displays the updated network object *Internal Network* for the device.

A third example and a standard use of a network object is to define a network object (for example, *My Network)* at the PIX Firewall level. The network object is then used only at the device scope (Figure 6-7).

RQS nº 03/2005 - CN
CPMI CORREIOS
Fls Nº 078
Doc 3702

16.613
2

Figure 6-7 Example 3—Network Object "My Network" Defined at the Device Scope

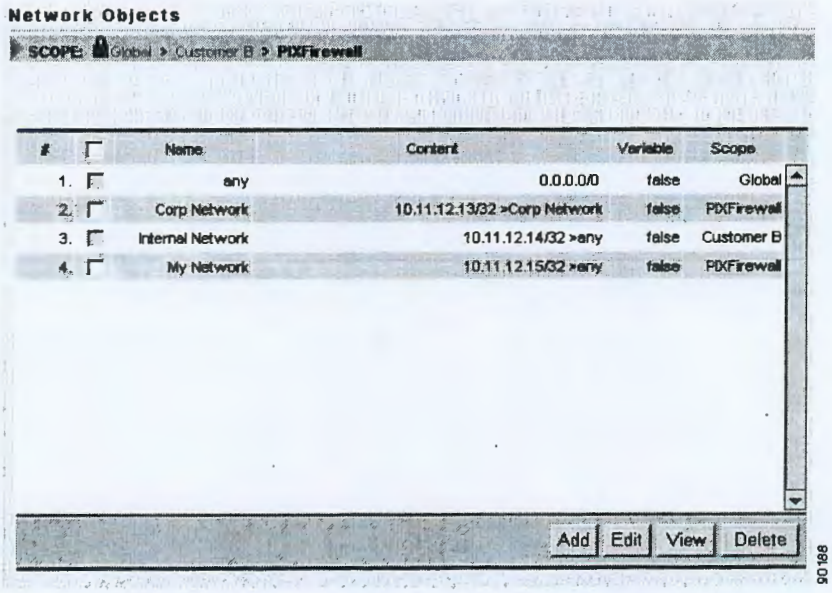


Table 6-1 shows the wizard used to configure network objects with the variable enabled.

Table 6-2 shows the wizard used to configure network objects with the variable disabled.

Table 6-1 Wizard Used to Add or Edit a Network Object (Variable Enabled)

	Wizard Page
Step 1	Enter Definition—Allows you to identify a network object.
Step 2	Summary—Allows you to verify configuration settings before committing settings to the database for deployment.

RQS nº 03/2005 - CN
CPMI — CORREIOS
Fls. Nº 079
3702
Doc

16.612
L.

Table 6-2 Wizard Used to Add or Edit a Network Object (Variable Disabled)

	Wizard Page
Step 1	Enter Definition—Allows you to identify a network object.
Step 2	Enter IPs—Allows you to enter an IP address and mask.
Step 3	Select Network—Allows you to select available objects.
Step 4	Summary—Allows you to verify configuration settings before committing settings to the database for deployment.

Adding or Editing a Network Object

Before You Begin

- If workflow is enabled, select an activity. (See the "Understanding Activity Actions and States" section on page 9-6.)
- Using the Object Selector, select the scope for the devices to configure. (See the "Object Selector" section on page 2-18.)

Step 1 Select **Configuration>Building Blocks>Network Objects**.

The Network Objects page appears.

Step 2 Do one of the following:

- To add a row in the table, click **Add**.

  The Enter Definition page appears.
- To edit a row, select the check box for the row in the table, then click **Edit**.

  The Enter Definition page appears.

Step 3 Enter the network entity name to be assigned to network object.

Step 4 Enter a comment in the Description field.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 080
3702
Doc

Step 5 Select the Variable check box to use a value in place of a defined building block. For more information, see the online help.

Note This feature allows different values to be set for a building block for different devices or groups; the values are substituted into the same rule as applied to those different devices and groups.

Step 6 Click **Next**.

The Enter IP(s) page appears.

Step 7 Enter the network IP address and mask.

No IP address and mask are needed if you plan to use only nested network objects.

Step 8 Click **Next**.

The Select Networks page appears.

Step 9 Select the available object, then click **Select =>**.

The object is moved to the Selected Objects column.

Step 10 Click **Next**.

The network objects summary page appears.

Step 11 Verify the information is correct, then click **Finish**.

Changes are applied to the assigned firewall device configuration files when they are generated. The configuration files are then downloaded to the firewall devices at deployment. (See Chapter 9, "Managing Activities and Jobs.")

Deleting a Network Object

Before You Begin

Make sure you have the necessary permissions to perform this function. (See Appendix B, "Understanding User Roles and Permissions.")

Step 1 Select **Configuration>Building Blocks>Network Objects**.

The Network Objects page appears.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 081
Nº 3702
Doc.

Step 2 Select the check box for the row in the table, then click **Delete**.

You are prompted to confirm the delete request.

Step 3 Click **OK**.

As the page refreshes, you are prompted with another popup window if access rules or translation rules are affected by the deletion. You will need to review the rules tables and make corrections as needed.

Step 4 Click **OK**.

The row is removed from the table, and the information is removed from the assigned firewall device configuration files when they are deployed. (See Chapter 9, "Managing Activities and Jobs.")

Configuring Service Definitions

The Service Definition feature allows you to create a single access rule that controls access to multiple protocols, for example, WWW.

Table 6-3 shows the wizard used to add or edit service definitions.

Table 6-3 Wizard Used to Add or Edit Service Definitions

	Wizard Page
Step 1	Specify Name and Select Transport—Allows you to enter service protocol information.
Step 2	Select ICMP Values—Used to define ICMP only.
Step 3	Summary—Allows you to verify configuration settings before committing settings to the database for deployment.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 082
3702
Doc.

Adding or Editing a Service Definition

Before You Begin

- If workflow is enabled, select an activity. (See the "Understanding Activity Actions and States" section on page 9-6.)
- Using the Object Selector, select the scope for the devices to configure. (See the "Object Selector" section on page 2-18.)

Step 1 Select **Configuration > Building Blocks > Service Definitions**.

The Service Definitions table appears.

Step 2 Do one of the following:

- To add a row in the table, click **Add**.

  The Specify Name and Select Transport page appears.
- To edit a row, select the check box for the row in the table, then click **Edit**.

  The Specify Name and Select Transport page appears.

Step 3 Enter the name of the service.

Step 4 Enter an optional comment in the Description field.

Step 5 Select the transport protocol from the list box, then click **Next**.

Note Only IP requires an IP protocol number.

Step 6 Do one of the following:

- If you selected ICMP as the transport protocol, the select ICMP Values page appears. To select the ICMP values, go to Step 7.
- If you selected TCP or UDP as the transport protocol, the Select TCP/UDP Values page appears. To select the TCP/UDP values, go to Step 8.
- If you selected IP as the transport protocol, enter the IP protocol number, then click **Next**.

  The service descriptions summary page appears. Go to Step 9.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 083
Doc. 3702

Step 7 Do the following:

a. Select the type of message from the list box.

b. Click **Next**.

The service descriptions summary page appears. Go to Step 9.

Step 8 **If you selected TCP or UDP as the transport protocol**:

The Select TCP/UDP Values page appears.

a. Enter the destination port or port range. Values are 0–65,535.

b. Enter the source port or port range. Values are 0–65,535.

c. Click **Next**.

The service descriptions summary page appears. Go to Step 9.

If you selected IP as the transport protocol:

a. Enter the IP protocol number, then click **Next**.

The service descriptions summary page appears.

Step 9 Verify the information is correct, then click **Finish**.

Changes are applied to the assigned firewall device configuration files when they are generated. The configuration files are then downloaded to the firewall devices at deployment. (See Chapter 9, "Managing Activities and Jobs.")

Deleting a Service Definition

Before You Begin

- Make sure you have the necessary permissions to perform this function. (See Appendix B, "Understanding User Roles and Permissions.")

Step 1 Select **Configuration > Building Blocks > Service Descriptions**.

The Service Descriptions page appears.

Step 2 Select the check box for the row in the table, then click **Delete**.

You are prompted to confirm the delete request.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 084
Nº 3702
Doc

Step 3 Click **OK**.

As the page refreshes, you are prompted with another popup window if access rules or translation rules are affected by the deletion. You will need to review the rules tables and make corrections as needed.

Step 4 Click **OK**.

The row is removed from the table, and the information is removed from the assigned firewall device configuration files when they are deployed. (See Chapter 9, "Managing Activities and Jobs.")

Configuring Service Groups

The Service Definitions feature allows you to create a single access rule that controls access to multiple services, for example, you can write a rule that permits traffic for Telnet and HTTP in a single rule.

Table 6-4 shows the wizard used to add or edit service groups.

Table 6-4 Wizard Used to Add or Edit Service Groups

	Wizard Page
Step 1	Add Name and Description—Allows you to define a service group.
Step 2	Select Service—Allows you to identify the services used for the defined service group.
Step 3	Summary—Allows you to verify configuration settings before committing settings to the database for deployment.

Adding or Editing a Service Group

Before You Begin

- If workflow is enabled, select an activity. (See the "Understanding Activity Actions and States" section on page 9-6.)
- Using the Object Selector, select the scope for the devices to configure. (See the "Object Selector" section on page 2-18.)

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 0085
3702
Doc

Note Some elements in the main table might be grayed out. This is because they are defined at a higher scope and cannot be edited from this level.

Step 1 Select **Configuration>Building Blocks>Service Groups**.

The Service Groups page appears.

Step 2 Do one of the following:

- To add a new row in the table, click **Add**.

  The Add Name and Description page appears.

- To edit a row, select the check box for the row in the table, then click **Edit**.

  The Add Name and Description page appears.

Step 3 Enter the service group name.

Step 4 Enter an optional comment in the Description field.

Step 5 Click **Next**.

The Select Services page appears.

Step 6 Select the available object, then click **Select =>**.

The object is moved to the Selected Objects column.

Step 7 Click **Next**.

The service groups summary page appears.

Step 8 Verify the information is correct, then click **Finish**.

Changes are applied to the assigned firewall device configuration files when they are generated. The configuration files are then downloaded to the firewall devices at deployment. (See Chapter 9, "Managing Activities and Jobs.")

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 086
Doc 3702

16.605

Deleting a Service Group

Before You Begin

Make sure you have the necessary permissions to perform this function. (See Appendix B, "Understanding User Roles and Permissions.")

Step 1 Select **Configuration>Building Blocks>Service Groups**.

The Service Groups table appears.

Step 2 Select the check box for the row in the table, then click **Delete**.

You are prompted to confirm the delete request.

Step 3 Click **OK**.

As the page refreshes, you are prompted with another popup window if access rules or translation rules are affected by the deletion. You will need to review the rules tables and make corrections as needed.

Step 4 Click **OK**.

The row is removed from the table, and the information is removed from the assigned firewall device configuration files when they are deployed. (See Chapter 9, "Managing Activities and Jobs.")

Configuring AAA Server Groups

Firewall MC lets you define separate groups of TACACS+ or RADIUS servers for specifying different types of traffic, for example, a TACACS+ server for inbound traffic and another for outbound HTTP traffic authenticated by a TACACS+ server and inbound traffic authenticated by RADIUS.

AAA server groups use tags, which are used to direct different types of traffic to each authentication server. If the first authentication server in the list fails, the AAA subsystem fails over to the next server in the tag group. You can have up to 14 tag groups, and each group can have up to 14 AAA servers, totaling up to 196 AAA servers.

RQS nº 03/2005 CN
CPMI - CORREIOS
Fls. Nº 087
Doc. 3702

Configuring an AAA server group is a two-tier process. First, you create an AAA server group. Second, you define AAA servers within that group. You have the option of inserting an AAA server while you are creating an AAA server group.

Note In Firewall MC, the Group LOCAL protocol local scoped from Global entry represents the AAA group, named LOCAL, that exists by default on PIX Firewalls running version 6.2 or later. The default group cannot be modified or disabled. This group is used for administrative authentication and talks directly to the PIX Firewall instead of a separate AAA server. LOCAL specifies to use the PIX Firewall local user database for local command authorization. The LOCAL group is displayed in the configuration file as `aaa-server LOCAL protocol local.`

To set LOCAL for AAA Authentication, select **Configuration>Settings> AAA Admin Authentication**.

Table 6-5 shows the wizard used to create an AAA server group and insert an AAA server.

Table 6-5 Wizard Used to Create, Insert, or Edit an AAA Server Group

	Wizard Page
Step 1	Select Group Name—Allows you to define a new AAA server group.
Step 2	Define Server—Allows you to assign a server to the AAA server group.
Step 3	Summary—Allows you to verify configuration settings before committing settings to the database for deployment.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 088
Doc 3702

Creating or Editing an AAA Server Group

Note While you are creating an AAA server group, you can insert an AAA server.

Before You Begin

- If workflow is enabled, select an activity. (See the "Understanding Activity Actions and States" section on page 9-6.)
- Using the Object Selector, select the scope for the devices to configure. (See the "Object Selector" section on page 2-18.)

Note The following procedure assumes you are defining a server group and identifying a server within that group.

Step 1 Select **Configuration>Building Blocks>AAA Server Group**.

The AAA Server Group page appears.

Step 2 Do one of the following:

- To add a server group in the table, click **Create**.

  The Select Group Name page appears.
- To add a server to a group in the table, select the check box for the row in the table after which you want to new row inserted, then click **Insert**.

  The Define Server page appears.
- To edit a group, select the check box for the row in the table, then click **Edit**.

  The Select Group Name page appears.
- To edit a server, select the check box for the row in the table, then click **Edit**.

  The Define Server page appears.

Step 3 Enter the AAA server group name. Spaces are not permitted. A maximum of 14 server groups is permitted.

Step 4 Click the Radius or TACACS protocol radio button to identify the authentication protocol used for the server group.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 089
3702
Doc.

Step 5 Click **Next**.

The Define Server page appears.

Step 6 Select the interface from the list box.

Step 7 Enter the IP address.

Step 8 Enter the server key. For more information, see the online help.

Step 9 Verify the timeout value. Default is 5 seconds.

Step 10 Click **Next**.

The AAA server group summary page appears.

Step 11 Verify the information is correct, then click **Finish**.

Changes are applied to the assigned firewall device configuration files when they are generated. The configuration files are then downloaded to the firewall devices at deployment. (See Chapter 9, "Managing Activities and Jobs.")

Deleting an AAA Server Group or Element

Before You Begin

Make sure you have the necessary permissions to perform this function. (See Appendix B, "Understanding User Roles and Permissions.")

Step 1 Select **Configuration>Building Blocks>AAA Server Group**.

The AAA Server Group page appears.

Step 2 Select the check box for the row in the table, then click **Delete**.

You are prompted to confirm the delete request.

Step 3 Click **OK**.

As the page refreshes, you are prompted with another popup window if access rules or translation rules are affected by the deletion. You will need to review the rules tables and make corrections as needed.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 090
Doc 3702

Step 4 Click **OK**.

The row is removed from the table, and the information is removed from the assigned firewall device configuration files when they are deployed. (See Chapter 9, "Managing Activities and Jobs.")

Configuring Address Translation Pools

The Address Translation Pools feature allows you to create global address pools used in dynamic NAT rules.

Configuring address translation pools is a two-tier process. First, you create a pool. Second, you define the elements within that pool. You have the option of defining the elements while you are creating an address translation pool.

Table 6-6 shows the wizard used to create an address translation pool and insert a pool element in a single procedure.

Table 6-6 Wizard Used to Create or Edit an Address Translation Pool and Pool Element

	Wizard Page
Step 1	Enter Pool Name—Allows you to define an address pool.
Step 2	Define Element—Allows you to assign IP addresses and masks to the address pool.
Step 3	Summary—Allows you to verify configuration settings before committing settings to the database for deployment.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 091
Doc 3702

Creating or Editing an Address Translation Pool

Note While you are creating an address translation pool, you can insert an address pool element as part of the procedure.

Before You Begin

- If workflow is enabled, select an activity. (See the "Understanding Activity Actions and States" section on page 9-6.)
- Using the Object Selector, select the scope for the devices to configure. (See the "Object Selector" section on page 2-18.)

Note The following procedure assumes you are defining an address translation pool and identifying a range of pool values within that pool group.

Step 1 Select **Configuration>Building Blocks> Address Translation Pools**.

The Address Translation Pool page appears.

Step 2 Do one of the following:

- To add a pool group to the table, click **Create**.

  The Enter Pool Name page appears.
- To add a pool element to the table, select the check box for the row in the table after which you want to new row inserted, then click **Insert**.

  The Enter Pool Element page appears.
- To edit a pool, select the check box for the row in the table, then click **Edit**.

  The Enter Pool Name page appears.
- To edit a pool range, select the check box for the row in the table, then click **Edit**.

  The Enter Pool Element page appears.

Step 3 Enter the pool name to identify the address translation pool, for example, external addresses.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 092
Doc 3702

16.599
2

Step 4 Click **Next**.

The Enter Pool Element page appears.

Step 5 Select the interface from the list box.

Step 6 To use the interface address as the closing PAT address, select the PAT check box.

Step 7 Enter address ranges and masks. For more information, see the online help.

Step 8 Click **Next**.

The address translation pool summary page appears.

Step 9 Verify the information is correct, then click **Finish**.

Changes are applied to the assigned firewall device configuration files when they are generated. The configuration files are then downloaded to the firewall devices at deployment. (See Chapter 9, "Managing Activities and Jobs.")

Note Settings enabled during the configuration process are displayed as true in the wizard summary page.

Deleting an Address Translation Pool or Element

Before You Begin

Make sure you have the necessary permissions to perform this function. (See Appendix B, "Understanding User Roles and Permissions.")

Step 1 Select **Configuration>Building Blocks> Address Translation Pools**.

The Address Translation Pool page appears.

Step 2 Select the check box for the row in the table, then click **Delete**.

You are prompted to confirm the delete request.

Step 3 Click **OK**.

As the page refreshes, you are prompted with another popup window if access rules or translation rules are affected by the deletion. You will need to review the rules tables and make corrections as needed.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 093
Doc. 3702

Step 4 Click **OK**.

The row is removed from the table, and the information is removed from the assigned firewall device configuration files when they are deployed. (See Chapter 9, "Managing Activities and Jobs.")

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 094
Doc 3702

16.534
2

Table 2-13 Inventory Manager Tasks (continued)

Task	Purpose	Action
Create and view inventory custom reports.	Create a customized report that gathers all or any of this information about specified devices: • IP address • User field • RAM size • Flash size • Port count • Hardware version • Card type • Serial number • SAA (Service Assurance Agent) information	Select Resource Manager Essentials > Administration > Inventory > Custom Reports. To view a previously-created report, select Resource Manager Essentials > Inventory > Custom Reports.
Define filters for change reports.	Define filters that determine what data is displayed in your inventory change reports.	Select Resource Manager Essentials > Administration > Inventory > Inventory Change Filter.
Schedule inventory collection.	Schedule polling and collection to update your network inventory.	Select Resource Manager Essentials > Administration > Inventory > Schedule Collection.
Update inventory collection.	Run inventory collection as a one-time event for specific devices.	Select Resource Manager Essentials > Administration > Inventory > Update Inventory.
Schedule device polling.	Schedule periodic polling of managed devices. Since the poller uses fewer network resources, you should schedule inventory polling to run more frequently than inventory collection.	Select Resource Manager Essentials > Administration > Inventory > Inventory Poller.
Run an inventory 24-hour report.	Determine what inventory changes were made in the last 24 hours.	Select Resource Manager Essentials > 24-Hour Reports > Inventory Change Report.

RQS nº 03/2005 CN
CPMI CORREIOS
Fls Nº 095
Doc. 3702

16.533
2

Table 2-13 Inventory Manager Tasks (continued)

Task	Purpose	Action
View a hardware report.	View user-specified hardware information for each device.	Select Resource Manager Essentials > Inventory > Hardware Report.
View a software report.	View user-specified software information for each device.	Select Resource Manager Essentials > Inventory > Software Report.
View information about devices.	View detailed hardware, software, chassis, and interface information for multiple devices.	Select Resource Manager Essentials > Inventory > Detailed Device Report.
View a device Y2K compliance report.	View which managed devices are compliant to the year 2000. Compliance is determined by device type and software version.	Select Resource Manager Essentials > Inventory > Year 2000 Report.
View device information within device classes.	View a bar chart of the distribution of all managed devices among the recognized device classes.	Select Resource Manager Essentials > Inventory > Hardware Summary Graph.
View the software versions in each device class.	View a bar chart of the distribution of the major and minor software versions running on your selected devices in each device class.	Select Resource Manager Essentials > Inventory > Software Version Graph.
View device information in each device class.	View a bar chart showing the distribution of your selected devices in each device class.	Select Resource Manager Essentials > Inventory > Chassis Summary Graph.
View a summary of chassis slots.	View the total number of selected devices and the number of devices with free slots for each device class that supports capacity planning.	Select Resource Manager Essentials > Inventory > Chassis Slot Summary.
View the chassis slot details.	View the total slots, available slots, location, and userfield information for each device.	Select Resource Manager Essentials > Inventory > Chassis Slot Details.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 096
Doc.
3702

Table 2-13 Inventory Manager Tasks (continued)

Task	Purpose	Action
View details on multiservice ports.	Check the switch multiservice ports, which support voice traffic, to make sure the power supply is adequate for the number of multiservice modules installed in each switch.	Select Resource Manager Essentials > Inventory > MultiService Port Details.
Verify community strings, usernames, and passwords.	Ensure that the database used to store the community strings and passwords remains synchronized with the actual devices. Detect errors made when devices were added or imported.	Select Resource Manager Essentials > Administration > Inventory > Check Device Attributes.
View attribute check results.	View the results of updated device attributes.	Select Resource Manager Essentials > Administration > Inventory > View Check Results.
View historical data.	View all historical data associated with scheduled inventory collection. It shows the last run, duration, devices scanned, and average scan time.	Select Resource Manager Essentials > Inventory > Scan History.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 097
Nº Doc. 3702

Job Approval

Software Management and Configuration Management tasks allow you to set up approval checkpoints before you run a job that will change a configuration or update the software image on a device. This can help increase the security on your network, by forcing these types of high-impact jobs to be approved before they are scheduled or executed. Moreover, other CiscoWorks applications can also take advantage of this feature (for example, ACL Manager).

Job Approval is used by other applications to ensure that a job be approved before it can run. Job Approval sends job requests via e-mail to the users on the approver list of a job. If none of the approvers approves the job by its scheduled run time, or if an approver rejects the job, the job is moved to the rejected state and will not run.

When Job Approval is enabled, applications that use it require that the user do the following for each job that is scheduled:

- Assign one or more approver lists to the job
- Schedule the job to run in the future, rather than immediately

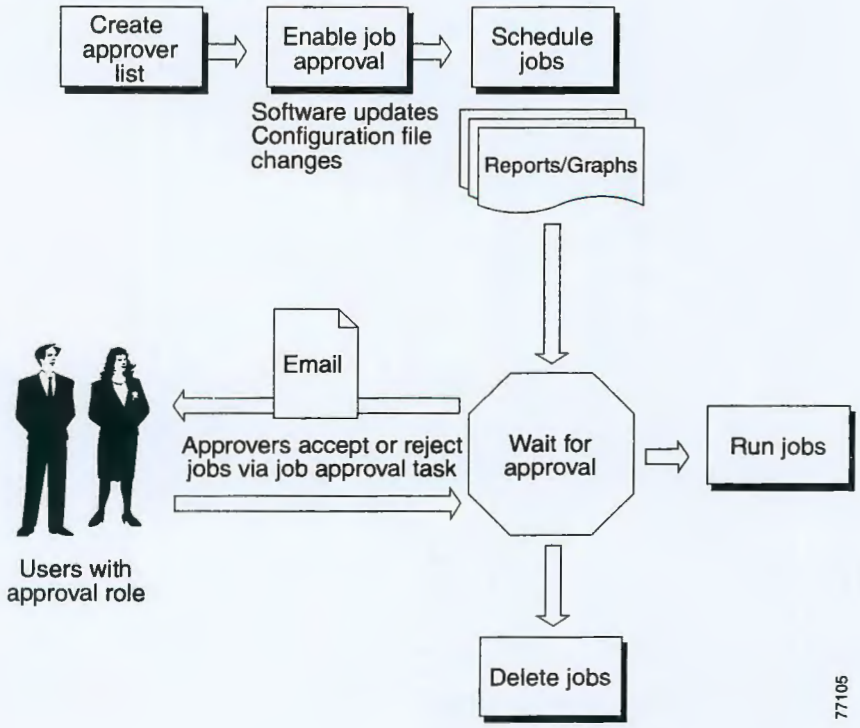
Job Approval Process

The job approval process requires that you first create an approver list; a list of CiscoWorks user accounts that must approve the job before it can be run. Users must have the role of approver to be included in an approver list.

After you have created at least one approver list, you can enable the job approval feature for Software Management, Configuration Management, or both. See Figure 2-15.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 098
Doc 3702

Figure 2-15 Job Approval Workflow



The user must have the user role of system administrator or network administrator to perform this task. You must create at least one approver list before you can enable job approval. Only users who have been assigned the approver role, will be displayed in the list of valid user accounts for approval.

For Software Management, you can also be specific as to the types of jobs that require approval (new image distribution, undo image distribution, retry image distribution).

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 099
Doc 3702

During scheduling of a job that requires job approval, the user will be queried to select an approver list. When scheduling is complete (the job must be scheduled for the future and not for immediate execution), an e-mail will be sent to all users on the approver list and the job will be placed in the job execution queue with a wait for approval status. The job will not run until at least one user on the approval list has accepted it. If anyone rejects the job, or if no one accepts the job by its scheduled time, the job will not run. The URL to this task is included in the e-mail.

The approver can only accept or reject the job and cannot change any of the operational parameters of the job. All approvers on the list and the creator of the job will receive e-mail notification when the job is either accepted or rejected.

Table 2-14 shows the tasks that can be accomplished with the Job Approval application.

Table 2-14 Job Approval Tasks

Task	Purpose	Action
Approve or reject jobs.	Approve or reject a job for which you are an approver.	Select Resource Manager Essentials > Administration > Job Approval > Approve or Reject Jobs.
Set up Job Approval.	Enable or disable the option.	Select Resource Manager Essentials > Administration > Job Approval > Edit Preferences.
Create an approver list.	Create a new approver list.	Select Resource Manager Essentials > Administration > Job Approval > Create Approver List.
Edit an approver list.	Edit an existing approver list.	Select Resource Manager Essentials > Administration > Job Approval > Edit Approver List.
Enable jobs	Enable all imported Essentials jobs.	Select Resource Manager Essentials > Administration > Job Approval > Enable Jobs.

For information on how to perform the Job Approval tasks, see the online help.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 100
Doc 3702

Software Management

The Software Management application automates the steps associated with upgrade planning, scheduling, downloading software images, and monitoring your network.

New Features of Software Management

The Software Management application has the following new features:

- With the remote staging and distribution feature you can select a software image, store it temporarily on a device, and then distribute the staged image to the devices that require an upgrade, in your network (**Resource Manager Essentials > Software Management > Remote Staging**).

  After the device is successfully upgraded, the stored image on the remote stage device is deleted automatically, if delete and squeeze operations are supported by the device.

  The remote staging feature is useful when the Resource Manager Essentials server and the devices (including the remote stage device you have chosen) are distributed across a WAN.

  For details, see the Essentials online help.
  (In the left navigation pane of the Essentials online help, select **Resource Manager essentials > Software Management > Remote Staging**).

- With the image-centric distribution feature, you can now select a software image and use it to perform an image upgrade on homogenous devices in your network (**Resource Manager Essentials > Software Management > Distribution > Distribute by Images**).

  For details, see the Essentials online help.
  (In the left navigation pane of the Essentials online help, select **Resource Manager essentials > Software Management > Distribution > Distributing by Images**).

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 101
Doc 3702

Benefits of Software Management

The Software Management application provides tools making it easier to store backup copies of all Cisco software images running on network devices. It also helps you to store any additional software images that you may wish to maintain, and to plan and execute software image upgrades to multiple devices on the network at the same time.

It gives you flexibility in upgrading devices with software images. You can either select a set of devices and perform an image upgrade, or select a software image and select a set of devices on which to perform the upgrade. You can even select one of your devices as a remote stage to temporarily store a software image.

It can analyze devices against software image requirements to determine device compatibility and make recommendations before performing a software upgrade.

The Software Management application can also download and list applicable images from Cisco.com, while recommending an image for the device upgrade. You should select the Cisco.com filters in Administration preferences, to avail this benefit.

If any errors occur during a software image upgrade, Software Management will allow you to roll back to the previous version. Optionally, for added security and change-management control, software images will not be downloaded unless approved by specifically assigned users. Software Management reports also allow you to track all software upgrades and monitor known bugs in the software versions running on your network.

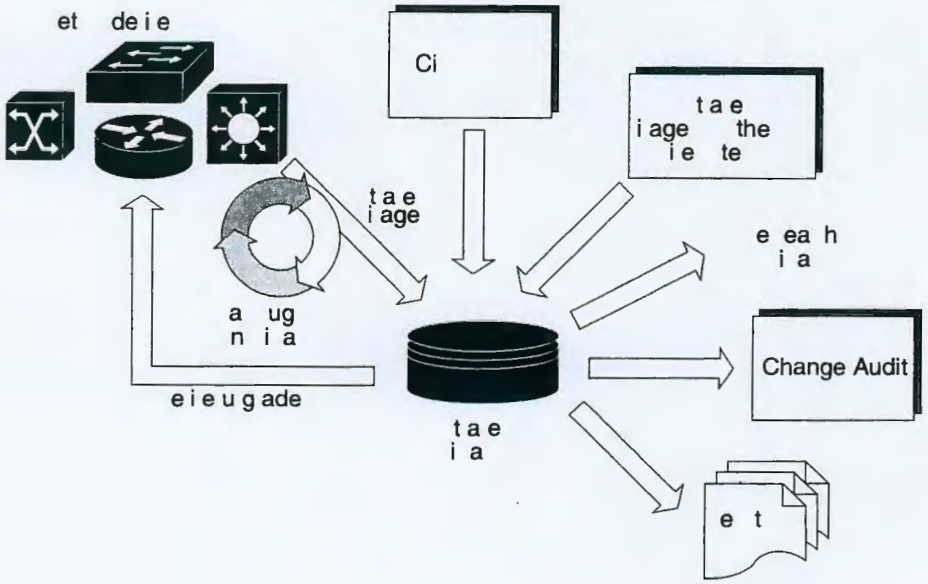
Software Management Functional Flow

Software images must be imported into Essentials to be maintained in the Software Image Library. Images can initially be imported to the Essentials Software Library from all managed Cisco devices on the network to create a baseline backup copy of all software images running on your network.

Images can also be imported from Cisco.com or the local machine to be used for software image upgrades. See Figure 2-16.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 102
Doc 3702

Figure 2-16 Software Management Functional Flow



After images are imported into the Software Image Library, the Software Management application can be configured to automatically poll devices on the network and produce a report of images running on devices that are not stored in the Essentials database. This ensures that for disaster recovery purposes, there is a backup of all software images running on the network in the software library at all times.

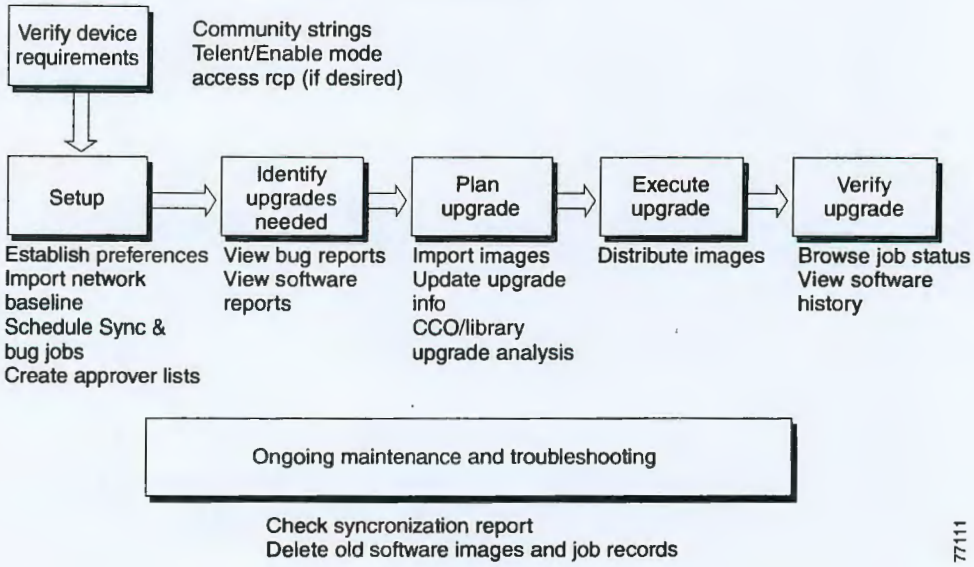
Any image that is stored in the Software Image Library can be used to perform a software upgrade. Each step of the process is recorded in the distribution, so if there is a failure, the network administrator will know the reasons for the failure. Software Manager maintains a log of all software upgrades, to make it easy to identify and track when software modifications are made to devices.

In addition, whenever a change is made to the software image on a device, a change record is sent to the Change Audit application, which collects and organizes all changes to network devices.

Software Management can also be configured to periodically check Cisco.com for known software bugs, and produce a report to show all bugs that affect devices on your network.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 103
Doc 3702

Figure 2-17 Software Management Workflow



The image depicts the Software Management workflow and associated tasks within Essentials (see Figure 2-17):

- Device requirements must be verified to ensure that Essentials will be able to access the devices to retrieve and upgrade software images.
- Perform setup tasks to begin using Software Management. Setup tasks include setting preferences that will be used for all Software Management import and upgrade jobs, creating any approver lists that will be used to approve software jobs, and scheduling jobs to periodically synchronize the software library with network devices and check Cisco.com for known software bugs.
- When Software Manager is set up, software and bug reports can be used to help identify when software upgrades might be needed.
- If a software upgrade is required, Software Management features can be used to analyze whether or not devices can accommodate the new image, and to actually distribute the new images to devices on the network.
- In addition, ongoing maintenance should be performed to ensure that a copy of every image running on the network is stored in the Essentials Software Library, and to remove images no longer needed from the Software Library.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 104
Doc. 3702

Table 2-15 shows the tasks you can accomplish with the Software Management application.

Table 2-15 Software Management Tasks

Task	Purpose	Action
Set up your Software Management preferences.	Specify information such as history page size, the directory where images are stored, the pathname of the user-supplied script to run before and after each device software upgrade. Specify if the images on Cisco.com should also be included during image recommendation of the device, and also specify the Cisco.com filters so that only those images that match the filter criteria are selected.	Select Resource Manager Essentials > Administration > Software Management > Edit Preferences.
Add images to the library.	Import images from all Software Management supported devices in your network into the Software Image Library.	Select Resource Manager Essentials > Software Management > Library > Add Images.
	Download images from Cisco.com into the Software Image Library.	
	Add images from a file system to the Software Image Library.	
Browse the library.	Generate a report of all the images in the Software Image Library. You can also delete images from the image library and edit image attributes.	Select Resource Manager Essentials > Software Management > Library > Browse Images.
Search the library.	Generate a report of a subset of images in the Software Image Library, based on details such as, device type, image type, and version. You can also delete images from the image library and edit image attributes.	Select Resource Manager Essentials > Software Management > Library > Search for Images.

RQS nº 03/2005 CN
CPMI CORREIOS
Fls Nº 105
Doc. 3702

Table 2-15 Software Management Tasks (continued)

Task	Purpose	Action
View a synchronization report.	Generate a synchronization report to determine which Software Management-supported devices are running software images not in the Software Image Library.	Select Resource Manager Essentials > Software Management > Library > Synchronization Report.
Schedule a synchronization job.	Specify the date, time, and frequency of a synchronization job. Cancel a scheduled synchronization job.	Select Resource Manager Essentials > Administration > Software Management > Schedule Synchronization Job.
Create approver lists.	Specify who can approve the various tasks necessary during a software upgrade.	Select Resource Manager Essentials > Administration > Job Approval > Create Approver List.
Edit or delete approver lists.	Edit and delete the list specifying who can approve tasks during a software upgrade.	Select Resource Manager Essentials > Administration >Job Approval > Edit Approver List.
Schedule image upgrade jobs.	Select devices and schedule software image upgrades to those devices.	Select Resource Manager Essentials > Software Management > Distribution > Distribute by Devices.
	Select a software image and use it to perform an image upgrade on the suitable devices in your network.	Select Resource Manager Essentials > Software Management > Distribution > Distribute by Images.
	Select a software image and use one of your devices as a remote stage to temporarily stage the image. Then upgrade suitable devices in your network with this staged image.	Select Resource Manager Essentials > Software Management > Remote Staging > Remote Staging and Distribution.
	Undo the upgrade and roll back to the previous image, after you have scheduled and completed upgrading the image.	Select Resource Manager Essentials > Software Management > Job Management > Browse Jobs.
Plan an upgrade from Cisco.com.	Determine the impact to and prerequisites for a new software deployment using images that reside in Cisco.com.	Select Resource Manager Essentials > Software Management > Distribution > CCO Upgrade Analysis.

RQS nº 03/2005 - CN
CPMI CORREIOS
Fls Nº 106
Doc 3702

Table 2-15 Software Management Tasks (continued)

Task	Purpose	Action
Plan an upgrade from the library.	Determine the impact to and prerequisites for a new software deployment using images in your software library.	Select Resource Manager Essentials > Software Management > Distribution > Library Upgrade Analysis.
Review scheduled jobs or undo an upgrade.	Review, or remove scheduled jobs. If the job is in the pending state, you can modify the schedule time. You can also retry failed jobs and undo completed image upgrade jobs.	Select Resource Manager Essentials > Software Management > Job Management > Browse Jobs.
View consolidated job information.	View a report of device upgrade results for selected jobs.	Select Resource Manager Essentials > Software Management > Job Management > Consolidated Job Report.
View recent software upgrade results.	Generate a report summarizing the most recent device software upgrade results stored in the history database.	Select Resource Manager Essentials > 24-Hour Reports > Software Upgrade Report.
Mail or copy log files.	Mail or copy log files if requested to do so by Cisco Support after you report abnormal Software Management behavior. Delete unnecessary log files after mailing or copying them.	Select Resource Manager Essentials > Software Management > Job Management > Mail or Copy Log File.
Browse history.	Generate a summary of device software upgrades stored in the history database.	Select Resource Manager Essentials > Software Management > History > Browse History.
Search history by device.	Generate a summary of software upgrades for selected devices.	Select Resource Manager Essentials > Software Management >History > Search History by Device.
Search history by user.	Generate a summary of software upgrades performed by a particular user.	Select Resource Manager Essentials > Software Management > History > Search History by User.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 107
Doc 3702

16.5.21
2

Table 2-15 Software Management Tasks (continued)

Task	Purpose	Action
Browse bugs.	Compare images running on Software Management supported devices in your network with the images on Cisco.com and report catastrophic and severe bugs specific to your network. Identify devices running deferred software images.	Select Resource Manager Essentials > Software Management > Bug Reports > Browse Bugs.
Schedule a Browse Bugs job.	Specify the date, time, and frequency of a Browse Bugs job. Cancel a scheduled Browse Bugs job.	Select Resource Manager Essentials > Administration > Software Management > Schedule Browse Bugs Job.
Browse bugs by device.	Generate a summary of software image bugs for a group of devices.	Select Resource Manager Essentials > Software Management > Bug Report > Browse Bugs by Device.
Locate devices by bugs.	Search for known bugs that could affect the devices on your network.	Select Resource Manager Essentials > Software Management > Bug Report > Locate Devices by Bugs.
Update upgrade information.	Update the source for upgrade knowledge base files. The source can be either Cisco.com or a local file.	Select Resource Manager Essentials > Administration > Software Management > Update Upgrade Info.

Syslog Analysis

The Syslog Analysis application lets you centrally log and track system error messages from Cisco devices. Use logged error message data to analyze router and network performance. You can store a maximum of 1 million messages for up to 14 days.

Before you can use Syslog Analysis, you must configure your devices to forward messages either to the Essentials server directly or to a system on which you have installed a Syslog Analyzer Collector (SAC).

RQS nº 03/2005 CN
CPMI CORREIOS
Fls. Nº 108
3702
Doc.

The collector filters and forwards the messages to the Essentials server. For more information on configuring network devices for Syslog Analysis, and for installing a remote SAC, see the online help.

New Features of Syslog Analysis

The Syslog Analysis application has the following new features:

- You can now store syslog messages in the database for a maximum of 14 days, including today (**Resource Manager Essentials > Administration > Syslog Analysis > Change Storage Options**).

  For details, see the Essentials online help.
  (In the left navigation pane of the Essentials online help, select **Resource Manager Essentials > Syslog Analysis > Administrative Procedures > Changing Storage Options**)

- You can back up the purged syslog messages at a location that you have specified (**Resource Manager Essentials > Administration > Syslog Analysis > Change Storage Options**). The messages will be stored in the CSV format.

  If you choose to back up the purged messages, you will also be allowed to select the size of the backup file. You can also specify the email addresses, for receiving an email notification, after the backup file crosses the size limit that you have specified.

  For details, see the Essentials online help.
  (In the left navigation pane of the Essentials online help, select **Resource Manager Essentials > Syslog Analysis > Administrative Procedures > Changing Storage Options**)

- The Remote Syslog Analyzer Collector (RSAC) now avoids restart, by sensing the reboot of its specified server.

  When the server goes down, the RSAC goes into the polling mode and re-connects automatically when its specified server restarts. When the server is down RSAC sends the messages to a local log file. The default location for this log file is the RSAC installed directory.

  For details, see the Essentials online help.
  (In the left navigation pane of the Essentials online help, select **Resource Manager Essentials > Syslog Analysis > Administrative Procedures > Remote Syslog Analyzer Collector (RSAC)).**

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 109
Doc 3702

16,519
L

Syslog Analysis Functional Flow

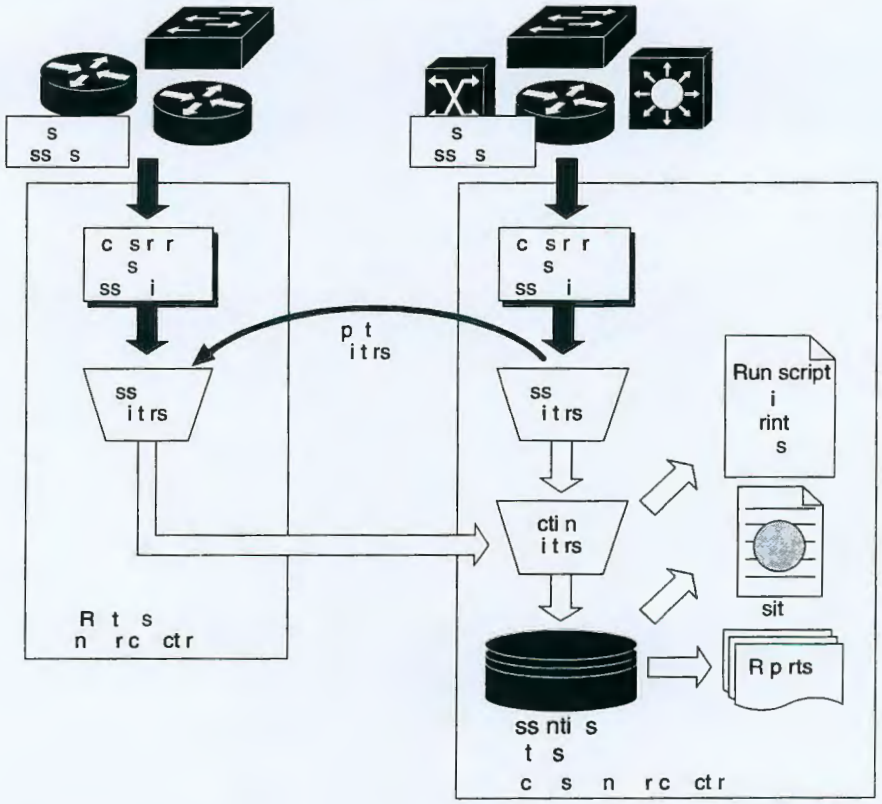
To use the Syslog Analysis features, devices must be configured to forward syslog messages to the Essentials server. When devices are configured correctly, all syslog messages will be forwarded to the Essentials server or a remote SAC.

These messages are stored on the server and are periodically read by the Syslog Analyzer process (approximately every 30 seconds). The Syslog Analyzer reads and processes the messages in the Syslog file, applies any filters that have been defined, and writes remaining messages to the Essentials Syslog message database. All syslog messages that can be read, and that are not filtered out, will be written to the Essentials Syslog database. The database is then used to produce Syslog reports and initiate user-defined scripts.

To reduce the load on the network and the CiscoWorks Server, SACs can be configured on remote workstations to collect and periodically forward syslog messages to the Essentials server. Any filters that have been defined on the Essentials server will be synchronized on SACs during scheduled updates. See Figure 2-18.

RQS nº 03/2005 - CN
CPMI - CORREIOS
-Fls Nº 110
Nº
Doc 3702

Figure 2-18 Syslog Analysis Functional Flow



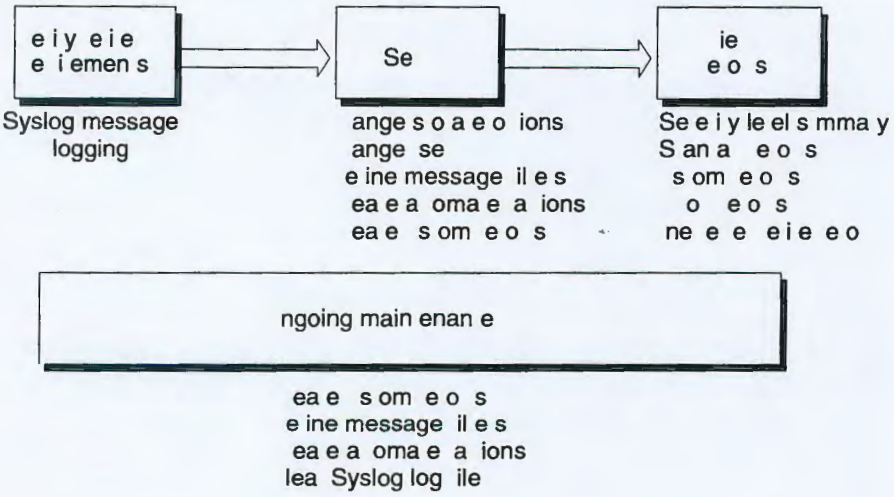
Syslog Analysis on Windows

Since system message logging is not part of the Windows operating system, CiscoWorks adds a logging service—CMF Syslog Service, when it is installed on Windows systems. All system messages are stored in the Syslog.log file under the ciscoworks/log directory on the server. The Syslog Analyzer then reads this file to populate the syslog database. See Figure 2-19.

RQS nº 03/2005 - CN
CPMI CORREIOS
Fls Nº 111
Nº 3702
Doc

Syslog Analysis Workflow

Figure 2-19 Syslog Analysis Workflow



The above chart depicts the Syslog Analysis workflow and associated tasks within Essentials. Syslog Analysis will automatically store any supported syslog messages that are forwarded from devices. You must ensure that devices are configured to forward messages to the Essentials server or a remote SAC.

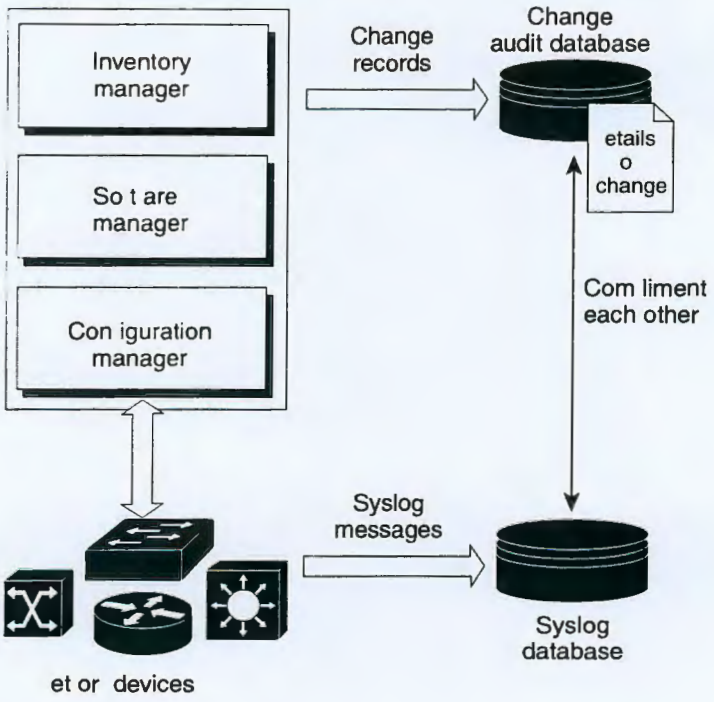
After the devices are configured properly, you can view Syslog reports at any time. You are required to perform Syslog Analysis setup tasks only if you want to filter out specific syslog messages, change how long syslog messages are stored, display syslog messages in a custom URL, group syslog in a custom report, or execute a user-defined script when specified syslog messages are detected.

Syslog Vs. Change Audit

Many actions that trigger change audit records will also trigger generation of syslog messages. Change Audit complements syslog message logging by providing additional details about some changes, tracking changes for devices, and providing multiple ways to organize and view changes to network devices. See Figure 2-20.

RQS nº 03/2005 CN
CPMI CORREIOS
Fls Nº 112
Doc. 3702

Figure 2-20 Syslog Analysis Vs. Change Audit Workflow



Changes in the network, such as a configuration change or the upload of a new Cisco IOS software image, can result in a device triggering a syslog message.

Some of these syslog messages in turn cause the inventory or the configuration management applications to poll the device and update the Essentials data appropriately. These applications will also log a record with the change audit application.

Besides, if the inventory or the configuration management applications independently detect changes to the network, they will poll the device, update the Essentials data, and log a change audit record.

For example, when a device sends a syslog message about a change in device configuration, this is passed on to Configuration Management, which determines the exact nature of the change. It retrieves the new configuration file, and then writes a change record into the Change Audit log.

RQS nº 03/2005 CN
CPMI CORREIOS
Fls. Nº 113
Doc 3702

Table 2-16 shows the tasks you can accomplish with the Syslog Analysis application.

Table 2-16 Syslog Analysis Tasks

Task	Purpose	Action
Set up data storage options.	Configure how long to store data, the maximum number of messages to store, and the message source. You should restart daemon manager and CMF Syslog Service (CRM Logger) for the Message Source changes to take effect. If you want to back up the purged data, you can specify the back up details—the backup directory, backup file size, email address for notification when the backed up file exceeds the specified size, etc.	Select Resource Manager Essentials > Administration > Syslog Analysis > Change Storage Options.
Define custom reports.	Create new reports and select the message types to be included in each report. Modify the standard reports provided with Essentials Delete reports that you no longer use. You can also enable 24-hour reporting.	Select Resource Manager Essentials > Administration > Syslog Analysis > Define Custom Reports.
Define automated actions.	Add and modify command-line instructions to be executed automatically whenever Syslog Analyzer receives a specific message type. Modify existing actions and delete actions you no longer use. You can also enable or disable actions.	Select Resource Manager Essentials > Administration > Syslog Analysis > Define Automated Action.
Define message filters.	Exclude messages you do not want reported. Enable or disable filtering. Modify or delete filters.	Select Resource Manager Essentials > Administration > Syslog Analysis > Define Message Filter.

RQS nº 03/2005 - CN
CPMI - CORREIOS
114
Fls Nº
Doc 3702

Table 2-16 Syslog Analysis Tasks (continued)

Task	Purpose	Action
View status.	View the status of your Syslog Collector. You can view the status of the local and all the remote collectors that have been configured to use the Essentials server as the forwarding server.	Select Resource Manager Essentials > Administration > Syslog Analysis > Syslog Collector Status.
Change your URL.	Link your message reports to a customized web page. You can do this only if you know basic CGI programming.	Select Resource Manager Essentials > Administration > Syslog Analysis > Change User URL.
Generate a severity level summary.	Generate summaries of messages about selected devices sorted by severity level.	Select Resource Manager Essentials > Syslog Analysis > Severity Level Summary.
Generate a standard report.	Generate a system message report for a device or a set of devices. You can generate the report for the current date, or for any date in the previous week, or for all dates. You can include all the messages, or choose the severity level or alert type for which the report should be generated.	Select Resource Manager Essentials > Syslog Analysis > Standard Reports.
Generate a custom report.	Generate a full custom syslog report. You can select a report from the custom syslog reports that are defined in Administration.	Select Resource Manager Essentials > Syslog Analysis > Custom Reports.
	Generate a summary custom syslog report. You can see a summary of the various reports.	Select Resource Manager Essentials > Syslog Analysis > Custom Report Summary.
Generate a report for unmanaged devices.	Generate a syslog information report on all unmanaged devices in your network.	Select Resource Manager Essentials > Syslog Analysis > Unexpected Device Report.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 115
Doc. 3702

Table 2-16 Syslog Analysis Tasks (continued)

Task	Purpose	Action
Generate a report for workflow devices.	Capture syslog messages that are generated from MCS servers running WF application.	Select Resource Manager Essentials > Syslog Analysis > WorkFlow Report.
Generate a 24-hour syslog report.	Generate a report for the past 24 hours. The report can be a custom report created by a system administrator or a default report.	Select Resource Manager Essentials > 24-Hour Reports > Syslog Messages.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 116
Doc. 3702

For more details about:

- Enabling the job password policy, see the Essentials online help. (In the left navigation pane of the Essentials online help, select **Resource Manager Essentials > Configuration Management > Configuration Management Administration > Password Policy for NetConfig, Config Editor and NetShow Jobs**).
- Job password for Config Editor jobs, see the Essentials online help. (In the left navigation pane of the Essentials online help, select **Resource Manager Essentials > Config Editor > Config Editor Tasks > Configuring Job Properties**).
- Usage Scenarios when the job password is configured on devices, see the Essentials online help. (In the left navigation pane of the Essentials online help, select **Resource Manager Essentials > Configuration Management > Configuration Management Administration > Usage Scenarios When Job Password is Configured on Devices**).

Multiple Selection of Jobs for Deletion

You can now select more than one job at a time, for deletion from the Job Browser.

For details, see the Essentials online help.
(In the left navigation pane of the Essentials online help, select **Resource Manager Essentials > Config Editor > Config Editor Tasks > Working with Files > Displaying the Job Status**).

Separate Protocol Ordering for Configuration Download and Fetch Operations

For Config Editor jobs, you can now use your preferred transport protocols, separately, for downloading configurations, and for fetching configurations.

For example, you can use Telnet to download configuration to the device, and TFTP to fetch the configuration, thus improving the overall performance of Config Editor.

For downloading the configurations, the protocols used are Telnet and SSH.

The default order is,

- Telnet
- SSH (Secure Shell)

RQS nº 03/2005 - CN
CPMI CORREIOS
Fls Nº 117
Doc 3702

For fetching the configurations, the protocols used are Telnet, TFTP, SSH, and rcp. The default order is,

- TFTP (Trivial File Transport Protocol)
- Telnet
- rcp (remote copy protocol)
- SSH (Secure Shell)

You can change the transport protocol order for both downloading and fetching the configurations.

You can select the fallback option for these protocols. If you select this option, and the first preferred protocol fails, the next protocol in the list is used for configuration download or fetch operations.

For details, see the Essentials online help.
(In the left navigation pane of the Essentials online help, select **Resource Manager Essentials > Configuration Management > Configuration Management Administration > Setting the Transport Protocol Order for NetConfig, Config Editor and NetShow Jobs**).

Support for Interactive Commands

Interactive commands can be edited using Config Editor.

For example, you can enter an interactive command in the Enter CLI Commands area, using the following syntax:

CLI Command<R>*command response 1* <R>*command response 2*

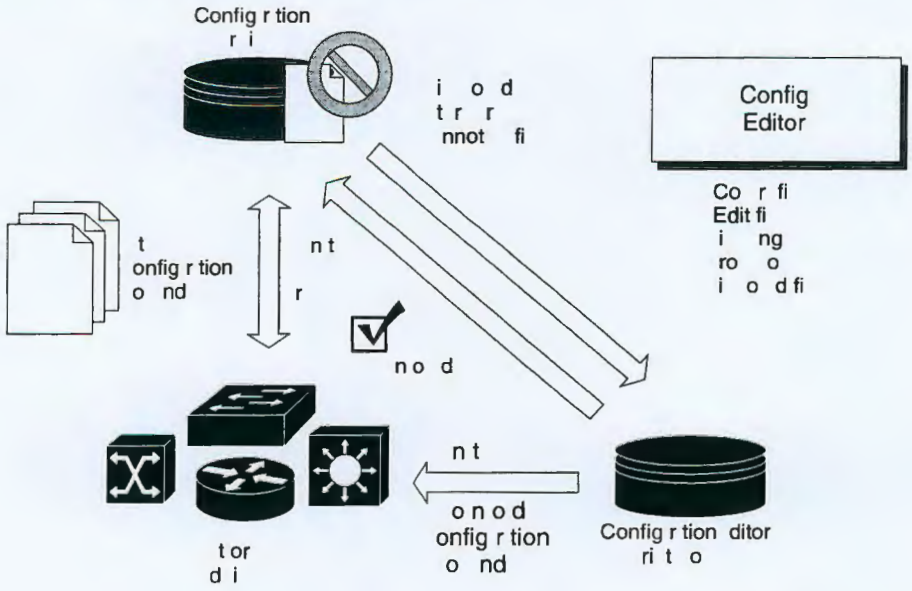
Benefits of Config Editor

Config Editor allows you to edit and download configuration files to devices using a GUI instead of the command line interface (CLI). Use Config Editor to edit individual device configurations within Essentials and then download them back to a device. A copy of the updated configuration will automatically be stored in the Configuration Archive.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 118
Doc
Nº 3702

When a configuration file is opened with Config Editor, the file is locked so that other users will not be able to make changes at the same time. While the file is locked, it is maintained in a *private* archive available only to the user who checked it out. If other users attempt to open the file to edit it, they will be notified that the file is already checked out and they can open only a *read only* copy. The file will remain locked until it is downloaded to the device or manually unlocked within Config Editor. See Figure 2-11.

Figure 2-11 Config Editor Functional Flow



Note Many applications rely on access to configuration file within the Configuration Archive (NetConfig, ACL Manager). Hence, you must ensure that all files have been unlocked before exiting Config Editor.
Select **Resource Manager Essentials > Configuration Management > Config Editor > Tools > List Checked Out Files** before exiting Config Editor to get a list of files that have to be checked in.

RQS nº 03/2005 CN
CPMI CORREIOS
Fls Nº 119
Doc 3702

16.549

Table 2-10 shows the tasks you can accomplish with the Config Editor option.

Table 2-10 Config Editor Tasks

Task	Purpose	Action
Edit configuration files from the archives.	Check out a file from the archive, and edit it.	Select Resource Manager Essentials > Configuration Management > Config Editor > File > Open.
Schedule download jobs.	Define and schedule a download job.	Select Resource Manager Essentials > Configuration Management > Config Editor > File > Download.
Print configuration files.	Print a configuration file.	Select Resource Manager Essentials > Configuration Management > Config Editor > File > Print.
Configure job policies.	Configure a default policy for job properties that applies to all future jobs. You can also specify if the property can be configured by other users.	Select Resource Manager Essentials > Configuration Management > Config Editor > Edit > Set Job Policies.
Set up editing preferences.	Set up your editing preferences. Config Editor remembers your preferred mode even across different invocations of the application. After you open a file in a specific mode, you can view it only in that mode until you unlock it.	Select Resource Manager Essentials > Configuration Management > Config Editor > Edit > Preferences.
View changes.	View the changes to the checked out file. Essentials compares the current file with the checked out version.	Select Resource Manager Essentials > Configuration Management > Config Editor > Tools > Show Changes Made.
Compare versions of the configuration files.	Compare the current file with any version in the Configuration Archive.	Select Resource Manager Essentials > Configuration Management > Config Editor > Tools > Compare.
Enter comment lines.	Enter comment lines while editing a configuration file.	Select Resource Manager Essentials > Configuration Management > Config Editor > Tools > Insert Comment Line.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 120
Doc. 3702

Table 2-10 Config Editor Tasks (continued)

Task	Purpose	Action
List checked out files.	View a list of files checked out by all users.	Select Resource Manager Essentials > Configuration Management > Config Editor > Tools > List Checked Out Files.
Browse and edit Config Editor jobs.	Browse the Config Editor jobs that are registered on the system and edit them as necessary.	1. Select Resource Manager Essentials > Configuration Management > Config Editor > Tools > Job Browser. 2. Select a job record. 3. Click Edit Job, Copy Job, Remove Job, Stop Job, or Job Details.
View job details.	View detailed information about a registered Config Editor job. You can also edit a job from its detailed view.	1. Select Resource Manager Essentials > Configuration Management > Config Editor > Tools > Job Browser. 2. Select a job record. 3. Click Job Details. 4. Click Edit Job, Copy Job, Remove Job, Stop Job, or Print Job.

Contract Connection

Contract Connection lets you verify which of your Cisco IOS devices are covered by a service contract, and when they will expire. Contract Connection uses Inventory Manager, Cisco Connection Online (Cisco.com) and Contract Agent, Cisco's internal tracking service, to provide the status of your service coverage.

To view contract status, however, you must have login privileges to the Cisco.com web site and a Cisco.com profile that enables access to the Contract Agent.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 121
Doc. 3702

Contract Connection Workflow

Contract Connection checks the devices in your Essentials Inventory against devices logged in the Cisco Contract Agent and displays a summary. You can also view a detailed report on the contract status, which shows when the contract was initiated and when it will expire.

Three different serial numbers can be associated with a device. This determines how Contract Connection works:

- Shipment serial number—The number tagged on the device when it is shipped from Cisco. Also the number logged in the Cisco Contract Agent.
- Managed serial number—The number stored in the Essentials Inventory database. It is entered or retrieved from the device when a device is added or imported into the database.
- Electronic serial number—The number stored in the device MIB. It can be set or modified through the command line interface (CLI) on the device.

For Contract Connection to work properly and display contract details, the managed serial number in the Essentials Inventory must match the shipment serial number logged with the Cisco Contract Agent. If these numbers do not match, select **Resource Manager Essentials > Administration > Inventory > Change Device Attributes**, to edit the serial numbers.

Table 2-11 shows the task you can accomplish with the Contract Connection application.

Table 2-11 Contract Connection Task

Task	Purpose	Action
Check the status of a contract.	Check which of your Cisco IOS managed devices are covered by a service contract and review contract details.	Select Resource Manager Essentials > Contract Connection > Check Contract Status.

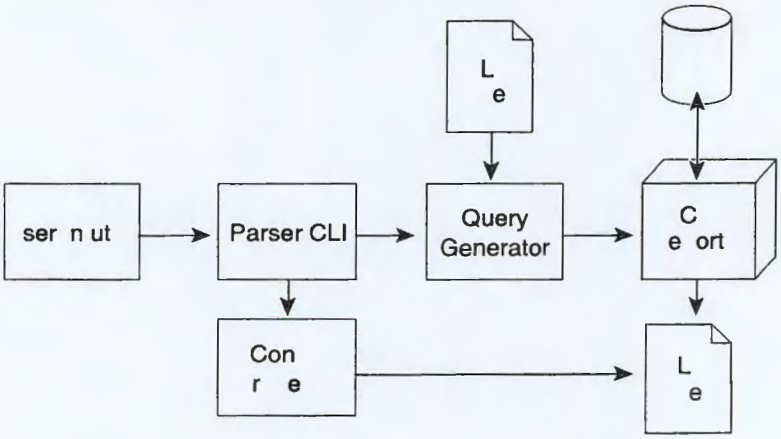
Data Extracting Engine (DEE)

Data Extracting Engine (DEE) is a tool that enables you to extract detailed device inventory and running configuration information in XML format from the Essentials server. See Figure 2-12.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 122
Doc. 3702

16.546
2

Figure 2-12 Data Extracting Engine Functional Flow



Using DEE, you can extract data, in the following ways:

- Through a command line utility
- Through a servlet utility, which can be accessed by any client script through HTTP or HTTPS.

Benefits of Data Extracting Engine

DEE has the following benefits. You can:

- Generate inventory data in the XML format.
  DEE has servlet access and command line utilities that can generate inventory data for devices managed by the Essentials server.
- Generate configuration data in XML format.
  DEE uses existing Configuration Archive APIs and generates latest configuration data from the Configuration Archive in XML format. Elements in the XML file are created at the configlet level in the current Configuration Archive. Predefined rules that currently exist in the Configuration Archive are used to get the configlets data. The exported data contains the entire running configuration data.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 123
Doc 3702

- Archive XML Data.
  By default, the data generated through CLI is archived at the following location:

  For Inventory,

  PX_DATADIR/archive/cwexport/*timestamp*inventory.xml

  For Config,

  PX_DATADIR/archive/cwexport/*timestamp*config.xml

  Where *PX_DATADIR* is the *NMSROOT*/files directory, and *NMSROOT* is the Essentials installed directory.

  You can also specify a directory to store the output. This application does not have a feature to automatically delete the files created in the archive. You should manually delete the files when necessary. While generating data through the servlet, the output will be displayed in the client terminal.
- Generate and download inventory and configuration data in XML format using the servlet.
  You have to upload a payload XML file, which contains the cwexport command options and CiscoWorks user credentials. You have to write your own script to invoke the servlet with a payload of this XML file and the servlet returns the exported file in XML format, if the credentials are correct and options are valid.
  For details of payload XML file, see the DEE online help.

Device Navigator

Device Navigator lets you access a device that has a Hypertext Transfer Protocol (HTTP) server enabled, directly from a Web Browser. You can select a device and go to the device home page to perform some operations typically performed by Telnet and CLI. You must have the appropriate permissions to access these features.

All Cisco routers and access servers with Cisco IOS 11.0(6) or later have an embedded HTTP server that allows you to access the device from a Web Browser.

From the device web page, you can view the configuration and connectivity information, and even modify the device configuration.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 124
Doc. 3702

The Device Navigator allows you to connect to the HTTP server on a device directly from Essentials.

In order to utilize this feature, the HTTP server must be enabled on the device. TTP server is 80.

To enable the HTTP server, use the following Cisco IOS global configuration command:

```
router(config)# ip http server
```

To change the default port used to access the device Web page, use the following global configuration command:

```
router(config)# ip http port number
```

Table 2-13 shows the tasks you can accomplish with the Device Navigator application.

Table 2-12 Device Navigator Tasks

Task	Purpose	Action
Browse Device	Allows you to access a device that has a Hypertext Transfer Protocol (HTTP) server enabled, directly from a Web Browser.	Select Management Connection > Device Navigator > Browse Devices.
Configure Fallback Port.	Enables you to configure a fallback port. Typically, the HTTP server for a device is configured to run on port 80. However, you can configure it to run on any port.	Select Management Connection > Device Navigator > Configure Fallback Port.

Benefits of Device Navigator

With the Device Navigator you can:

- Browse Devices
- Configure a Fallback Port

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 125
Doc 3702

Browse Devices

When the HTTP server is enabled on a device, you can use the Device Navigator to display the device home page in Essentials:

1. Select **Management Connection > Device Navigator > Browse Device** from the CiscoWorks desktop.
2. Select the required device, and click **Next.**

   The Device Login dialog box appears.
3. Enter the enable password to access the device and click **OK**. You do not need to enter a username.

   The home page for the device appears.

The device home page provides links to the following configuration and connectivity information:

Telnet	Opens a telnet sessions
Show Interfaces	Displays command output
Show Diagnostic Log	Displays show logging command output
Monitor the router	Provides drill-down menus to execute configuration commands
Connectivity test	Pings the device
Show Tech Support	Displays the command output

There are also links to additional resources and Cisco tech support information at the bottom of the Web page.

Configure a Fallback Port

Typically the HTTP server for a device is configured to run on Port 80. However you can configure the HTTP server to run on any port, in case Port 80 is used by another service.

When browsing the device, the Device Navigator will attempt to connect to Port 80 first.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 126
Doc 3702

If this fails, Device Navigator attempts to connect to the fallback port, if one has been configured in Essentials.

To select a fallback port for Device Navigator, select **Management Connection > Device Navigator > Configure Fallback Port** from the CiscoWorks desktop.

Inventory

Networks are a mix of heterogeneous and geographically dispersed systems. Tracking of hardware and software assets in such an environment is very critical. Inventory details are essential as a basic requirement for all network management applications.

Having all the information about all of your devices in a central place, makes it easier to locate necessary information, resolve problems quickly, and provide detailed information to interested parties.

New Features of Inventory

The Inventory application has the following new features:

- The length of the user fields (**Resource Manager Essentials > Administration > Inventory > Add Device**) has been increased to contain 128 characters. You can now use these fields to enter specific notes about the device. For example, you can enter information about the device, such as, its location, the contact person for the device, the asset tag of the device, etc.
- You can customize the labels for the user fields (**Resource Manager Essentials > Administration > Inventory > Add Device**) by editing the mapping.properties file.

  The mapping.properties file is in *NMSROOT*/htdocs.

  The changes that you make to these field labels are reflected in the:

  - Inventory reports (In the Custom Reports, Hardware Reports, Software Reports, Chassis Slot Details Reports and MultiService Port Details Reports).
  - GUI (In the GUI for Add Devices, Change Device Attributes, and in the Custom Reports search criteria field selection GUI).

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 127
Doc. 3702

For example, in the mapping.properties file, you can change the user fields to show meaningful names in the reports and in the GUI, as follows:

- User Field 1 = Purchase Date
- User Field 2 = Price
- User Field 3 = Vendor
- User Field 4 = Contract Details

For details, see the Essentials online help.
(In the left navigation pane of the Essentials online help, select **Resource Manager Essentials > Inventory > Add, Import, and Delete Devices > Adding Devices.** In this topic, Step 2 of Procedure, click the link, "device access, user, and serial number".

Benefits of Inventory Management

As a network administrator, you need to be able to quickly troubleshoot problems on the network, identify when network capacity is being reached, and provide information to management on the number and types of devices being used on the network. If the network goes down, one of the first things you will need to know is what devices are running on the network.

Most Essentials tasks are performed against a set of devices. Hence, information about a particular device must be available in the Essentials database. Inventory Manager is used to specify which devices to manage.

Since Essentials takes advantage of many different management services to collect device information (for example, SNMP, TFTP, Telnet), each device placed into the Essentials database (Inventory) must include the necessary parameters (device attributes) for various management services (community strings, passwords). When this information is included in the Essentials Inventory, the device is considered to be managed by Essentials, and data collection from the device takes place.

Therefore, nothing happens in Essentials until the devices and their attributes are included in the inventory. Inventory Manager is the starting point for all Essentials applications.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 128
Doc. 3702

16.940
2

When devices are added to Essentials, Inventory Manager (and other applications within Essentials) proceed to contact the device and collect necessary information to be stored in the database. Inventory Management can now be configured to automatically poll devices on the network to look for any changes.

If any changes are detected in hardware or software components, the inventory database will be updated and a change audit record will be created to inform the network manager of the change, and to document the event. This helps to ensure that the information displayed in the Inventory reports reflects the current state of network devices.

The Inventory application lets you:

- Import devices from databases or files.
- Export device information to files.
- Add, delete, change, and list devices in your network inventory.
- Delete devices listed in a CSV file
- Poll, update and schedule collection on devices to update your network inventory.
- Display reports and graphs of your hardware and software inventory and create Inventory custom reports.
- Check and change device attributes.
- Display a Year 2000 compliance report.
- Change system-wide configuration for SNMP, SMTP, proxy and rcp settings.
- Allow other network management systems to manipulate Essentials devices.

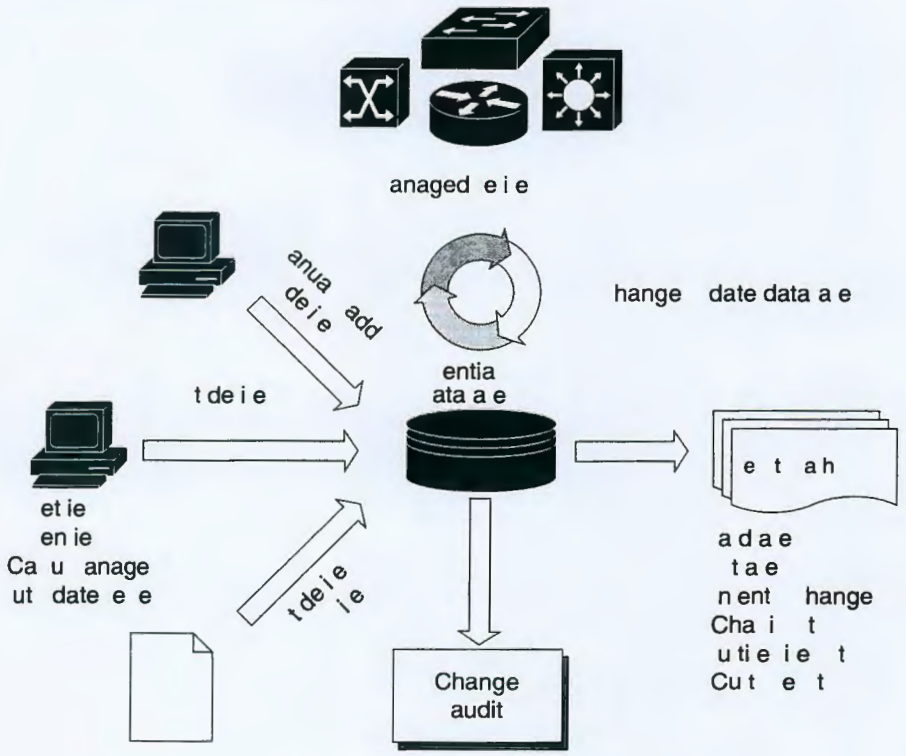
Inventory Management Functional Flow

To use Essentials at its full potential, the device attributes of the devices in the network must be included in the Inventory. Essentials does not auto–discover devices on the network. Devices must be manually added or imported into the Inventory database before information can be displayed in reports.

To simplify the process of populating the Inventory database, device information can be imported from a supported network management system, such as HP OpenView, or from a formatted text file. Essentials can also import the device data directly from Campus Manager Topology Services, which can auto–discover devices. For detailed information, see *User Guide for Campus Manager.*

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 129
Doc 3702

Figure 2-13 Inventory Management Functional Flow



You can use the various tasks in the Inventory Manager to populate the database, start tracking any changes to the inventory, and produce inventory reports. The database or inventory population is also the starting point for using other Essentials applications. See Figure 2-13.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 130
Doc 3702

Figure 2-14 Inventory Management Workflow

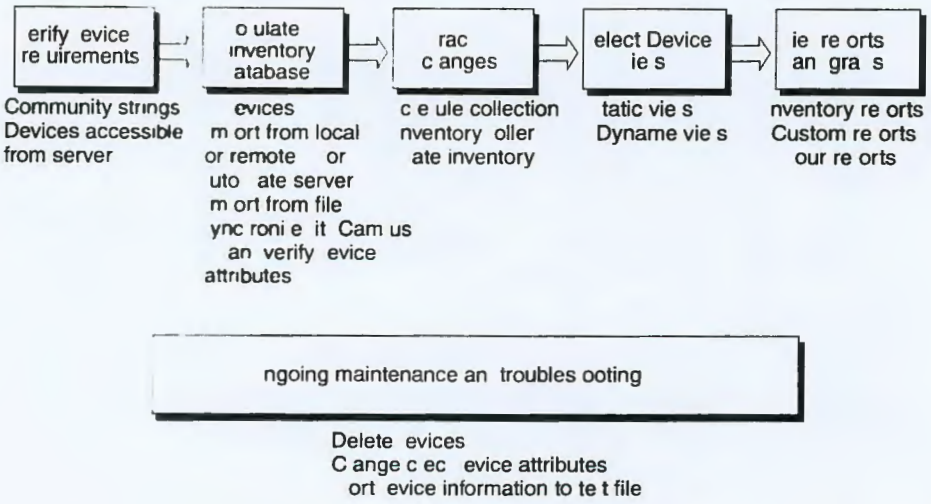


Figure 2-14 depicts the Inventory Management workflow and Essentials tasks:

- Verify device requirements to ensure that Essentials is able to communicate with the devices.
- Add or import device information into the Essentials database. An extremely important part of this step is associating device attributes with the imported or added devices. These attributes include the device community strings and appropriate passwords. These are required parameters for many of the management services (for example SNMP, Telnet) used by the various Essentials applications.
- Schedule periodic polling of devices to track changes, and keep the database up-to-date.
- Create device views to facilitate running of reports against numerous associated devices at one time.

Note The network administrator should perform ongoing maintenance, such as deleting devices that are no longer on the network, and checking device attributes to ensure that login and Telnet authentication information is correct in the Inventory database.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 131
Doc 3702

16.537
2

Table 2-13 shows the tasks you can accomplish with the Inventory application.

Table 2-13 Inventory Manager Tasks

Task	Purpose	Action
List managed devices.	Determine whether a particular device is managed by displaying devices that have inventory data.	Select Resource Manager Essentials > Administration > Inventory > List Devices.
Add devices.	Add devices individually by specifying basic device information for each.	Select Resource Manager Essentials > Administration > Inventory > Add Devices.
Import devices from a file.	Import devices in bulk from a comma separated values (CSV) file or a data integration file (DIF) instead of adding them individually.	Select Resource Manager Essentials > Administration > Inventory > Import from File.
Import device data from a local host.	Import device data from a supported network management system (NMS) database residing on the local host. Device import supports these NMS databases: • HP OpenView (Solaris, and Windows only) • Cisco WAN Manager (Solaris only) • Tivoli NetView (Solaris, and Windows only)	Select Resource Manager Essentials > Administration > Inventory > Import from Local NMS.

RQS nº 03/2005 CN
CPMI CORREIOS
Fls Nº 132
Doc 3702

16.536
L

Table 2-13 Inventory Manager Tasks (continued)

Task	Purpose	Action
Import device data from a remote host.	Import device data from a supported NMS database residing on a remote host. Device import supports these NMS databases: • CiscoWorks for Switched Internetworks (CWSI) • HP OpenView • Cisco WAN Manager (Solaris only) • Tivoli NetView (running on remote Solaris hosts only)	Select Resource Manager Essentials > Administration > Inventory > Import from Remote NMS.
Proxy Management	Import devices from AutoUpdate Server	Select Resource Manager Essentials > Administration > Inventory > Proxy Management.
Check status of import from local host, remote host, or file.	Determine whether a device import was successful and rectify the import if the device remains unmanaged.	Select Resource Manager Essentials > Administration > Inventory > Import Status.
Delete managed devices.	Delete managed devices, including all the related device information, that you no longer track.	Select Resource Manager Essentials > Administration > Inventory > Delete Devices.
Delete devices from a file.	Delete a group of devices from a comma separated values (CSV) file instead of deleting them individually.	Select Resource Manager Essentials > Administration > Inventory > Delete from File.
View status of deleted devices.	View the status of deleted devices and see which ones are in a suspended state.	Select Resource Manager Essentials > Administration > Inventory > Delete Device Status.

RQS nº 03/2005 - CN
CPMI CORREIOS
Fls. Nº 133
Doc 3702

Table 2-13 Inventory Manager Tasks (continued)

Task	Purpose	Action
Change device attributes.	Change these device attributes on selected devices: • SNMP read and write community strings • Telnet passwords • TACACS usernames and passwords • Enable TACACS usernames and passwords • Enable secret passwords • Local usernames and passwords • User fields • Device serial numbers	Select Resource Manager Essentials > Administration > Inventory > Change Device Attributes.
Export devices to a file.	Export your device and device access information to an output file in CSV or DIF format.	Select Resource Manager Essentials > Administration > Inventory > Export to File.
Exporting Data for AVVID Tool	AVVID Solution Analysis Tool provides a feature that allows you to export data from the Essentials inventory database. This option allows you to export the data in the format required by AVVID Solution Analysis Tool for analysis.	Select Resource Manager Essentials > Administration > Inventory > Export Data for AVVID Tool.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 134
Doc 3702

16 547
L

Segurança Tipo 1 doc 6

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 135
Doc 3702

Resource Manager Essentials Applications

This chapter lists all the Essentials applications and the tasks that can be accomplished with each of these applications. The applications are:

- Device Views
- Availability
- Change Audit
- Configuration Management
- Contract Connection
- Case Management
- Data Extracting Engine (DEE)
- Device Navigator
- Inventory
- Job Approval
- Software Management
- Syslog Analysis

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 136
Doc 3702

Device Views

Essentials provides device views—logical groupings that are used to specify a device or group of devices. You can define views to group selected devices into logical groups. Device views allow you to quickly view reports on all devices of a certain type, or with specific characteristics, such as all Catalyst switches or all devices that you are responsible for.

Since almost every Essentials task requires the set of devices to be executed against, views provide a convenient way to create groups of devices. For example, before you can display an Inventory report, you must select the devices to be included in the report. Views can speed up the selection (instead of running the report for one device at a time).

Note Essentials graphical user interface (GUI) performance may be affected if the number of devices in the selected view is too large. You should avoid setting *all devices* views when the number of devices in the inventory is large. You can use system views or create custom views to keep the number of devices in a view from growing too large.

Creating a view using the Device Views application enables you to run reports for specific devices based on common attributes or user-defined characteristics.

Types of Views

Three categories of device views are available:

- System Views—Predefined and available immediately after you install Essentials. System views include most major classes of Cisco devices. For example all Catalyst switches, all Cisco 7000 Series routers, and all SwitchProbes.
- Custom Views—Defined by users and, when created, are available for use by anyone with the appropriate access to the server.
- PrivateViews—Defined by users, but are available only to the user.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 137
Doc 3702

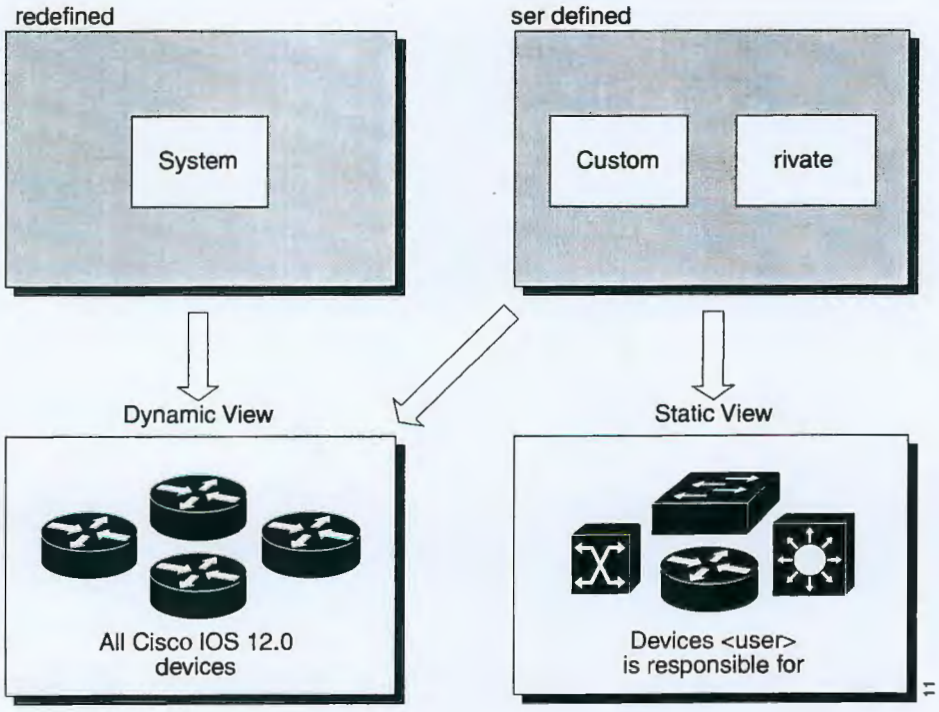
Two different types of views can be created within custom or private views:

- Dynamic Views
- Static Views

Dynamic views are logical groups based on device attributes, such as device class or software version. The devices in a dynamic view can change based on the attribute value of devices in the Inventory. An example of a dynamic view is all devices with Cisco IOS Version 12.0. Any device that currently has this attribute would be included in the device view. All system views are dynamic.

Static views are logical groups based on user-defined characteristics. Static views include any devices that you add to the view. The members of the group do not change unless you manually add or remove devices. Use static views when you do not want the membership to change automatically. See Figure 2-1.

Figure 2-1 Device Views



RQS nº 03/2005 - CN
CPMI CORREIOS
Fls Nº 138
Doc. 3702

Table 2-1 shows the tasks that you can accomplish with the Device Views application.

Table 2-1 Device Views Tasks

Task	Purpose	Action
Add static views.	Create views to monitor a specific group of devices in your network inventory.	Select Resource Manager Essentials > Administration > Device Views > Add Static Views.
Add dynamic views.	Create views to monitor devices with common attributes, such as device type. **Note** Any new, managed device added to inventory that fits the listed attributes, is automatically incorporated into the dynamic view.	Select Resource Manager Essentials > Administration > Device Views > Add Dynamic Views.
Change static views.	Modify static views.	Select Resource Manager Essentials > Administration > Device Views > Change Static Views.
Delete views.	Delete any views you have created.	Select Resource Manager Essentials > Administration > Device Views > Delete Views.
Browse dynamic views.	Determine which devices belong to the dynamic views.	Select Resource Manager Essentials > Administration > Device Views> Browse Dynamic Views.
Browse device membership.	Determine which views a device belongs to.	Select Resource Manager Essentials > Administration > Device Views > Browse Device Membership.

Setting Device Credentials

It is important to configure the device credentials correctly on every Cisco device that you will manage and monitor using Essentials.

Table 2-2 lists all the applications and the device credentials required for proper functioning of the applications.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 139
Nº - Doc. 3702

16592
L

Table 2-2 Applications and the Device Credentials

Application	Telnet Password	Enable Password	SNMP Read Only	SNMP Read / Write
NetConfig	Required	Required	Required	Required if configuration fetch is through TFTP
NetShow	Required	Required	Required	Not required
Config Editor	Required	Required	Required	Required if configuration fetch is through TFTP
ChangeAudit	Not required	Not required	Required	Not required
Configuration Management (Telnet)	Required	Required	Required	Not required
Configuration Management (TFTP)	Not required	Not required	Required	Required
Device Views	Not required	Not required	Required	Not required
Inventory	Not required[1]	Not required[2]	Required	Not required[3]
SWIM	Required[4]	Required[5]	Required	Required
Syslog	Not required	Not required	Required	Not required
Availability	Required	Required	Required	Not required
Case Management	Required	Not required	Required	Not required
Contract Connection	Required	Not required	Required	Not required

1. Inventory requires Telnet password to perform the check device attributes operation.
2. Inventory requires enable password to perform the check device attributes operation.
3. Inventory requires SNMP Read/Write string to perform the check device attributes operation.
4. Required in case of few devices.
5. Required in case of few devices.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 140
Doc 3702

System Configuration

System Configuration lets you configure system-wide information on the CiscoWorks server. In this way, you can centrally locate information that is used by more than one Essentials application.

Note Network administrators should perform these tasks with care. If errors occur, users may not be able to log in.

Table 2-3 shows the tasks that you can accomplish with System Configuration.

Table 2-3 System Configuration Tasks

Task	Purpose	Action
Set up a proxy URL.	Enable applications to connect to Cisco.com. If the server access to the outside world is controlled through a proxy server, this must be configured.	Select Resource Manager Essentials > Administration > System Configuration, then select the Proxy tab.
Define SNMP timeouts and retries.	Specifies the timeout value and the number of retries while querying devices for inventory collection.	Select Resource Manager Essentials > Administration > System Configuration, then select the SNMP tab.
Define the SMTP server name.	Define your Simple Mail Transfer Protocol (SMTP) server in Essentials to use e-mail, to automatically notify network administrators when certain tasks and jobs are completed.	Select Resource Manager Essentials > Administration > System Configuration, then select the SMTP tab.
Define rcp usernames.	Specify the username to authenticate rcp transfers between the devices and the server for remote operations.	Select Resource Manager Essentials > Administration > System Configuration, then select the rcp tab.

RQS nº 03/2005 - CN
CPMI CORREIOS
Fls Nº 141
Doc. 3702

Availability

The Availability application lets you monitor the reachability and response time of your network devices. You can view the availability of a selected group of devices, a summary of interface status, reports of reloads (reboots) and unreachable devices, and protocol distribution graphs.

Benefits of Availability

If you experience connectivity problems trying to reach certain resources or services on the network, one of the first things you must check is the status of a device. If a device is unreachable, you will want to find out when it was last operational and whether any abnormal reloads have occurred. This can be the first step in troubleshooting the exact location of the fault. Availability helps you track the reachability of devices on your network.

The Availability application periodically polls selected devices to determine device reachability, interface status, and response times. Availability reports display the status of devices, show devices that are offline for more than three hours, and summarize the percentage of Layer 3 protocol traffic forwarded on each Layer 3 device.

The Reloads Report shows the cause of the past five reloads for a device and includes a link to the Cisco.com Cisco Output Interpreter to help troubleshoot any device failures. Availability provides reports to quickly assess the status of selected devices on the network. Information can be tracked for all devices on the network, or only critical devices to reduce the load on the network and the network management system.

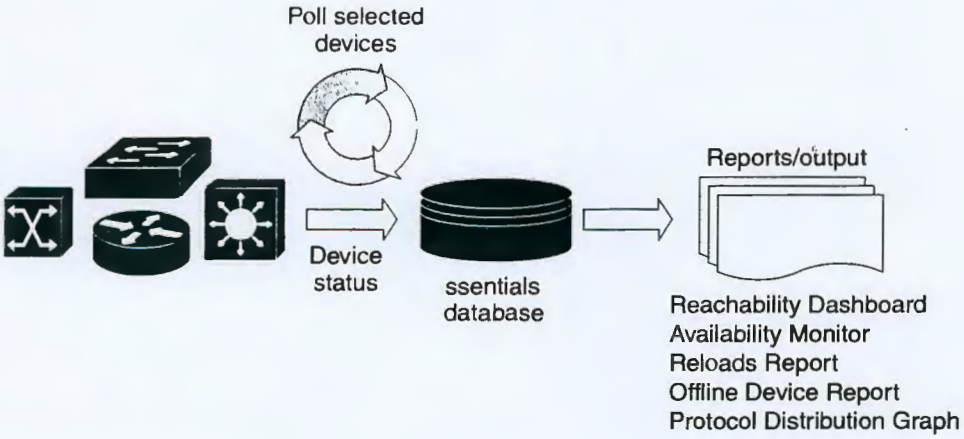
Availability Functional Flow

Before device availability information will be stored in Essentials, you must select the specific device views that needs to be monitored for Availability. When devices are selected to be included in Availability polling, Essentials will poll the devices according to the schedule set by the network administrator (only one schedule for all views). Devices will be polled for reachability, response time, interface status, reload, and protocol information.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 142
Doc 3702

This information will be updated in the Availability database after each scheduled poll, and can be viewed by displaying Availability Reports. Historical information on reachability and response times is also stored in the Essentials database and can be displayed in trend graphs under Availability Monitor. See Figure 2-2.

Figure 2-2 Availability Functional Flow



Availability Workflow

Figure 2-3 depicts the Availability workflow and associated tasks within Essentials:

- In order to retrieve Availability information from devices, each device must be in the Essentials Inventory with the proper SNMP read community string attribute.
- Polling options must be set, including selecting which device views are going to be polled for availability information. When devices are selected, availability information can be viewed in any of the Availability Reports within Essentials. Information is automatically purged according to the options you set, so no ongoing maintenance is required.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 143
Doc 3702

Figure 2-3 Availability Workflow

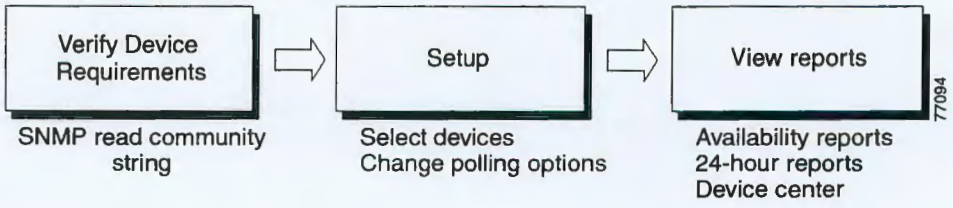


Table 2-4 shows the tasks you can accomplish with the Availability application.

Table 2-4 Availability Manager Tasks

Task	Purpose	Action
Set polling views and options.	Select views to be monitored. You must do this before you can monitor device availability. If your system performance is degraded by availability polling, you can add more system resources, poll fewer devices, or poll less frequently.	Select Resource Manager Essentials > Administration > Availability > Change Polling Options.
Change polling options.	Select default Availability polling option values or to select new values from the drop-down list boxes. The polling options you set, apply to all Availability views.	Select Resource Manager Essentials > Administration > Availability > Change Polling Options.
View the Reachability Dashboard.	View device status for all views set for availability monitoring. The dashboard continuously reports: • All views being polled and the number of devices in each view. • Device names of all devices in each view and the time they last responded.	Select Resource Manager Essentials > Availability > Reachability Dashboard.
Monitor device availability.	Continuously monitor selected devices and access interface availability details.	Select Resource Manager Essentials > Availability > Availability Monitor.

RQS nº 03/2005 - CN
CPMI CORREIOS
Fls Nº 144
Doc 3702

16.537

Table 2-4 Availability Manager Tasks (continued)

Task	Purpose	Action
View the Reloads report.	Display the most recent reloads (up to 5) for selected devices. The report shows the reason for each reload and when it occurred.	Select Resource Manager Essentials > Availability > Reloads Report. To view reloads that occurred only within the past 24 hours, select Resource Manager Essentials > 24-Hour Reports > Reloads Report.
View the Cisco Output Interpreter Analysis.	Decode and analyze the device's stack dump, to enable troubleshooting of devices that reload unexpectedly. An unexpected reload is any reload that is neither initiated by you nor a result of a power-on. The Reloads report applies only to routers running Cisco IOS Release 10.2 or later and is available only for the most recent reload.	Select Resource Manager Essentials > Availability > Reloads Report. In the generated report, click on the reload reason. You may be prompted to enter your Cisco.com (CCO) username and password. See the Cisco home page to have your Cisco.com (CCO) profile updated or changed, or, after you log in, use the Cisco.com Profile button to update your Cisco.com profile.
View the Offline Device report.	Generate a report of managed devices that have not responded to polling for more than a specified period of time (3, 6, 12, 24, 48, or 72 hours).	Select Resource Manager Essentials > Availability > Offline Device Report. To view only devices that have been off line for the past 24 hours, select Resource Manager Essentials > 24-Hour Reports > Offline Device Report.
View the Protocol Distribution graph.	View the distribution of IP, AppleTalk, IPX, DECnet, VINES, and XNS packets for selected devices in a bar or pie chart. This report shows the Layer 3 protocol packet types that are forwarded by the devices.	Select Resource Manager Essentials > Availability > Protocol Distribution Graph.

RQS nº 03/2005 CN
CPMI CORREIOS
Fls Nº 145
Doc 3702

Case Management

You can use Case Management to open and track a case for network problems that require assistance from Cisco Technical Assistance Centre. Case Management can collect critical network information, such as protocol, interface, and configuration data from Essentials and send to Cisco.com.

When you open a case, you can designate specific Telnet command data (if applicable) and SNMP inventory values to be collected from selected devices. Case Management will attach this information to the case description and forward it to Cisco.com, which can reduce the time it takes a Cisco representative to help resolve the problem.

Inquiries to Cisco TAC are categorized according to the urgency of the issue. New cases are automatically set to Priority level 3 (P3). If your case requires higher priority handling, you must contact the Cisco TAC or your sales engineer to request that the priority be raised. For more information on priority categories, see "Obtaining Technical Assistance" section on page -xvii.

Table 2-5 shows the tasks you can accomplish with the Case Management application.

Table 2-5 Case Management Tasks

Task	Purpose	Action
Open a case and attach network device statistics.	Open a case to Cisco.com through the CiscoWorks desktop	Select Management Connection > Case Management > Open Case.
View status of cases and update description.	View the history and status of your case and update description of problems.	Select Management Connection > Case Management > Query or Update Case.

RQS nº 03/2005 - CN
CPMI CORREIOS
Fls Nº 146
Doc. 3702

16585
L

Change Audit

The Change Audit application lets you track and report network changes. It provides the capability for other Essentials applications to log change information to a central repository called the Change Audit log.

New Features in Change Audit

You can now delete change audit records that are older than a specified number of days.
For example, if you specify 15 days, change audit records that are over 15 days old (including today) will be deleted (**Resource Manager Essentials > Administration > Change Audit > Delete Change History**).

Change Audit Functional Flow

Change Audit tracks all changes discovered by the Inventory Manager, Software Manager, and Configuration Manager. Every time one of these applications detects a change, it sends a change record to the Change Audit Service, with details of who, when, and what type of change occurred. See Figure 2-4.

Inventory changes include any changes to device information stored in the Inventory database, such as chassis, interfaces, and system information. Software Management changes include upgrades to new software image versions. Configuration Management changes include all changes made to configuration files on devices. This includes changes made outside of Essentials tasks, detected by the Configuration Archive process, as well as changes made using Essentials functionality—NetConfig or Config Editor.

Inventory changes can be filtered to limit the types of changes that are stored in the Change Audit database. For example, you might not want to track every time the port status on a switch changes because users have shut down their computers connected to the switch. Software and configuration management changes cannot be filtered.

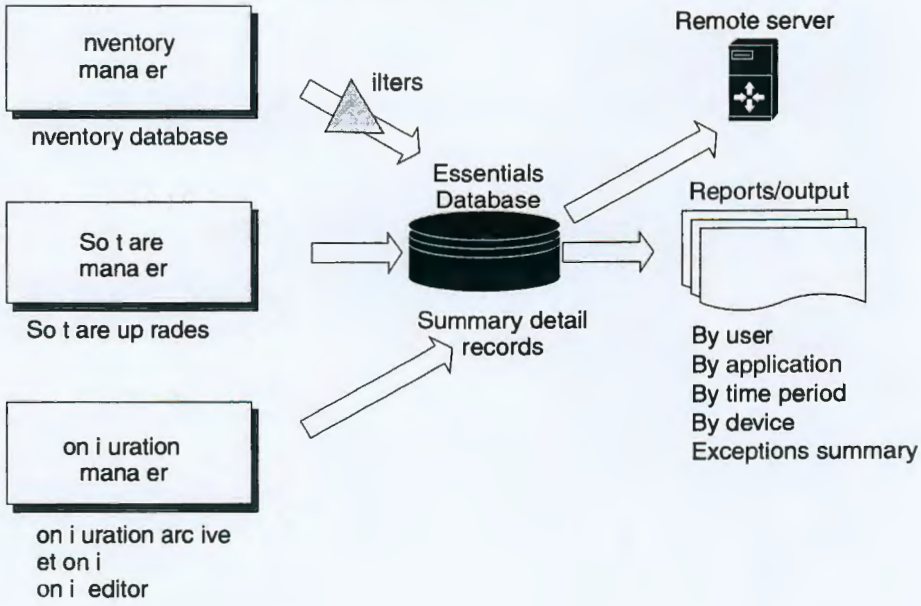
You can view change records or search for specific change records to determine who made a change or when a change was made. Change reports can also be time based to quickly report on changes that have, or have not, occurred during specified time periods—possibly detecting unauthorized change activity.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 147
Doc 3702

16.584
2

The Change Audit Service application can also be configured to forward change records, in the form of SNMP traps to remote servers, allowing you to monitor and view changes from a remote network-management station that has event-collection capabilities, such as HP OpenView.

Figure 2-4 Change Audit Functional Flow



RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 148
3702
Doc.

Figure 2-5 Change Audit Work Flow

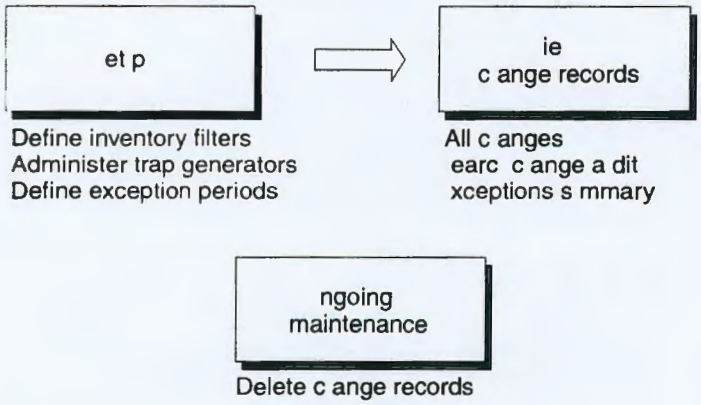


Figure 2-5 depicts the Change Audit workflow and associated tasks within Essentials. Change Audit automatically stores any change records sent from the Inventory Manager, Software Manager, and Configuration Manager applications. After these applications are set up, you can view change records at any time.

You need to perform Change Audit setup tasks only if you want to filter out specific Inventory changes, forward change records to a remote server, or report on changes during specific time periods every week. Change records are stored in the Essentials database until they are removed. Therefore, ongoing maintenance is required to delete old records from the database.

Table 2-6 shows the tasks that you can accomplish with the Change Audit application.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 149
3702
Doc

Table 2-6 Change Audit Tasks

Task	Purpose	Action
View Change Audit logs.	View the two log tables: Change Audit summary and Change Audit details.	Select Resource Manager Essentials > 24-Hour Reports > Change Audit Report. Or Select any report from Resource Manager Essentials > Change Audit.
Delete records from the log.	Delete or schedule deletion of change records from the Change Audit log.	Select Resource Manager Essentials > Administration > Change Audit > Delete Change History.
Convert change records to SNMP traps.	Convert some or all change notifications into SNMP V1 traps and send them to a destination you configure.	Select Resource Manager Essentials > Administration > Change Audit > Administer Trap Generator.
Define an exceptions period.	Specify a period of time when no network changes should occur.	Select Resource Manager Essentials > Administration > Change Audit > Define Exceptions Summary.
Set up filtering options.	Define one or more filter fields to filter report data.	Select Resource Manager Essentials > Change Audit > Search Change Audit.
View changes in an exception period.	Generate a report on changes that occurred in the network during a defined exception.	Select Resource Manager Essentials > Change Audit > Exceptions Summary.
View all change records.	Generate a report that enables you to view changed data in the Change Audit log.	Select Resource Manager Essentials > Change Audit > All Changes.
View a summary of changes made in the last 24-hours.	Generate a summary of changes made in the past 24 hours from Change Audit log data.	Select Resource Manager Essentials > 24-Hour Reports > Change Audit Report.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 150
Doc 3702

NC 531
2

Configuration Management

The Configuration Management application stores the current, and a user-specified number of previous versions, of the configuration files for all supported Cisco devices maintained in the Inventory. It automatically tracks changes to configuration files and updates the database if a change is made.

New Features of Configuration Management

The Configuration Management application has the following new features, that allow you to:

- Enable Job Password Policy for NetConfig, NetShow, and Config Editor Jobs
- Specify the Transport Protocol Order for NetConfig, Config Editor, and Network Show Jobs
- Quick Configuration Download from Configuration Archive
- Archive and Restore VLAN Configuration Files

For more details of the new features, see Configuration Management, in the Essentials online help.

Enable Job Password Policy for NetConfig, NetShow, and Config Editor Jobs

Essentials stores passwords in the database. While the job is run, the password is retrieved from the database for each of the selected devices. For example, if the TACACS server is managing the devices, the passwords in the TACACS server and the passwords in the Essentials database should be synchronized (with every password change).

You now have the option of entering a username and password for running a specific NetConfig, Network Show, or Config Editor job. If you enter a username and password, NetConfig, Network Show or Config Editor applications use this username and password to connect to the device, instead of taking these credentials from the Essentials database.

This option of entering the username and password for job execution is useful in high security installations where device passwords are changed at frequent intervals. In such instances, the passwords may be changed every 60-90 seconds.

RQS nº 03/2005 - CN
CPMI CORREIOS
Fls. Nº 151
3702
Doc

To use this option of entering a username and password for running a specific job, you should enable the job password policy for NetConfig, Network Show, or Config Editor jobs using the Password Policy tab of the Configuration Job Setup dialog box, in the Configuration Management application. To invoke the Configuration Job Setup dialog box, select **Resource Manager Essentials > Administration > Configuration Management > Configuration Job Setup**.

You can also set the job password to be mandatory, or user configurable.

If you do not enable the job password policy, then the NetConfig, Network Show, or Config Editor applications take the device credentials from the Essentials database to connect to the device.

For details about:

- Enabling the job password policy, see the Essentials online help. (In the left navigation pane of the Essentials online help, select **Resource Manager Essentials > Configuration Management > Configuration Management Administration > Password Policy for NetConfig, Config Editor and NetShow Jobs**).
- Usage Scenarios when the job password is configured on devices, see the Essentials online help. (In the left navigation pane of the Essentials online help, select **Resource Manager Essentials > Configuration Management > Configuration Management Administration > Usage Scenarios When Job Password is Configured on Devices**).

Specify the Transport Protocol Order for NetConfig, Config Editor, and Network Show Jobs

Essentials now provides you with the option of separately specifying the transport protocol order for the download operations of NetConfig, Config Editor and Network Show jobs, and for the fetch operations of NetConfig and Config Editor jobs.

You can use the Transport Protocol tab of the Configuration Management application (**Resource Manager Essentials > Configuration Management > Administration > Configuration Job Setup**) to specify the transport protocol order.

This option allows you to use your preferred protocols for downloading or fetching configurations.

RQS nº 03/2005 CN
CPMI CORREIOS
Fls Nº 152
Nº 3702
Doc.

16.579

For example, you can use Telnet to download configuration to the device, and TFTP to fetch the configuration, thereby improving the overall performance of NetConfig.

You can select the fallback option for these protocols. If you select this option, and the first preferred protocol fails, the next protocol in the list is used for configuration download or fetch operations, and so on.

For details, see the Essentials online help.
(In the left navigation pane of the Essentials online help, select **Resource Manager Essentials > Configuration Management > Configuration Management Administration > Setting the Transport Protocol Order for NetConfig, Config Editor and NetShow Jobs**).

Quick Configuration Download from Configuration Archive

You can now create a job to immediately download a selected version of the running configuration, to a device from the Configuration Archive (**Resource Manager Essentials > Configuration Management > Search Archive by Device** or **Resource Manager Essentials > Configuration Management > Search Archive by Pattern**).

This method of download is useful when you know the version of the running configuration that has to be downloaded to the device.

For details, see the Essentials online help.
(In the left navigation pane of the Essentials online help, select **Resource Manager Essentials > Configuration Management > Configuration Management Administration > Making a Quick Download of a Device Configuration**).

Archive and Restore VLAN Configuration Files

For all Cisco devices that support VLAN configuration such as Catalyst IOS switches, Essentials creates a version of the VLAN configuration file (vlan.dat) for each version of the running configuration file of a device. That is, the running configuration and the vlan configuration files are archived in pairs.

You can download the vlan configuration file to the device, using the Command Line Interface.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 153
Nº 3702
Doc

You can view the status of the archived VLAN files using the VLAN Configuration tab of the Configuration Archive Status Summary window (**Resource Manager Essentials > Administration > Configuration Management > Archive Status**).

This table details the scenarios under which VLAN configuration is fetched.

Scenarios	VLAN Config Fetched/Not Fetched
On adding a device to Inventory	Fetched
On using the Update Archive option from GUI	Fetched
On receiving a Config Change syslog event	Fetched
Scheduled Config Polling	Fetched
Scheduled Config Collection	Fetched
Using the command cwconfig get from CLI	Fetched
Sync Config Archive Before Execution Policy of NetConfig/Config editor.	Fetched
Config Fetch following download of commands through NetConfig/Config Editor/Quick Config Restore /cwconfig command	Not fetched

(In the left navigation pane of the Essentials online help, select **Resource Manager Essentials > Configuration Management > Configuration Management Administration > Checking VLAN Configuration Archive Status.**)

Benefits of Configuration Management

One of the most difficult but important things to manage on network devices, is the device configuration. Often a change to the device configuration leads to network performance issues and faults. The device configuration is the key to how a device operates on the network and traffic is passed.

RQS nº 03/2005 CN
CPMI CORREIOS
Fls Nº 154
Doc 3702

As the network administrator, you need to be able to control and track changes to device configurations to minimize errors and assist in troubleshooting problems. This can be very difficult if several different users are making changes to the device configurations. It can also become very repetitive and time-consuming. Configuration Management can help simplify and automate these tasks.

Configuration Management gives you easy access to the configuration files for all file-based or Cisco IOS-based Catalyst switches, FastSwitches, Cisco routers, Content Service Switches (CSS) and Content Engine (CE) devices in Essentials.

Configuration files are collected and stored in the Configuration Archive for all the devices supported by the Configuration Management application. (For the list of supported devices, on Cisco.com select **Products and Services > Network Management CiscoWorks > CiscoWorks Resource Manager Essentials > Technical Details > Device Support Tables.**)
When you change the configuration, an event is sent to the archive which automatically collects the latest configuration.

Before you can use the Configuration Archive, you must make sure you have completed all the necessary setup tasks. For information on these tasks, see:

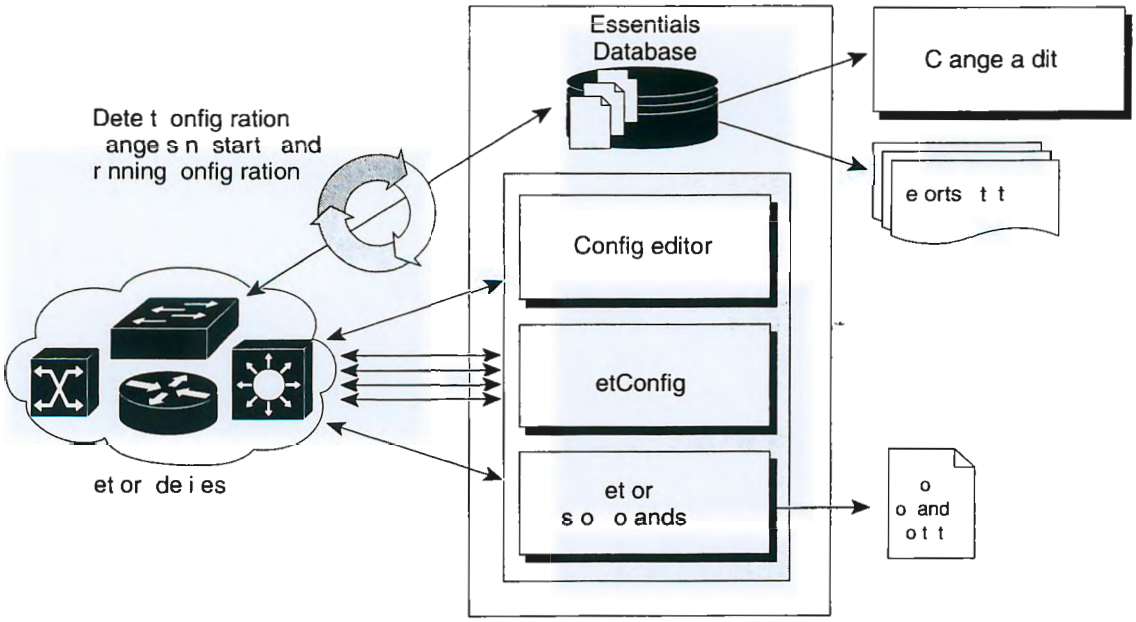
- Installation and Setup Guide for Resource Manager Essentials on Solaris.
- Installation and Setup Guide for Resource Manager Essentials on Windows.

Configuration Management Functional Flow

After you add or import devices into your inventory, the configuration files for each supported device are collected and stored in the Configuration Archive. When you change the configuration, an alert is sent to the archive which automatically collects the latest configuration information. In addition, a change record is sent to the Change Audit application, which collects and organizes all changes to network devices. This allows you to view all configuration changes made over any period of time or by any specific user. See Figure 2-6

RQS nº 03/2005 CN
CPMI - CORREIOS
Fls Nº 155
Nº 3702
Doc

Figure 2-6 Configuration Management Functional Flow



ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 156
Doc 3702

16 575
L

Figure 2-7 Configuration Management Workflow

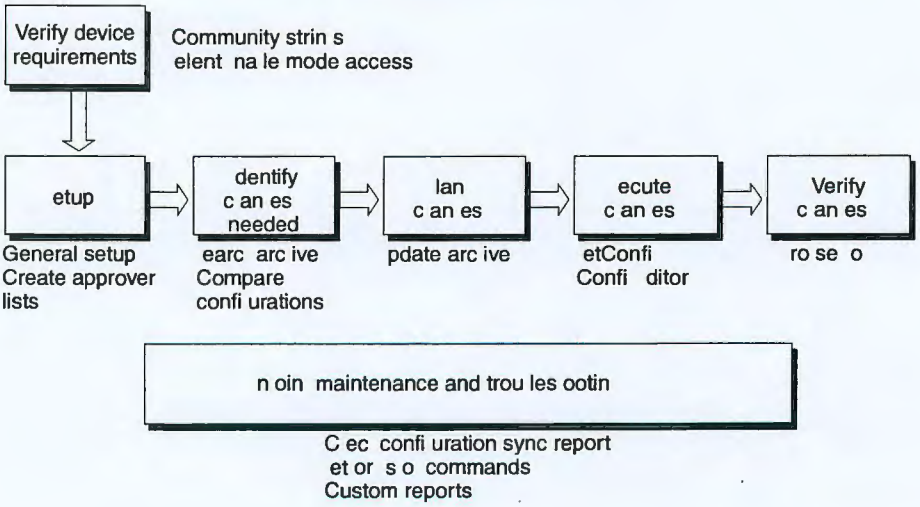


Figure 2-7 depicts Configuration Management workflow and associated tasks:

- Verify device requirements to ensure that Essentials is able to communicate with the devices.
- Create approver lists, if specific users are going to be required to approve configuration updates before they are executed and set Configuration Archive preferences (update schedule, number of copies to retain, and so on), and After the Configuration Archive is set up, it can be used to view device configurations and identify and plan necessary changes. Then, the NetConfig or Config Editor applications can be used to actually execute and confirm the changes.

  As ongoing maintenance, the Configuration Sync report should be checked daily to ensure that all running and startup configurations on devices match. In addition, the network administrator can use Network Show Commands and Custom reports to troubleshoot problems and gather information as needed.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 157
3702
Doc

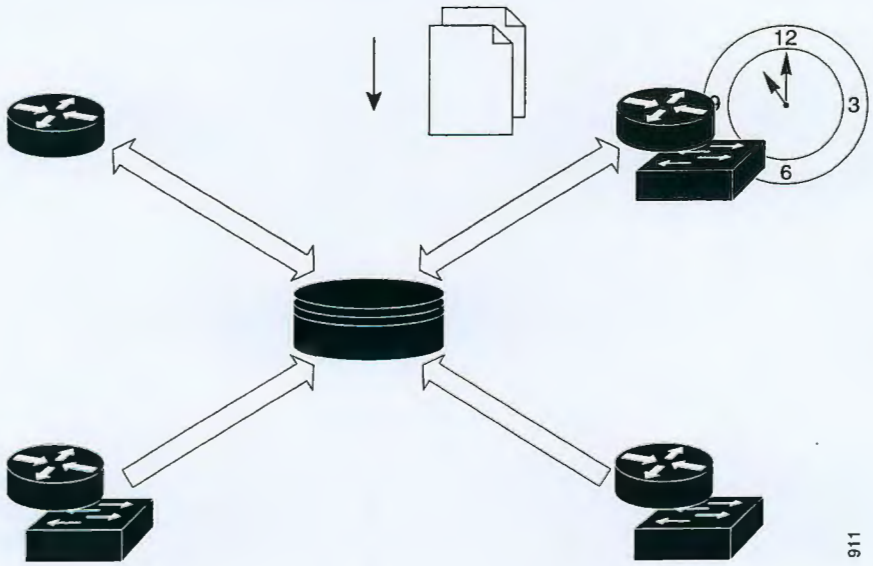
16.514

Configuration Archive

The Configuration Archive maintains a history of configuration files for all managed devices on the network. The network administrator can specify how long files should be kept in the archive, how many versions should be maintained in the archive, and how often devices on the network should be polled for changes. In addition, there are multiple ways to detect changes on devices and trigger an update to the Configuration Archive.

For example, specific syslog messages sent from the device can indicate that a change has occurred and can trigger the Configuration Archive to retrieve the new configuration. The Configuration Archive can also be scheduled to poll all devices at a specific time each week.

Figure 2-8 Configuration Archive Functional Flow



RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 158
Nº 3702
Doc

NetConfig, Config Editor, and Network Show Commands

Two additional applications, NetConfig and Config Editor, are available to edit configuration files. The NetConfig application allows you to save sets of commands and execute those commands on multiple devices at the same time.

The Config Editor application can be used to edit any device configuration that is stored in the Configuration Archive, and then download the new configuration to the device. The new configuration is stored in the Configuration Archive and will also trigger a change record to be sent to Change Audit. Additional Configuration reports specific to active virtual private network (VPN) devices are also available.

The NetConfig application provides a set of wizard-based templates that can be used to update the device configuration on multiple devices all at once. The devices must already be managed by Essentials. The new configuration will be stored in the archive for each device changed, and associated change records will be created.

The Network Show Command application accesses network devices in real time to display output for common show commands. This can help in troubleshooting by allowing you to display interface statistics, routing tables, and system information for selected devices.

RQS nº 03/2005 CN
CPMI CORREIOS
Fls Nº 159
Doc 3702

Table 2-7 shows the archive-specific tasks you can accomplish with the Configuration Management application.

Table 2-7 Configuration Management Archive-Specific Tasks

Task	Purpose	Action
Search for configuration files.	Search for configuration files based on device name or text pattern.	Select Resource Manager Essentials > Configuration > Management > Search Archive by Device. or Select Resource Manager Essentials > Configuration Management > Search Archive by Pattern.
Create, run, modify, and delete custom reports.	Create and run custom reports that gather device configuration files from the archive for specified devices. You can also modify and delete custom reports.	Select Resource Manager Essentials > Configuration Management > Custom Reports.
Compare device configuration files.	Compare configuration files of two devices or two versions of a single file. Compare the starting and current configurations of a device. Compare the current and the most recently archived configurations of a device.	Select Resource Manager Essentials > Configuration Management > Compare Configurations.
Find out-of-sync configurations.	Determine whether a device's startup and running configurations are synchronized. The two configurations might differ if you change a device configuration after the device is booted.	Select Resource Manager Essentials > Configuration Management > Startup/Running Out of Sync Report or Select Resource Manager Essentials > 24 Hour Reports > Configuration Sync Report.

RQS nº 03/2005 - CN
CPMI CORREIOS
Fls. Nº 160
Doc. 3702

Table 2-7 Configuration Management Archive-Specific Tasks (continued)

Task	Purpose	Action
Move the Configuration Archive.	Move the Configuration Archive to a new location.	Select Resource Manager Essentials > Administration > Configuration Management > General Setup, then select the Archive Setup tab.
Specify criteria for purging the archive.	Specify when to purge configurations from the archive. You can specify two criteria: • Age. Configurations older than the specified age are purged. • Maximum number of versions. The oldest configuration is purged when the maximum number is reached. You can also choose not to purge labelled files.	Select Resource Manager Essentials > Administration > Configuration Management > General Setup, then select the Archive Setup tab.
Modify Configuration Archive retrieval.	Modify how and when the Configuration Archive retrieves configurations.	Select Resource Manager Essentials > Administration > Configuration Management > General Setup, then select the Change Probe Setup tab.
Change the transport protocol order used by the Configuration Archive.	Change the order of the transport protocols the Configuration Archive uses to download configurations from devices to the archive. The default order is: • TFTP (Trivial File Transport Protocol) • Telnet • SSH • rcp (Remote Copy Protocol)	Select Resource Manager Essentials > Administration > Configuration Management > General Setup, then select the Transport Setup tab.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 161
Doc 3702

Table 2-7 Configuration Management Archive-Specific Tasks (continued)

Task	Purpose	Action
Update the Configuration Archive.	Update the archive manually if you make a significant change to a device configuration and want the archive to reflect the changes. The Configuration Archive retrieves configurations at 12.30 a.m. every Friday by default. It also listens to Syslog messages and fetches the configuration.	Select Resource Manager Essentials > Configuration Management > Update Archive.
Check the archive status.	Check archive status for the latest attempt to archive a device configuration (running or startup).	Select Resource Manager Essentials > Administration > Configuration Management > Archive Status.
Configure labels.	Select configuration files from different managed devices, group them, and label them as a set. You can also view, modify, and remove configuration labels.	Select Resource Manager Essentials > Administration > Configuration Management > Label Configuration.
Use the **cwconfig** command at the command line.	Access the Configuration Archive to update, export, and import configurations on devices and in the archive. For more information about the command syntax and parameters, see the cwconfig man page on UNIX systems, by entering: `man -M /opt/CSCOpx/man cwconfig`	This command cannot be entered from the desktop; use the command line.
Locate the Configuration Archive shadow directory.	Access the Configuration Archive shadow directory, which is an image of the most recent configurations gathered by the Configuration Archive.	The shadow directories cannot be accessed from the desktop. • On Solaris, as root or casuser, enter: `/var/adm/CSCOpx/files/archive/shadow` • On Windows, as admin, enter: *NMSROOT*`\files\archive\shadow`

RQS nº 03/2005 - CN
CPMI CORREIOS
Fls Nº 162
Doc 3702

NetConfig Option

Using the NetConfig option, which runs as a separate application in its own window, you can make configuration changes to your managed network devices.

New Features of NetConfig

NetConfig application has the following new features:

- Job Password Option
- Job Retry Option
- Multiple Selection of Jobs for Deletion
- Separate Protocol Ordering for Configuration Download and Fetch Operations
- Support for New Templates
- Support for System- Defined Templates to Configure IPSec and SSH on Devices
- Support for Interactive and Multiline Commands

For more details of the new features, see the section, NetConfig, in the Essentials online help.

Job Password Option

Essentials stores passwords in the database. While the job is run, the password is retrieved from the database for each of the selected devices. For example, if the TACACS server is managing the devices, the passwords in the TACACS server and the passwords in the Essentials database should be synchronized (with every password change).

You now have the option of entering a username and password for running a specific job. If you enter a username and password, NetConfig uses this username and password to connect to the device, instead of taking these credentials from the Essentials database.

This option of entering the username and password for job execution is useful in high security installations where device passwords are changed at frequent intervals. In such instances, the passwords may be changed every 60-90 seconds.

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 163
Nº 3702
Doc

To use this option of entering a username and password for running a specific job, you should enable the job password policy for NetConfig jobs using the Password Policy tab of the Configuration Job Setup dialog box, in the Configuration Management application. To invoke the Configuration Job Setup dialog box, select **Resource Manager Essentials > Administration > Configuration Management > Configuration Job Setup**.

You can also set the job password to be mandatory, or user configurable.

If you do not enable the job password policy, then NetConfig takes the device credentials from the Essentials database to connect to the device.

For details about:

- Enabling the job password policy, see the Essentials online help. (In the left navigation pane of the Essentials online help, select **Resource Manager Essentials > NetConfig > NetConfig Administration > Password Policy for NetConfig Jobs**).
- Usage Scenarios when job password is configured on devices, see the Essentials online help. (In the left navigation pane of the Essentials online help, select **Resource Manager Essentials > Configuration Management > Configuration Management Administration > Usage Scenarios When Job Password is Configured on Devices**).
- The NetConfig usage scenario, see the topic, "Performing a NetConfig Job with the Job Password Policy Enabled", in this User Guide.

Job Retry Option

You now have the retry option for failed NetConfig jobs. When you retry a job, it runs the job on the failed devices, and retains the job ID of the failed job.

For details, see the Essentials online help.
(In the left navigation pane of the Essentials online help, select **Resource Manager Essentials > NetConfig > Browsing and Editing NetConfig Jobs > Browsing and Editing Jobs**.)

RQS nº 03/2005 CN
CPMI CORREIOS
Fls. Nº 164
3702
Doc.

Multiple Selection of Jobs for Deletion

You can now select more than one job at a time, for deletion from the Job Browser.

For details, see the Essentials online help.
(In the left navigation pane of the Essentials online help, select **Resource Manager Essentials > NetConfig > Browsing and Editing NetConfig Jobs > Browsing and Editing Jobs.**)

Separate Protocol Ordering for Configuration Download and Fetch Operations

Earlier, the NetConfig application used Telnet to download configuration diffs to the device, and same session was used to fetch the entire configuration from the device. If the configurations are large (for example, ACLs) this adversely affected the overall performance of NetConfig.

For NetConfig jobs, you can now set the transport protocol order separately, for downloading configurations, and for fetching configurations.

This option allows you to use your preferred protocols for downloading and fetching the configuration. For example, you can use Telnet to download configuration to the device, and TFTP to fetch the configuration, thus improving the overall performance of NetConfig.

For downloading the configurations, the protocols used are Telnet and SSH.

The default order is,

- Telnet
- SSH (Secure Shell)

For fetching the configurations, the protocols used are Telnet, TFTP, SSH, and rcp. The default order is,

- TFTP (Trivial File Transport Protocol)
- Telnet
- rcp (remote copy protocol)
- SSH (Secure Shell)

You can change the transport protocol order for both downloading and fetching the configurations.

You can select the fallback option for these protocols. If you select this option, and the first preferred protocol fails, the next protocol in the list is used for configuration download or fetch operations, and so on.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 165
Doc 3702

For details, see the Essentials online help.
(In the left navigation pane of the Essentials online help, select **Resource Manager Essentials > Configuration Management > Configuration Management Administration > Setting the Transport Protocol Order for NetConfig, Config Editor and NetShow Jobs**).

Support for New Templates

Resource Manager Essentials now supports eleven new templates, that can be used through the NetConfig application. They are:

IOS Templates. (These are global IOS templates. They can be applied to one or more IOS device at a time.)

- SNMP Security
- SNMP Traps Management

IOS-Interface-specific Templates. (These can be applied to only one IOS device at a time.)

- IGMP
- Interface IP Address

Cable Templates (These are global templates. They can be applied to one or more Cable-CMTS devices at a time.)

- Cable N+1 Redundancy
- Cable Spectrum Management

Cable Interface-specific Templates. (These can be applied to only one Cable-CMTS device at a time.)

- Cable BPI/BPI+
- Cable DHCP-GiAddr and Helper
- Cable DownStream
- Cable Interface Bundling
- Cable Upstream

For details, see the Essentials online help.
(In the left navigation pane of the Essentials online help, select **Resource Manager Essentials > NetConfig >Configuration Templates**).

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 166
Nº 3702
Doc

Support for System- Defined Templates to Configure IPSec and SSH on Devices

Essentials now supports system-defined templates for configuring IPSec and SSH on devices:

- Use the SSH system-defined template to configure SSH on devices.
- Use the Internet Key Exchange (IKE), Transform, Crypto Map system-defined templates to configure IPSec on devices.

For details, see the Essentials online help.
(In the left navigation pane of the Essentials online help, select **Resource Manager Essentials > NetConfig >Configuration Templates**).

Support for Interactive and Multiline Commands

You can now specify interactive and multi-line commands in user defined templates.

For example, as a part of user-defined templates in NetConfig, you can do the following:

- Enter an interactive command in the Enter CLI Commands area, using the following syntax:

  CLI Command<R>*command response 1* <R>*command response 2*

- Enter a multi-line command, using the following syntax:

  <MLTCMD> banner login *"Welcome to*

  CiscoWorks Resource Manager

  Essentials – you are using

  multiline commands" **</MLTCMD>**

Note The tags, <R>, <MLTCMD> and </MLTCMD>, are case sensitive and should always be uppercase.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 167
Doc: 3702

Support for interactive and multi-line commands is not available through the NetConfig CLI.

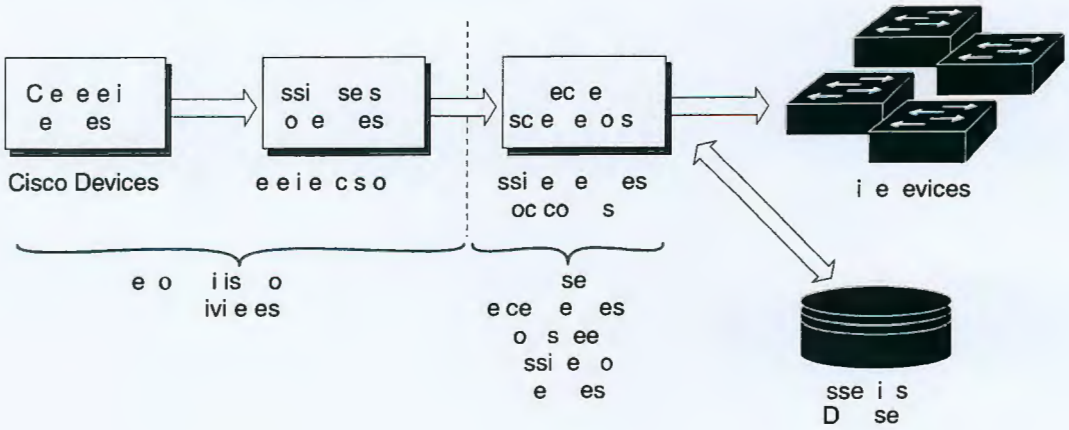
For details, see the Essentials online help.
(In the left navigation pane of the Essentials online help, select **Resource Manager Essentials > NetConfig >Defining and Scheduling a NetConfig Job > Handling Interactive Commands in NetConfig and Config Editor Jobs** and **Handling Multi-line Commands**).

Benefits of Netconfig

The NetConfig application provides you with wizard-based templates to simplify and reduce the time it takes to make global changes to network devices. These templates can be used to execute one or more configuration commands on multiple devices at the same time.

For example, if you want to change passwords on a regular basis to increase security on devices, you can use the appropriate password template to update passwords on all devices at once. A copy of all updated configurations will be automatically stored in the Configuration Archive. See Figure 2-9.

Figure 2-9 NetConfig Functional Flow



RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 168
Doc. 3702

NetConfig uses configuration templates to create the configuration commands run on devices when a NetConfig job runs. There are three types of configuration templates:

- System-defined—Provided with NetConfig, these templates simplify the creation of common configuration commands.
- User-defined—Created by system administrators, these templates can contain any configuration commands.
- Adhoc—Allows you to add any configuration commands to a NetConfig job while you are defining it.

Caution NetConfig does not verify the commands entered in the user-defined and adhoc templates. These commands are executed on devices exactly as they appear in the template. If you enter incorrect configuration commands, you could misconfigure or disable the devices on which the job runs.

By default, only network administrators have access to configuration templates. Network administrators can assign template access privileges to the other system users. When you define or edit a job, the configuration templates to which you have access privileges, appear in the job definition wizard.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 169
Doc: 3702

Table 2-8 shows the tasks that can be accomplished with the NetConfig option.

Table 2-8 NetConfig Tasks

Task	Purpose	Action
Define and schedule a NetConfig job.	Define a NetConfig job to make device configuration changes, and schedule it to run.	1. Select Resource Manager Essentials > Configuration Management > NetConfig > Jobs > New Job. or Click the New Job button. 2. Complete the job definition wizard.
Browse and edit NetConfig jobs.	Browse the NetConfig jobs that are registered on the system and edit them as necessary.	1. Select Resource Manager Essentials > Configuration Management > NetConfig > Jobs > Job Browser. or Click the Job Browser button. 2. Select a job record. 3. Click Edit Job, Copy Job, Remove Job, Stop Job, or Job Details.
View NetConfig job details.	View detailed information about a registered NetConfig job. You can also edit a job from its detailed view.	1. Select Resource Manager Essentials > Configuration Management > NetConfig > Jobs > Job Browser. or Click the Job Browser button. 2. Select a job record. 3. Click Job Details. 4. Click Edit Job, Copy Job, Remove Job, Stop Job, Retry Job (for failed jobs), or Print.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 170
3702
Doc.

Table 2-8 NetConfig Tasks (continued)

Task	Purpose	Action
Launch Essentials.	Launch Essentials if it is not already running.	Select Resource Manager Essentials > Configuration Management > NetConfig >Tools > Launch RME. or Click the Launch RME button.
Create and edit user-defined configuration templates.	Create and edit configuration templates that can contain any configuration commands.	Select Resource Manager Essentials > Configuration Management > NetConfig >Admin> Create/Edit User Templates.
Assign configuration template access privileges to users.	Assign access privileges to the system-defined and user templates on the system.	Select Resource Manager Essentials > Configuration Management > NetConfig > Admin > Assign Template Users.
Set default template policies.	Set the default policies for NetConfig jobs that are defined.	Select Resource Manager Essentials > Configuration Management > NetConfig > Admin > Set Template Policies.
View online help for the task you are performing.	View the online help for information about the task you are performing.	Select Resource Manager Essentials > Configuration Management > NetConfig > Help > Context-Sensitive Help. or Click the Help button.
Use the NetConfig command to make batch configuration changes.	Define and schedule NetConfig jobs from the command line.	Enter the NetConfig command at the command line with the appropriate syntax. For more information, see the online help and the netconfig man page. To view the man page, add the path `install_dir/CSCOpx/man` to the *MANPATH* variable.

RQS nº 03/2005 CN
CPMI - CORREIOS
Fls. Nº 171
Nº Doc 3702

Network Show Commands Option

As a network administrators you must be familiar with *show commands* used on Cisco routers and switches. Network show commands represent a set of read-only commands that you can run on routers, Catalyst switches, Content Engine, Content Service Switches, FastSwitchs and PIX devices. These commands display configuration or status information. You can run Network Show commands from the GUI or from the command line interface.

New Features in Network Show

Network Show has the following new features:

- Job Password Option
- Multiple Selection of Jobs for Deletion
- Protocol Ordering for Running Network Show Commands

For more details of the new features, see NetConfig, in the Essentials online help.

Job Password Option

Essentials stores passwords in the database. While the job is run, the password is retrieved from the database for each of the selected devices.
For example, if the TACACS server is managing the devices, the passwords in the TACACS server and the passwords in the Essentials database should be synchronized (with every password change).

You now have the option of entering a username and password for running a specific job. If you enter a username and password, Network Show uses this username and password to connect to the device, instead of taking these credentials from the Essentials database.

This option of entering the username and password for job execution is useful in high security installations where device passwords are changed at frequent intervals. In such instances, the passwords may be changed every 60-90 seconds.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 172
Doc. 3702

16.559

To use this option of entering a username and password for running a specific job, you should enable the job password policy for Network Show jobs using the Password Policy tab of the Configuration Job Setup dialog box, in the Configuration Management application. To invoke the Configuration Job Setup dialog box, select **Resource Manager Essentials > Administration > Configuration Management > Configuration Job Setup**.

You can also set the job password to be mandatory, or user configurable.

If you do not enable the job password policy, then Network Show takes the device credentials from the Essentials database to connect to the device.

For more details about:

- Enabling the job password policy, see the Essentials online help. (In the left navigation pane of the Essentials online help, select **Resource Manager Essentials > Configuration Management > Configuration Management Administration > Password Policy for NetConfig, Config Editor and NetShow Jobs**).
- Job password for Network Show jobs, see the Essentials online help. (In the left navigation pane of the Essentials online help, select **Resource Manager Essentials > Network Show > Network Show Batch Reports > Network Show Batch Reports Tasks > Scheduling a Report**).
- Usage Scenarios when the job password is configured on devices, see the Essentials online help. (In the left navigation pane of the Essentials online help, select **Resource Manager Essentials > Configuration Management > Configuration Management Administration > Usage Scenarios When Job Password is Configured on Devices**).

Multiple Selection of Jobs for Deletion

You can now select more than one job at a time, for deletion from the Job Browser.

For details, see the Essentials online help. (In the left navigation pane of the Essentials online help, select **Resource Manager Essentials > Network Show > Network Show Batch Reports > Network Show Batch Reports Tasks > Browsing Jobs**).

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 173
Doc: 3702

Protocol Ordering for Running Network Show Commands

You can now set the transport protocol order for running network show commands on devices.

For running the commands, the protocols used are Telnet and SSH. The default order is,

- Telnet
- SSH (Secure Shell)

This option allows you to use your preferred protocol order for running network show commands on devices. If you select the fallback option for these protocols and the first preferred protocol fails, the next protocol in the list is used for running the show commands, and so on.

For details, see the Essentials online help.
(In the left navigation pane of the Essentials online help, select **Resource Manager Essentials > Configuration Management > Configuration Management Administration > Setting the Transport Protocol Order for NetConfig, Config Editor and NetShow Jobs**).

Benefits of Network Show Commands

As an Essentials user, you can execute Show commands against many devices and view the results from Essentials, using the Network Show Commands application.

This application can be used to display Show command output for multiple devices in two modes:

- Immediate execution—Run the selected set of Show commands for the selected devices immediately.
- Batch mode—Schedule a set of Show commands to be run against a selected set of devices.

You can use the Network Show tasks to organize and save one or more related Show commands into logical groups, called command sets. These command sets can then be applied to devices whenever specific configuration or status information is needed. You specify which commands you want to group together and run the commands on one or many devices. The output is displayed in a browser window.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 174
3702
Doc

All users have access to the following predefined command sets, which ship with Essentials. Some of the most common Show commands used in monitoring and troubleshooting a network are:

- `show interface info`
- `show IP routing info`
- `show protocol info`
- `show switch VLAN info`
- `show system info`
- `show system performance`
- `Show Interfaces Rate-Limit Info`
- `Show Cable QoS Profile Info`
- `Show Cable Modulation-Profile`
- `Show Cable Hop Info`
- `Show Cable Tech Info`
- `Show HCCP details Info`
- `Show IGMP Info`
- `Show SNMP Users and Groups Info`
- `Show Cable Spectrum Info`
- `Show Cable Modem Info`

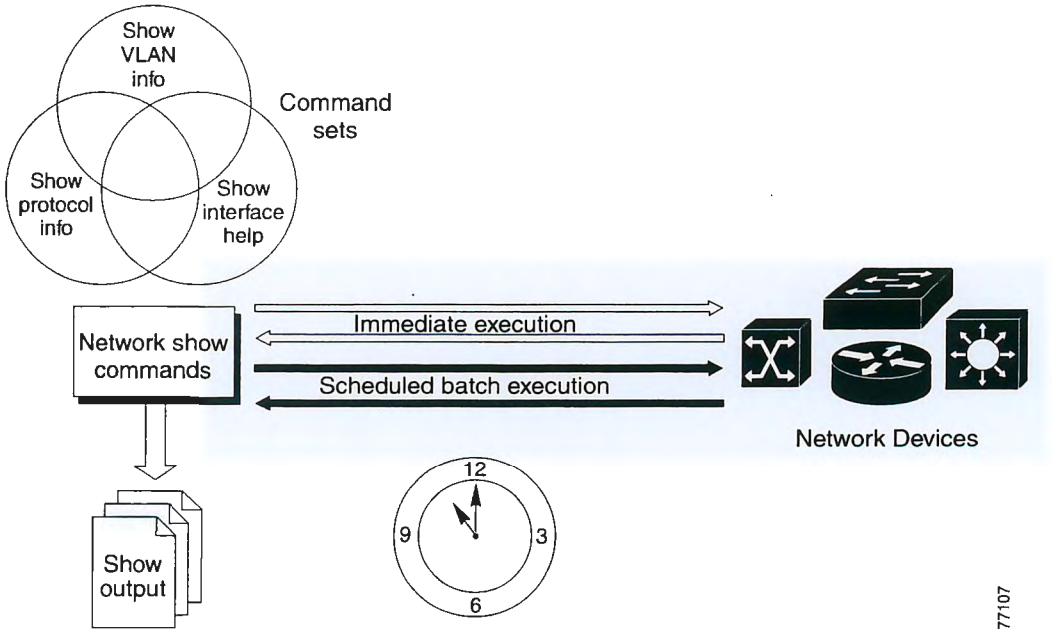
For details of all the available Show commands, see the Essentials online help. (In the left navigation pane of the Essentials online help, select **Resource Manager Essentials > Network Show > The Basics > List of Network Show Commands**).

In order to display output for other Show commands within Essentials, you must first define the command set, and then assign users to be able to access the command set.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 175
Doc 3702

Essentials ships with a set of default network command sets, which you cannot edit or delete. See Figure 2-10.

Figure 2-10 Network Show Commands Functional Flow



RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 176
Nº 3702
Doc

Table 2-9 shows the tasks you can accomplish with the Network Show Commands option.

Table 2-9 Network Show Commands Tasks

Task	Purpose	Action
Create a network show command set.	Create, edit, and delete a logical group of custom commands for a user or a set of users.	Select Resource Manager Essentials > Administration > Configuration Management > Network Show > Define Command Set.
Assign users to the network show command set.	Specify which user or set of users can run network show commands.	Select Resource Manager Essentials > Administration > Configuration Management > Network Show > Assign Users.
Execute a network show command set immediately.	Run network show commands on one or more devices.	Select Resource Manager Essentials > Configuration Management > Network Show Commands > Immediate Execution.
Define a batch report.	Create a batch report containing command sets and remote console commands that can be run on a set of devices to generate a report. You can also modify or delete existing reports.	Select Resource Manager Essentials > Configuration Management > Network Show Commands > Batch Reports > Define Reports.
Schedule a batch report.	Schedule reports in batches and generate these batch reports at a specified time.	Select Resource Manager Essentials > Configuration Management > Network Show Commands > Batch Reports > Schedule Reports.
View report output.	View the output of a batch report.	Select Resource Manager Essentials > Configuration Management > Network Show Commands > Batch Reports > View Report Output.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 177
Doc 3702

Table 2-9 Network Show Commands Tasks (continued)

Task	Purpose	Action
Browse network show jobs.	Browse the network show jobs that are registered on the system and view job details. You can also edit or delete jobs.	1. Select Resource Manager Essentials > Configuration Management > Network Show Commands > Batch Reports > Job Browser. 2. Select a job record. 3. Click Edit Job, Stop Job, Remove Job, Copy Job, or Job Details.
Set job policies.	Each network show job has properties that define how the job runs. You can configure a default policy for these properties that apply to all future jobs.	Select Resource Manager Essentials > Configuration Management > Network Show Commands > Batch Reports > Set Job Policies.
Use the **cwconfig netshow** command.	Define and execute command sets command sets to be run against a set of devices.	Enter the **cwconfig netshow** command at the command line. For more information, see the online help and the cwconfig netshow man page.
Use the **cwconfig netshow** batch command.	Define and schedule reports, comprising multiple network show command sets to be run against a set of devices.	Enter the **cwconfig netshow** batch command at the command line. For more information, see the online help and the cwconfig netshowbatch man page.

Config Editor Option

You can edit configuration files stored in the Configuration Archive and download files to devices, using the Config Editor option. This option runs as a separate application in its own window.

RQS nº 03/2005 CN
CPMI - CORREIOS
Fls Nº 178
Doc 3702

16-555

New Features of Config Editor

Config Editor has the following new features:

- Job Password Option
- Multiple Selection of Jobs for Deletion
- Separate Protocol Ordering for Configuration Download and Fetch Operations
- Support for Interactive Commands

For more details, see the Essentials online help.

Job Password Option

Essentials stores passwords in the database. While the job is run, the password is retrieved from the database for each of the selected devices.
For example, if the TACACS server is managing the devices, the passwords in the TACACS server and the passwords in the Essentials database should be synchronized (with every password change).

You now have the option of entering a username and password for running a specific job. If you enter a username and password, Config Editor uses this username and password to connect to the device, instead of taking these credentials from the Essentials database.

This option of entering the username and password for job execution is useful in high security installations where device passwords are changed at frequent intervals. In such instances, the passwords may be changed every 60-90 seconds.

To use this option of entering a username and password for running a specific job, you should enable the job password policy for Config Editor jobs using the Password Policy tab of the Configuration Job Setup dialog box, in the Configuration Management application. To invoke the Configuration Job Setup dialog box, select **Resource Manager Essentials > Administration > Configuration Management > Configuration Job Setup**.

You can also set the job password to be mandatory, or user configurable.

If you do not enable the job password policy, then Config Editor takes the device credentials from the Essentials database to connect to the device.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 179
Doc 3702

1652
2

Segurança Tipo 1 doc 7

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 180
Doc. 3702

CHAPTER 3

A through B Commands

aaa accounting

Enable, disable, or view LOCAL, TACACS+, or RADIUS user accounting (on a server designated by the **aaa-server** command). (Configuration mode.)

Configure with the command...	Remove with the command...
aaa accounting include | exclude *acctg_service* **inbound | outbound |** *if_name local_ip local_mask foreign_ip foreign_mask group_tag*	**no aaa accounting include | exclude** *authen_service* **inbound | outbound |** *if_name group_tag* **clear aaa** [**accounting include | exclude** *authen_service* **inbound | outbound |** *if_name group_tag*]
aaa accounting match *acl_name* **inbound | outbound |** *if_name group_tag*	**no aaa accounting match** *acl_name* **inbound | outbound |** *if_name group_tag*

Show command options	Show command output
show aaa	Displays the AAA authentication configuration.

Syntax Description

accounting	Enable or disable accounting services with authentication server. Use of this command requires that you previously used the **aaa-server** command to designate an authentication server.
acctg_service	The accounting service. Accounting is provided for all services or you can limit it to one or more services. Possible values are **any**, **ftp**, **http**, **telnet**, or *protocol/port*. Use **any** to provide accounting for all TCP services. To provide accounting for UDP services, use the *protocol/port* form. For *protocol/port*, the TCP *protocol* appears as 6, the UDP protocol appears as 17, and so on, and port is the TCP or UDP destination port. A port value of 0 (zero) means all ports. For protocols other than TCP and UDP, the *port* is not applicable and should not be used.
foreign_ip	The IP address of the hosts you want to access the *local_ip* address. Use 0 to mean all hosts.

IRQS nº 03/2005 - CN
CPMI - CORREIOS
181
Doc. 3702

foreign_mask	Network mask of *foreign_ip*. Always specify a specific mask value. Use 0 if the IP address is 0. Use 255.255.255.255 for a host.
exclude	Create an exception to a previously stated rule by excluding the specified service from authentication, authorization, or accounting to the specified host. The **exclude** parameter improves the former **except** option by allowing the user to specify a port to exclude to a specific host or hosts.
group_tag	The AAA server group tag defined by the **aaa-server** command. To use the local PIX Firewall user authentication database, enter **LOCAL** for this parameter.
if_name	Interface name from which users require authentication. Use *if_name* in combination with the *local_ip* address and the *foreign_ip* address to determine where access is sought and from whom. The *local_ip* address is always on the highest security level interface and *foreign_ip* is always on the lowest.
include	Create a new rule with the specified service to include.
inbound	Authenticate or authorize inbound connections. Inbound means the connection originates on the outside interface and is being directed to the inside interface.
local_ip	The IP address of the host or network of hosts that you want to be authenticated or authorized. You can set this address to **0** to mean all hosts and to let the authentication server decide which hosts are authenticated.
local_mask	Network mask of *local_ip*. Always specify a specific mask value. Use 0 if the IP address is 0. Use 255.255.255.255 for a host.
match *acl_name*	Specify an **access-list** command statement name.
outbound	Authenticate or authorize outbound connections. Outbound means the connection originates on the inside and is being directed to the outside interface.

Usage Guidelines

User accounting services keep a record of which network services a user has accessed. These records are also kept on the designated AAA server. Accounting information is only sent to the active server in a server group.

Use the **aaa accounting** command with the **aaa authentication** and **aaa authorization** commands.

The **include** and **exclude** options are not backward compatible with previous PIX Firewall versions. If you downgrade to an earlier version, the **aaa** command statements will be removed from your configuration.

Note Traffic that is not specified by an **include** statement is not processed.

For outbound connections, first use the **nat** command to determine which IP addresses can access the PIX Firewall. For inbound connections, first use the **static** and **access-list** command statements to determine which inside IP addresses can be accessed through the PIX Firewall from the outside network.

If you want to allow connections to come from any host, code the local IP address and netmask as **0.0.0.0 0.0.0.0**, or **0 0**. The same convention applies to the foreign host IP address and netmask; **0.0.0.0 0.0.0.0** means any foreign host.

Tip The **help aaa** command displays the syntax and usage for the **aaa authentication**, **aaa authorization**, **aaa accounting**, and **aaa proxy-limit** commands in summary form.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 182
Doc 3702

Examples

The default PIX Firewall configuration provides the following **aaa-server** protocols:

```
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server LOCAL protocol local
```

The following example uses the default protocol TACACS+ with the **aaa** commands:

```
aaa-server TACACS+ (inside) host 10.1.1.10 thekey timeout 20
aaa authentication include any outbound 0 0 0 0 TACACS+
aaa authorization include any outbound 0 0 0 0
aaa accounting include any outbound 0 0 0 0 TACACS+
aaa authentication serial console TACACS+
```

This example specifies that the authentication server with the IP address 10.1.1.10 resides on the inside interface and is in the default TACACS+ server group. The next three command statements specify that any users starting outbound connections to any foreign host will be authenticated using TACACS+, that the users who are successfully authenticated are authorized to use any service, and that all outbound connection information will be logged in the accounting database. The last command statement specifies that access to the PIX Firewall unit's serial console requires authentication from the TACACS+ server.

Related Commands

- **aaa authorization**
- **auth-prompt**
- **service**
- **ssh**
- **telnet**
- **virtual**

aaa authentication

Enable, disable, or view LOCAL, TACACS+, or RADIUS user authentication (on a server designated by the **aaa-server** command). Additionally, the **aaa authentication** command has been modified to support PDM authentication. (Configuration mode.)

Configure with the command...	Remove with the command...
aaa authentication include | exclude *authen_service* **inbound | outbound |** *if_name local_ip local_mask foreign_ip foreign_mask group_tag*	**no aaa authentication** [**include | exclude** *authen_service* **inbound | outbound |** *if_name local_ip local_mask foreign_ip foreign_mask group_tag*] **clear aaa** [**authentication include | exclude** *authen_service* **inbound | outbound |** *if_name local_ip local_mask foreign_ip foreign_mask group_tag*]
aaa authentication match *acl_name* **inbound | outbound |** *if_name group_tag*	**no aaa authentication match** *acl_name* **inbound | outbound |** *if_name group_tag*
aaa authentication [**serial | enable | telnet | ssh | http**] **console** *group_tag*	**no aaa authentication** [**serial | enable | telnet | ssh | http**] **console** *group_tag*

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 183
Nº 3702

Show command options	Show command output
show aaa	Displays the AAA authentication configuration.

Syntax Description

authen_service	The application with which a user is accessing a network. Use **any**, **ftp**, **http**, or **telnet**. The **any** value enables accounting or authentication for all TCP services. To have users prompted for authentication credentials, they must use FTP, HTTP, or Telnet. (HTTP is the Web and only applies to web browsers that can prompt for a username and password.) If the authentication or authorization server is authenticating services other than FTP, HTTP, or Telnet, using **any** will not permit those services to authenticate in the firewall. The firewall only knows how to communicate with FTP, HTTP, and Telnet for authentication and authorization. Only set this parameter to a service other than **any** if the authentication or authorization server is set the same way. Unless you want to temporarily restrict access to a specific service, setting a service in this command can increase system administration work and may cause all connections to fail if the authentication or authorization server is authenticating one service and you set this command to another.
authentication	Enable or disable user authentication, prompt user for username and password, and verify information with authentication server. When used with the **console** option, enables or disables authentication service for access to the PIX Firewall console over Telnet or from the Console connector on the PIX Firewall unit. Use of the **aaa authentication** command requires that you previously used the **aaa-server** command to designate an authentication server. The **aaa authentication** command supports HTTP authentication. The PIX Firewall requires authentication verification of the HTTP server through the **aaa authentication http console** command before PDM can access the PIX Firewall.
console	Specify that access to the PIX Firewall console require authentication and optionally, log configuration changes to a syslog server. The maximum password length for accessing the console is 16 characters.
enable	Access verification for the PIX Firewall unit's privilege mode.
exclude	Create an exception to a previously stated rule by excluding the specified service from authentication, authorization, or accounting to the specified host. The **exclude** parameter improves the former **except** option by allowing the user to specify a port to exclude to a specific host or hosts.
foreign_ip	The IP address of the hosts you want to access the *local_ip* address. Use 0 to mean all hosts.
foreign_mask	Network mask of *foreign_ip*. Always specify a specific mask value. Use 0 if the IP address is 0. Use 255.255.255.255 for a host.
group_tag	The AAA server group tag defined by the **aaa-server** command. To use the local PIX Firewall user authentication database, enter **LOCAL** for this parameter.

RQS nº 03/2005 - CN
CPMI - CORREIOS
184
Fls Nº
Doc 3702

http	Access verification for the HTTP (Hypertext Transfer Protocol) access to the PIX Firewall (via PDM). The maximum username prompt for HTTP authentication is 30 characters. The maximum password length is 15 characters.
if_name	The interface name from which to authenticate users.
inbound	Authenticate or authorize inbound connections. Inbound means the connection originates on the outside interface and is being directed to the inside interface.
include	Create a new rule with the specified service to include.
local_ip	The IP address of the host or network of hosts that you want to be authenticated or authorized. You can set this address to **0** to mean all hosts and to let the authentication server decide which hosts are authenticated.
local_mask	Network mask of *local_ip*. Always specify a specific mask value. Use 0 if the IP address is 0. Use 255.255.255.255 for a host.
match *acl_name*	Specify an **access-list** command statement name.
outbound	Authenticate or authorize outbound connections. Outbound means the connection originates on the inside and is being directed to the outside interface.
serial	Access verification for the PIX Firewall unit's serial console.
ssh	Access verification for the SSH access to the PIX Firewall console.
telnet	Access verification for the Telnet access to the PIX Firewall console.

Defaults

If an **aaa authentication http console** *group_tag* command statement is not defined, you can gain access to the PIX Firewall (via PDM) with no username and the PIX Firewall enable password (set with the **password** command). If the **aaa** commands are defined but the HTTP authentication requests a time out, which implies the AAA servers may be down or not available, you can gain access to the PIX Firewall using the username **pix** and the enable password. By default, the enable password is not set.

PIX Firewall supports authentication usernames up to 127 characters and passwords of up to 63 characters. A password or username may not contain an "@" character as part of the password or username string, with a few exceptions.

Tip The **help aaa** command displays the syntax and usage for the **aaa authentication**, **aaa authorization**, **aaa accounting**, and **aaa proxy-limit** commands in summary form.

Usage Guidelines

To use the **aaa authentication** command, you must first designate an authentication server with the **aaa-server** command. Also, for each IP address, one **aaa authentication** command is permitted for inbound connections and one for outbound connections.

Use the *if_name*, *local_ip*, and *foreign_ip* variables to define where access is sought and from whom. The address for *local_ip* is always on the highest security level interface and *foreign_ip* is always on the lowest.

The **aaa authentication** command is not intended to mandate your security policy. The authentication servers determine whether a user can or cannot access the system, what services can be accessed, and what IP addresses the user can access. The PIX Firewall interacts with FTP, HTTP (Web access), and

RQS nº 03/2005 CN
CPMI - CORREIOS
185
Fls. Nº
3702

Telnet to display the credentials prompts for logging in to the network or logging in to exit the network. You can specify that only a single service be authenticated, but this must agree with the authentication server to ensure that both the firewall and server agree.

The **include** and **exclude** options are not backward compatible with previous PIX Firewall versions. If you downgrade to an earlier version, these **aaa authentication** command statements will be removed from your configuration.

The aaa authentication console Command

The **aaa authentication serial console** command allows you to require authentication verification to access the PIX Firewall unit's serial console. The **serial console** options also logs to a syslog server changes made to the configuration from the serial console.

Authenticated access to the PIX Firewall console has different types of prompts depending on the option you choose with the **aaa authentication [serial | enable | telnet | ssh] console** command. While the **enable** and **ssh** options allow three tries before stopping with an access denied message, both the **serial** and **telnet** options cause the user to be prompted continually until successfully logging in. The **serial** option requests a username and password before the first command line prompt on the serial console connection. The **telnet** option forces you to specify a username and password before the first command line prompt of a Telnet console connection. The **enable** option requests a username and password before accessing privileged mode for serial, Telnet, or SSH connections. The **ssh** option requests a username and password before the first command line prompt on the SSH console connection. The **ssh** option allows a maximum of three authentication attempts.

Telnet access to the PIX Firewall console is available from any internal interface, and from the outside interface with IPSec configured, and requires previous use of the **telnet** command. SSH access to the PIX Firewall console is also available from any interface without IPSec configured, and requires previous use of the **ssh** command.

The new **ssh** option specifies the group of AAA servers to be used for SSH user authentication. The authentication protocol and AAA server IP addresses are defined with the **aaa-server** command statement.

Similar to the Telnet model, if an **aaa authentication ssh console** *group_tag* command statement is not defined, you can gain access to the PIX Firewall console with the username **pix** and with the PIX Firewall Telnet password (set with the **passwd** command). If the **aaa** command is defined but the SSH authentication requests timeouts, which implies the AAA servers may be down or not available, you can gain access to the PIX Firewall using username **pix** and the enable password (set with the **enable password** command). By default, the Telnet password is **cisco** and the enable password is not set.

If the console login request times out, you can gain access to the PIX Firewall from the serial console by entering the **pix** username and the enable password.

Enabling Authentication

The **aaa authentication** command enables or disables the following AAA (authentication, authorization, and accounting) features:

- User authentication services provided by a TACACS+ or RADIUS server are first designated with the **aaa authorization** command. A user starting a connection via FTP, Telnet, or over the World Wide Web is prompted for their username and password. If the username and password are verified by the designated TACACS+ or RADIUS authentication server, the PIX Firewall unit will allow further traffic between the authentication server and the connection to interact independently through the PIX Firewall unit's "cut-through proxy" feature.
- Administrative authentication services providing access to the PIX Firewall unit's console via Telnet, SSH, or the serial console. Telnet access requires previous use of the **telnet** command. SSH access requires previous use of the **ssh** command.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 186
Doc 3702

The prompts users see requesting AAA credentials differ between the three services that can access the PIX Firewall for authentication: Telnet, FTP, and HTTP (Web):

- Telnet users see a prompt generated by the PIX Firewall that you can change with the **auth-prompt** command. The PIX Firewall permits a user up to four chances to log in and then if the username or password still fails, the PIX Firewall drops the connection.
- FTP users receive a prompt from the FTP program. If a user enters an incorrect password, the connection is dropped immediately. If the username or password on the authentication database differs from the username or password on the remote host to which you are using FTP to access, enter the username and password in these formats:

  authentication_user_name@*remote_system_user_name*
  authentication_password@*remote_system_password*

  If you daisy-chain PIX Firewall units, Telnet authentication works in the same way as a single unit, but FTP and HTTP authentication have additional complexity for users because they have to enter each password and username with an additional at (@) character and password or username for each daisy-chained system. Users can exceed the 63-character password limit depending on how many units are daisy-chained and password length.

  Some FTP graphical user interfaces (GUIs) do not display challenge values.
- HTTP users see a pop-up window generated by the browser itself. If a user enters an incorrect password, the user is reprompted. When the web server and the authentication server are on different hosts, use the **virtual** command to get the correct authentication behavior.

Authenticated access to the PIX Firewall console has different types of prompts depending on the option you choose with the **aaa authentication console** command:

- **enable** option—Allows three tries before stopping with "Access denied." The **enable** option requests a username and password before accessing privileged mode for serial or Telnet connections.
- **serial** option—Causes the user to be prompted continually until successfully logging in. The **serial** option requests a username and password before the first command line prompt on the serial console connection.
- **ssh** option—Allows three tries before stopping with "Rejected by Server." The **ssh** option requests a username and password before the first command line prompt appears.
- **telnet** option—Causes the user to be prompted continually until successfully logging in. The **telnet** option forces you to specify a username and password before the first command line prompt of a Telnet console connection.

You can specify an interface name with the **aaa authentication** command. In previous versions, if you specified **aaa authentication include any outbound 0 0** *server*, PIX Firewall only authenticated outbound connections and not those to the perimeter interface. PIX Firewall now authenticates any outbound connection to the outside as well as to hosts on the perimeter interface. To preserve the behavior of previous versions, use these commands to enable authentication and to disable authentication from the inside to the perimeter interface:

```
aaa authentication include any outbound 0 0 server
aaa authentication exclude outbound perim_net perim_mask server
```

When a host is configured for authentication, all users on the host must use a web browser or Telnet first before performing any other networking activity, such as accessing mail or a news reader. The reason for this is that users must first establish their authentication credentials and programs such as mail agents and newsreaders do not have authentication challenge prompts.

RQS nº 03/2005 CN
CPMI - CORREIOS
Fls. Nº 187
Doc 3702

The PIX Firewall only accepts 7-bit characters during authentication. After authentication, the client and server can negotiate for 8 bits if required. During authentication, the PIX Firewall only negotiates Go-Ahead, Echo, and NVT (network virtual terminal).

HTTP Authentication

When using HTTP authentication to a site running Microsoft IIS that has "Basic text authentication" or "NT Challenge" enabled, users may be denied access from the Microsoft IIS server. This occurs because the browser appends the string: "Authorization: Basic=Uuhjksdkfhk==" to the HTTP GET commands. This string contains the PIX Firewall authentication credentials.

Windows NT Microsoft IIS servers respond to the credentials and assume that a Windows NT user is trying to access privileged pages on the server. Unless the PIX Firewall username password combination is exactly the same as a valid Windows NT username and password combination on the Microsoft IIS server, the HTTP GET command is denied.

To solve this problem, PIX Firewall provides the **virtual http** command, which redirects the browser's initial connection to another IP address, authenticates the user, then redirects the browser back to the URL which the user originally requested.

Once authenticated, a user never has to reauthenticate no matter how low the PIX Firewall uauth timeout is set. This is because the browser caches the "Authorization: Basic=Uuhjksdkfhk==" string in every subsequent connection to that particular site. This can *only* be cleared when the user exits *all* instances of Netscape Navigator or Internet Explorer and restarts. Flushing the cache is of no use.

As long as the user repeatedly browses the Internet, the browser resends the "Authorization: Basic=Uuhjksdkfhk==" string to transparently reauthenticate the user.

Multimedia applications such as CU-SeeMe, Intel Internet Phone, MeetingPoint, and MS Netmeeting silently start the HTTP service before an H.323 session is established from the inside to the outside.

Network browsers such as Netscape Navigator do not present a challenge value during authentication; therefore, only password authentication can be used from a network browser.

Note To avoid interfering with these applications, do not enter blanket outgoing **aaa** command statements for all challenged ports such as using the **any** option. Be selective with which ports and addresses you use to challenge HTTP, and when to set user authentication timeouts to a higher timeout value. If interfered with, the multimedia programs may fail on the PC and may even crash the PC after establishing outgoing sessions from the inside.

TACACS+ and RADIUS servers

Up to 196 TACACS+ or RADIUS servers are permitted (up to 14 servers in each of the up to 14 server groups—set with the **aaa-server** command). When a user logs in, the servers are accessed one at a time starting with the first server you specify in the configuration, until a server responds.

The PIX Firewall permits only one authentication type per network. For example, if one network connects through the PIX Firewall using TACACS+ for authentication, another network connecting through the PIX Firewall can authenticate with RADIUS, but one network cannot authenticate with both TACACS+ and RADIUS.

For the TACACS+ server, if you do not specify a key to the **aaa-server** command, no encryption occurs.

The PIX Firewall displays the same timeout message for both RADIUS and TACACS+. The message "aaa server host machine not responding" displays when either of the following occurs:

- The AAA server system is down.
- The AAA server system is up, but the service is not running.

RQS nº 03/2005 CN
CPMI CORREIOS
Fls Nº 188
Doc 3702

Previously, TACACS+ differentiated between the two preceding states and provided two different timeout messages, while RADIUS did not differentiate between the two states and provided one timeout message.

match *acl_name* Option Usage

The syntax for this command is as follows:

aaa authentication | authorization | accounting match *acl_name* **inbound | outbound |** *interface_name group_tag*

An example follows:

```
show access-list
access-list mylist permit tcp 10.0.0.0 255.255.255.0 172.23.2.0 255.255.255.0 (hitcnt=0)
access-list yourlist permit tcp any any (hitcnt=0)
show aaa
aaa authentication match mylist outbound TACACS+
```

Similar to IPSec, the keyword **permit** means "yes" and **deny** means "no." Therefore, the following command,

```
aaa authentication match yourlist outbound tacacs
```

is equal to this command:

```
aaa authentication include any outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 tacacs
```

The **aaa** command statement list is order dependent between **access-list** command statements. If the following command is entered:

```
aaa authentication match yourlist outbound tacacs
```

after this command:

```
aaa authentication match mylist outbound TACACS+
```

PIX Firewall tries to find a match in the mylist **access-list** command statement group before it tries to find a match in the yourlist **access-list** command statement group.

Old **aaa** command configuration and functionality stays the same and is not converted to the **access-list** format. Hybrid configurations; that is, old configurations combined with the new **access-list** configuration are not recommended.

Examples

The following example shows use of the **aaa authentication** command:

```
pixfirewall(config) aaa authentication telnet console radius
```

ROS nº 03/2005 CN
CPMI - CORREIOS
189
Fls Nº
Doc 3702

The following example lists the new include and exclude options:

```
aaa authentication include any outbound 172.31.0.0 255.255.0.0 0.0.0.0 0.0.0.0 tacacs+
aaa authentication exclude telnet outbound 172.31.38.0 255.255.255.0 0.0.0.0 0.0.0.0
tacacs+
```

The following examples demonstrate ways to use the *if_name* parameter. The PIX Firewall has an inside network of 192.168.1.0, an outside network of 209.165.201.0 (subnet mask 255.255.255.224), and a perimeter network of 209.165.202.128 (subnet mask 255.255.255.224).

This example enables authentication for connections originated from the inside network to the outside network:

```
aaa authentication include any outbound 192.168.1.0 255.255.255.0 209.165.201.0
255.255.255.224 tacacs+
```

This example enables authentication for connections originated from the inside network to the perimeter network:

```
aaa authentication include any outbound 192.168.1.0 255.255.255.0 209.165.202.128
255.255.255.224 tacacs+
```

This example enables authentication for connections originated from the outside network to the inside network:

```
aaa authentication include any inbound 192.168.1.0 255.255.255.0 209.165.201.0
255.255.255.224 tacacs+
```

This example enables authentication for connections originated from the outside network to the perimeter network:

```
aaa authentication include any inbound 209.165.201.0 255.255.255.224 209.165.202.128
255.255.255.224 tacacs+
```

This example enables authentication for connections originated from the perimeter network to the outside network:

```
aaa authentication include any outbound 209.165.202.128 255.255.255.224 209.165.201.0
255.255.255.224 tacacs+
```

This example specifies that IP addresses 10.0.0.1 through 10.0.0.254 can originate outbound connections and then enables user authentication so that those addresses must enter user credentials to exit the PIX Firewall. In this example, the first **aaa authentication** command permits authentication on FTP, HTTP, or Telnet depending on what the authentication server handles. The second **aaa authentication** command lets host 10.0.0.42 start outbound connections without being authenticated. This example uses the default authentication group **tacacs+**.

```
nat (inside) 1 10.0.0.0 255.255.255.0
aaa authentication include any outbound 0 0 tacacs+
aaa authentication exclude outbound 10.0.0.42 255.255.255.255 tacacs+ any
```

This example permits inbound access to any IP address in the range of 209.165.201.1 through 209.165.201.30 indicated by the 209.165.201.0 network address (subnet mask 255.255.255.224). All services are permitted by the **access-list** command, and the **aaa authentication** command permits authentication on FTP, HTTP, or Telnet depending on what the authentication server handles. The authentication server is at IP address 10.16.1.20 on the inside interface.

```
aaa-server AuthIn protocol tacacs+
aaa-server AuthIn (inside) host 10.16.1.20 thisisakey timeout 20
static (inside,outside) 209.165.201.0 10.16.1.0 netmask 255.255.255.224
access-list acl_out permit tcp 10.16.1.0 255.255.255.0 209.165.201.0 255.255.255.224
access-group acl_out in interface outside
aaa authentication include any inbound 0 0 AuthIn
```

RQS nº 03/2005 CN
CPMI CORREIOS
Fls Nº 190
Doc 3702

Related Commands

- **aaa authorization**
- **auth-prompt**
- **service**
- **ssh**
- **telnet**
- **virtual**

aaa authorization

Enable or disable LOCAL or TACACS+ user authorization services. (Configuration mode.)

Configure with the command...	Remove with the command...
aaa authorization command {**LOCAL** | *tacacs_server_tag*}	**no aaa authorization command** {**LOCAL** | *tacacs_server_tag*}
aaa authorization include | **exclude** *author_service* **inbound** | **outbound** | *if_name local_ip local_mask foreign_ip foreign_mask*	**no aaa authorization** [**include** | **exclude** *author_service* **inbound** | **outbound** | *if_name local_ip local_mask foreign_ip foreign_mask*] **clear aaa** [**authorization** [**include** | **exclude** *author_service* **inbound** | **outbound** | *if_name local_ip local_mask foreign_ip foreign_mask*]]
aaa authorization match *acl_name* **inbound** | **outbound** | *if_name group_tag*	**no aaa authorization match** *acl_name* **inbound** | **outbound** | *if_name group_tag*

Show command options	Show command output
show aaa	Displays the AAA authentication configuration.

RQS nº 03/2005 CN
CPMI – CORREIOS
191
Fls. Nº
Doc 3702

Syntax Description

authorization	Enable or disable TACACS+ user authorization for services (PIX Firewall does not support RADIUS authorization). The authentication server determines what services the user is authorized to access.
author_service	The services which require authorization. Use **any**, **ftp**, **http**, **telnet**, or *protocol/port*. Use **any** to provide authorization for all TCP services. To provide authorization for UDP services, use the *protocol/port* form. Services not specified are authorized implicitly. Services specified in the **aaa authentication** command do not affect the services which require authorization. For *protocol/port*: • *protocol*—the protocol (6 for TCP, 17 for UDP, 1 for ICMP, and so on). • *port*—the TCP or UDP destination port, or port range. The *port* can also be the ICMP type; that is, 8 for ICMP echo or ping. A port value of 0 (zero) means all ports. Port ranges only applies to the TCP and UDP protocols, not to ICMP. For protocols other than TCP, UDP, and ICMP the *port* is not applicable and should not be used. An example port specification follows. `aaa authorization include udp/53-1024 inside 0 0 0 0` This example enables authorization for DNS lookups to the inside interface for all clients, and authorizes access to any other services that have ports in the range of 53 to 1024. **Note** Specifying a port range may produce unexpected results at the authorization server. PIX Firewall sends the port range to the server as a string with the expectation that the server will parse it out into specific ports. Not all servers do this. In addition, you may want users to be authorized on specific services, which will not occur if a range is accepted.
foreign_ip	The IP address of the hosts you want to access the *local_ip* address. Use 0 to mean all hosts.
foreign_mask	Network mask of *foreign_ip*. Always specify a specific mask value. Use 0 if the IP address is 0. Use 255.255.255.255 for a host.
exclude	Create an exception to a previously stated rule by excluding the specified service from authentication, authorization, or accounting to the specified host. The **exclude** parameter improves the former **except** option by allowing the user to specify a port to exclude to a specific host or hosts.
group_tag	Specifies the AAA server. Enter **LOCAL** for the group tag value for local AAA services such as local command authorization using privilege levels, or use the AAA server group tag as defined by the **aaa-server** command.
if_name	Interface name from which users require authentication. Use *if_name* in combination with the *local_ip* address and the *foreign_ip* address to determine where access is sought and from whom. The *local_ip* address is always on the highest security level interface and *foreign_ip* is always on the lowest.
include	Create a new rule with the specified service to include.

RQS nº 03/2005 CN
CPMI CORREIOS
Fls Nº 192
Doc 3702

inbound	Authenticate or authorize inbound connections. Inbound means the connection originates on the outside interface and is being directed to the inside interface.
LOCAL	Specifies to use the PIX Firewall local user database for local command authorization (using privilege levels).
local_ip	The IP address of the host or network of hosts that you want to be authenticated or authorized. You can set this address to **0** to mean all hosts and to let the authentication server decide which hosts are authenticated.
local_mask	Network mask of *local_ip*. Always specify a specific mask value. Use 0 if the IP address is 0. Use 255.255.255.255 for a host.
match *acl_name*	Specify an **access-list** command statement name.
outbound	Authenticate or authorize outbound connections. Outbound means the connection originates on the inside and is being directed to the outside interface.
tacacs_server_tag	Specifies to use a TACACS user authentication server.

Usage Guidelines

Except for its use with command authorization, the **aaa authorization** command requires previous configuration with the **aaa authentication** command; however, use of the **aaa authentication** command does not require use of an **aaa authorization** command.

Currently, the **aaa authorization** command is supported for use with LOCAL and TACACS+ servers but not with RADIUS servers.

Tip The **help aaa** command displays the syntax and usage for the **aaa authentication**, **aaa authorization**, **aaa accounting**, and **aaa proxy-limit** commands in summary form.

For each IP address, one **aaa authorization** command is permitted. If you want to authorize more than one service with **aaa authorization**, use the **any** parameter for the service type.

If the first attempt at authorization fails and a second attempt causes a timeout, use the **service resetinbound** command to reset the client that failed the authorization so that it will not retransmit any connections. An example authorization timeout message in Telnet follows.

```
Unable to connect to remote host: Connection timed out
```

User authorization services control which network services a user can access. After a user is authenticated, attempts to access restricted services cause the PIX Firewall unit to verify the access permissions of the user with the designated AAA server.

The **include** and **exclude** options are not backward compatible with previous PIX Firewall versions. If you downgrade to an earlier version, the **aaa** command statements will be removed from your configuration.

Note RADIUS authorization is supported for use with **access-list** command statements and for use in configuring a RADIUS server with an **acl=***acl_name* vendor-specific identifier. Refer to the **access-list** command page for more information. Also see the **aaa-server radius-authport** commands.

If the AAA console login request times out, you can gain access to the PIX Firewall from the serial console by entering the **pix** username and the enable password.

RQS nº 03/2005 - CN
CPMI - CORREIOS
193
Doc 3702

Examples

The default PIX Firewall configuration provides the following **aaa-server** protocols:

```
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server LOCAL protocol local
```

The following example uses the default protocol TACACS+ with the **aaa** commands:

```
aaa-server TACACS+ (inside) host 10.1.1.10 thekey timeout 20
aaa authentication include any outbound 0 0 0 0 TACACS+
aaa authorization include any outbound 0 0 0 0
aaa accounting include any outbound 0 0 0 0 TACACS+
aaa authentication serial console TACACS+
```

This example specifies that the authentication server with the IP address 10.1.1.10 resides on the inside interface and is in the default TACACS+ server group. The next three command statements specify that any users starting outbound connections to any foreign host will be authenticated using TACACS+, that the users who are successfully authenticated are authorized to use any service, and that all outbound connection information will be logged in the accounting database. The last command statement specifies that access to the PIX Firewall unit's serial console requires authentication from the TACACS+ server.

The following example enables authorization for DNS lookups from the outside interface:

```
aaa authorization include udp/53 inbound 0.0.0.0 0.0.0.0
```

The following example enables authorization of ICMP echo-reply packets arriving at the inside interface from inside hosts:

```
aaa authorization include 1/0 outbound 0.0.0.0 0.0.0.0
```

This means that users will not be able to ping external hosts if they have not been authenticated using Telnet, HTTP, or FTP.

The following example enables authorization for ICMP echoes (pings) only that arrive at the inside interface from an inside host:

```
aaa authorization include 1/8 outbound 0.0.0.0 0.0.0.0
```

Related Commands

- **aaa authorization**
- **auth-prompt**
- **service**
- **ssh**
- **telnet**
- **virtual**

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 194
Doc 3702

aaa proxy-limit

Specifies the number of concurrent proxy connections allowed per user. (Configuration mode.)

Configure with the command...	Remove with the command...
aaa proxy-limit *proxy_limit* | **disable**	**no aaa-server** *group_tag* (*if_name*) **host** *server_ip key* **timeout** *seconds* **clear aaa-server** [*group_tag*]

Show command options	Show command output
show aaa proxy-limit	Displays the number of outstanding authentication requests allowed, or indicates that the proxy limit is disabled if disabled.

Syntax Description

disable	Disables the proxy limit.
group_tag	Specifies the AAA server. Enter **LOCAL** for the group tag value for local AAA services such as local command authorization using privilege levels, or use the AAA server group tag as defined by the **aaa-server** command.
proxy_limit	Specifies the number of concurrent proxy connections allowed per user, from 1 to 128. (The default value is 3.)

Usage Guidelines

The **aaa proxy-limit** command enables you to manually configure the uauth session limit by setting the maximum number of concurrent proxy connections allowed per user. By default, this value is set to 3. If a source address is a proxy server, consider excluding this IP address from authentication or increasing the number of allowable outstanding AAA requests.

Examples

The following example shows how to set and display the maximum number of outstanding authentication requests allowed:

```
pixdoc515(config)# aaa proxy-limit 6
pixdoc515(config)# show aaa proxy-limit
aaa proxy-limit 6
```

RQS nº 03/2005 CN
CPMI CORREIOS
195
Doc 3702

aaa-server

Specify an AAA server. (Configuration mode.)

Configure with the command...	Remove with the command...
aaa-server *group_tag* (*if_name*) **host** *server_ip key* **timeout** *seconds*	**no aaa-server** *group_tag* (*if_name*) **host** *server_ip key* **timeout** *seconds* **clear aaa-server** [*group_tag*]
aaa-server *group_tag* **protocol** *auth_protocol*	**N/A**
aaa-server radius-acctport *port*	**N/A**
aaa-server radius-authport *port*	**N/A**
debug radius session	**N/A**
show aaa-server	**N/A**

Show command options	Show command output
show aaa-server	Displays AAA server configuration.

Syntax Description

aaa-server	Specifies an AAA server or up to 14 groups of servers with a maximum of 14 servers each. Certain types of AAA services can be directed to different servers. Services can also be set up to fail over to multiple servers.
aaa-server radius-acctport	Sets the port number of the RADIUS server which the PIX Firewall unit will use for accounting functions. The default port number used for RADIUS accounting is **1646**.
aaa-server radius-authport	Sets the port number of the RADIUS server which the PIX Firewall will use for authentication functions. The default port number used for RADIUS authentication is **1645**.
debug radius session	Captures RADIUS session information and attributes for sent and received RADIUS packets.
group_tag	An alphanumeric string which is the name of the server group. Use the *group_tag* in the **aaa** command to associate **aaa authentication** and **aaa accounting** command statements to an AAA server. Up to 14 server groups are permitted. However, **LOCAL** cannot used with **aaa-server** command because **LOCAL** is predefined by the PIX Firewall.
host *server_ip*	The IP address of the TACACS+ or RADIUS server.
if_name	The interface name on which the server resides.
key	A case-sensitive, alphanumeric keyword of up to 127 characters that is the same value as the key on the TACACS+ server. Any characters entered past 127 are ignored. The key is used between the client and server for encrypting data between them. The *key* must be the same on both the client and server systems. Spaces are not permitted in the key, but other special characters are.
no aaa-server	Unbinds an AAA server from and interface or host.

RQS nº 03/2005 - CN
CPMI CORREIOS
Fls Nº 196
Doc 3702

16495

port	Specifies the destination TCP/UDP port number of the remote RADIUS server host to which you wish to assign authentication or accounting functions for the PIX Firewall. These port pairs are listed as assigned to authentication and accounting services on RADIUS servers: • 1645 (authentication), 1646 (accounting) - default for PIX Firewall • 1812 (authentication), 1813 (accounting) - alternate You can view these and other commonly used port number assignments online at the following website: http://www.iana.org/assignments/port-numbers See "Ports" in Chapter 2, "Using PIX Firewall Commands" for additional information.
protocol *auth_protocol*	The type of AAA server, either **tacacs+** or **radius**.
timeout *seconds*	The timeout interval for the request. This is the time after which the PIX Firewall gives up on the request to the primary AAA server. If there is a standby AAA server, the PIX Firewall will send the request to the backup server. The retransmit timeout is currently set to 10 seconds and is not user configurable.

Usage Guidelines

The **aaa-server** command lets you specify AAA server groups. PIX Firewall lets you define separate groups of TACACS+ or RADIUS servers for specifying different types of traffic; such as, a TACACS+ server for inbound traffic and another for outbound traffic. Another use is where all outbound HTTP traffic will be authenticated by a TACACS+ server, and all inbound traffic will use RADIUS.

AAA server groups are defined by a tag name that directs different types of traffic to each authentication server. If the first authentication server in the list fails, the AAA subsystem fails over to the next server in the tag group. You can have up to 14 tag groups and each group can have up to 14 AAA servers for a total of up to 196 AAA servers.

If your RADIUS server uses ports 1812 for authentication and 1813 for accounting, you are required to reconfigure the PIX Firewall to use ports 1812 and 1813.

If accounting is in effect, the accounting information goes only to the active server.

If you are upgrading from a previous version of PIX Firewall and have **aaa** command statements in your configuration, using the default server groups lets you maintain backward compatibility with the **aaa** command statements in your configuration.

Usage Notes

1. The **aaa** command references the tag group. This is a global setting that takes effect when the RADIUS service is started.
2. The previous server type option at the end of the **aaa authentication** and **aaa accounting** commands has been replaced with the **aaa-server** group tag. Backward compatibility with previous versions is maintained by the inclusion of two default protocols for TACACS+ and RADIUS.
3. Changing authorization and accounting port settings is possible. By default, PIX Firewall listens for RADIUS on ports 1645 and 1646. If your RADIUS server uses ports 1812 and 1813, you may also reconfigure it to use ports 1812 and 1813 with the **aaa-server radius-authport** and **aaa-server radius-acctport** commands.

ROS nº 03/2005 - CN
CPMI - CORREIOS
197
Doc 3702

4. Newer RADIUS servers may use the port numbers 1812 and 1813 as defined in RFC 2138 and RFC 2139. If your server uses ports other than 1645 and 1646, then you should define ports using the **aaa-server radius-authport** and **aaa-server radius-acctport** commands prior to starting the RADIUS service with the **aaa-server** command.

Defaults

By default, the PIX Firewall listens for RADIUS on ports **1645** for authentication and **1646** for accounting. (The default ports are 1645 for authentication and 1646 for accounting as defined in RFC 2058.)

The default configuration provides the following **aaa-server** protocols:

```
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server LOCAL protocol local
```

Examples

The following example uses the default protocol TACACS+ with the **aaa** commands:

```
aaa-server TACACS+ (inside) host 10.1.1.10 thekey timeout 20
aaa authentication include any outbound 0 0 0 0 TACACS+
aaa authorization include any outbound 0 0 0 0
aaa accounting include any outbound 0 0 0 0 TACACS+
aaa authentication serial console TACACS+
```

This example specifies that the authentication server with the IP address 10.1.1.10 resides on the inside interface and is in the default TACACS+ server group. The next three command statements specify that any users starting outbound connections to any foreign host will be authenticated using TACACS+, that the users who are successfully authenticated are authorized to use any service, and that all outbound connection information will be logged in the accounting database. The last command statement specifies that access to the PIX Firewall unit's serial console requires authentication from the TACACS+ server.

This example creates the AuthOut and AuthIn server groups for RADIUS authentication and specifies that servers 10.0.1.40, 10.0.1.41, and 10.1.1.2 on the inside interface provide authentication. The servers in the AuthIn group authenticate inbound connections, the AuthOut group authenticates outbound connections.

```
aaa-server AuthIn protocol radius
aaa-server AuthIn (inside) host 10.0.1.40 ab timeout 20
aaa-server AuthIn (inside) host 10.0.1.41 abc timeout 4
aaa-server AuthOut protocol radius
aaa-server AuthOut (inside) host 10.1.1.2 abc123 timeout 15
aaa authentication include any inbound 0 0 0 0 AuthIn
aaa authentication include any outbound 0 0 0 0 AuthOut
```

The following example lists the commands that can be used to establish an Xauth crypto map:

```
ip address inside 10.0.0.1 255.255.255.0
ip address outside 168.20.1.5 255.255.255.0
ip local pool dealer 10.1.2.1-10.1.2.254
nat (inside) 0 access-list 80
aaa-server TACACS+ host 10.0.0.2 secret123
crypto ipsec transform-set pc esp-des esp-md5-hmac
crypto dynamic-map cisco 4 set transform-set pc
crypto map partner-map 20 ipsec-isakmp dynamic cisco
crypto map partner-map client configuration address initiate
crypto map partner-map client authentication TACACS+
crypto map partner-map interface outside
isakmp key cisco1234 address 0.0.0.0 netmask 0.0.0.0
isakmp client configuration address-pool local dealer outside
isakmp policy 8 authentication pre-share
```

RQS nº 03/2005 - CN
CPMI CORREIOS
Fls Nº 198
Doc 3702

```
isakmp policy 8 encryption des
isakmp policy 8 hash md5
isakmp policy 8 group 1
isakmp policy 8 lifetime 86400
```

The **aaa-server** command is used with the **crypto map** command to establish an authentication association so that VPN clients are authenticated when they access the PIX Firewall.

Related Commands

- **crypto ipsec**
- **isakmp**

access-group

Binds the access list to an interface. (Configuration mode.)

Configure with the command...	Remove with the command...
access-group *acl_ID* **in interface** *interface_name*	**no access-group** *acl_ID* **in interface** *interface_name* **clear access-group** [*acl_ID*]

Show command options	Show command output
show access-group [*acl_ID*]	Displays the current access list bound to the interfaces.

Syntax Description

acl_ID	The name associated with a given access list.
in interface	Filter inbound packets at the given interface.
interface_name	The name of the network interface.

Usage Guidelines

The access-group command binds an access list to an interface. The access list is applied to traffic inbound to an interface. If you enter the **permit** option in an **access-list** command statement, the PIX Firewall continues to process the packet. If you enter the **deny** option in an **access-list** command statement, PIX Firewall discards the packet and generates the following syslog message.

```
%PIX-4-106019: IP packet from source_addr to destination_addr, protocol protocol received
from interface interface_name deny by access-group acl_ID
```

Always use the **access-list** command with the **access-group** command.

Note The use of **access-group** command overrides the **conduit** and **outbound** command statements for the specified *interface_name*.

The **no access-group** command unbinds the *acl_ID* from the interface *interface_name*.

The **show access-group** command displays the current access list bound to the interfaces.

CPMI - CORREIOS
Fls Nº 199
Doc 3702

The **clear access-group** command removes all entries from an access list indexed by *acl_ID*. If *acl_ID* is not specified, all **access-list** command statements are removed from the configuration.

Examples

The following example shows use of the **access-group** command:

```
static (inside,outside) 209.165.201.3 10.1.1.3
access-list acl_out permit tcp any host 209.165.201.3 eq 80
access-group acl_out in interface outside
```

The **static** command statement provides a global address of 209.165.201.3 for the web server at 10.1.1.3. The **access-list** command statement lets any host access the global address using port 80. The **access-group** command specifies that the **access-list** command statement applies to traffic entering the outside interface.

access-list

Create an access list, or use downloadable access lists. (Downloadable access lists are supported for RADIUS servers only). (Configuration mode.)

Configure with the command...	Remove with the command...
access-list [*acl_ID*] **compiled**	**no access-list** [*acl_ID*] **compiled**
access-list *acl_ID* {**deny** | **permit**} **icmp** {*source_addr* | *local_addr*} {*source_mask* | *local_mask*} {*destination_addr* | *remote_addr*} {*destination_mask* | *remote_mask*} *icmp_type*	**no access-list** [*acl_ID* {**deny** | **permit**} **icmp** {*source_addr* | *local_addr*} {*source_mask* | *local_mask*} {*destination_addr* | *remote_addr*} {*destination_mask* | *remote_mask*} *icmp_type*]
access-list *id* {**deny** | **permit**} **icmp** {*source_addr* | *local_addr*} {*source_mask* | *local_mask*} | **object-group** *network_obj_grp_id* {*destination_addr* | *remote_addr*} {*destination_mask* | *remote_mask*} | **object-group** *network_obj_grp_id* [*icmp_type* | **object-group** *icmp_type_obj_grp_id*]	**no access-list** *id* {**deny** | **permit**} {**icmp** {*source_addr* | *local_addr*} {*source_mask* | *local_mask*} | **object-group** *network_obj_grp_id* {*destination_addr* | *remote_addr*} {*destination_mask* | *remote_mask*} | **object-group** *network_obj_grp_id* [*icmp_type* | **object-group** *icmp_type_obj_grp_id*]}
access-list *acl_ID* {**deny** | **permit**} *protocol* {*source_addr* | *local_addr*} {*source_mask* | *local_mask*}[*operator port* [*port*] {*destination_addr* | *remote_addr*} {*destination_mask* | *remote_mask*} [*operator port* [*port*]	**no access-list** *acl_ID* [{**deny** | **permit**} *protocol* {*source_addr* | *local_addr*} {*source_mask* | *local_mask*} [*operator port* [*port*] {*destination_addr* | *remote_addr*} {*destination_mask* | *remote_mask*} [*operator port* [*port*]]

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 200
Doc 3702

Configure with the command...	Remove with the command...
access-list *id* {**deny** | **permit**}{*protocol* | **object-group** *protocol_obj_grp_id* {*source_addr* | *local_addr*} {*source_mask* | *local_mask*} | **object-group** *network_obj_grp_id* [*operator port* [*port*] | **object-group** *service_obj_grp_id*] {*destination_addr* | *remote_addr*} {*destination_mask* | *remote_mask*} | **object-group** *network_obj_grp_id* [*operator port* [*port*] | **object-group** *service_obj_grp_id*]}	**no access-list** *id* {**deny** | **permit**} {*protocol* | **object-group** *protocol_obj_grp_id* {*source_addr* | *local_addr*} {*source_mask* | *local_mask*} | **object-group** *network_obj_grp_id* [*operator port* [*port*] | **object-group** *service_obj_grp_id*] {*destination_addr* | *remote_addr*} {*destination_mask* | *remote_mask*} | **object-group** *network_obj_grp_id* [*operator port* [*port*] | **object-group** *service_obj_grp_id*]}
debug access-list all | standard | turbo	**no debug access-list all | standard | turbo**
N/A	**clear access-list** [*acl_ID*]
N/A	**clear access-list** *acl_ID* **counters**

Show command options	Show command output
show access-list [[*acl_ID*] *source_addr*]	Displays the **access-list** command statements in the configuration, the hit count of the number of times each element has been matched during an **access-list** command search, and whether or not the list is configured for TurboACL. The *source_addr* option filters the show output so that only those access-list elements that match the source IP address (or with **any** as source IP address) are displayed.

Syntax Description

acl_ID	Name of an access list. You can use either a name or number.
compiled	When used in conjunction with the **access-list** command, this turns on TurboACL unless the **no** qualifier is used, in which case the command **no access-list** *acl_ID* **compiled** turns off TurboACL for that access list. To use TurboACL globally, enter the **access-list compiled** command and to globally turn off TurboACL, enter the **no access-list compiled** command. After TurboACL has been globally configured, individual access lists or groups can have TurboACL enabled or disabled using individual **[no] access-list** *acl_ID* **compiled** commands. TurboACL is compiled only if the number of access list elements is greater than or equal to 19.
debug	Outputs access list debugging information to the console.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 201
Doc 3702

deny	When used with the **access-group** command, the **deny** option does not allow a packet to traverse the PIX Firewall. By default, PIX Firewall denies all inbound or outbound packets unless you specifically permit access. When used with a **crypto map** command statement, **deny** does not select a packet for IPSec protection. The **deny** option prevents traffic from being protected by IPSec in the context of that particular crypto map entry. In other words, it does not allow the policy as specified in the **crypto map** command statements to be applied to this traffic.
destination_addr	IP address of the network or host to which the packet is being sent. Specify a *destination_addr* when the **access-list** command statement is used in conjunction with an **access-group** command statement, or with the **aaa match access-list** command and the **aaa authorization** command. For inbound and outbound connections, *destination_addr* is the address before NAT has been performed.
destination_mask	Netmask bits (mask) to be applied to *destination_addr*, if the destination address is a network mask.
icmp_type	For non-IPSec use only, permit or deny access to ICMP message types. Refer to Table 3-1 for a list of message types. Omit this option to mean all ICMP types. ICMP message types are not supported for use with IPSec; that is when the **access-list** command is used in conjunction with the **crypto map** command, the *icmp_type* is ignored.
local_addr	Address of the network or host local to the PIX Firewall. Specify a *local_addr* when the **access-list** command statement is used in conjunction with a **crypto access-list** command statement, a **nat 0 access-list** command statement, or a **vpngroup split-tunnel** command statement. The *local_addr* is the address after NAT has been performed.
local_mask	Netmask bits (mask) to be applied to *local_addr*, if the local address is a network mask.
object-group	Specifies an object group. Refer to the object-group command for information on how to configure object groups.
obj_grp_id	An existing object group.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 202
Doc 3702

operator	The *operator* compares the source IP address (*sip*) or destination IP address (*dip*) ports. Possible operands include **lt** for less than, **gt** for greater than, **eq** for equal, **neq** for not equal, and **range** for an inclusive range. Use the **access-list** command the without an operator and port to indicate all ports by default.
	
	For example,
	
	`access-list acl_out permit tcp any host 209.165.201.1`
	
	Use **eq** and a port to permit or deny access to just that port. For example, use **eq ftp** to permit or deny access only to FTP.
	
	`access-list acl_out deny tcp any host 209.165.201.1 eq ftp`
	
	Use **lt** and a port to permit or deny access to all ports less than the port you specify. For example, use **lt 2025** to permit or deny access to the well known ports (1 to 1024).
	
	`access-list acl_dmz1 permit tcp any host 192.168.1.1 lt 1025`
	
	Use **gt** and a port to permit or deny access to all ports greater than the port you specify. For example, use **gt 42** to permit or deny ports 43 to 65535.
	
	`access-list acl_dmz1 deny udp any host 192.168.1.2 gt 42`
	
	Use **neq** and a port to permit or deny access to every port except the ports that you specify. For example, use **neq 10** to permit or deny ports 1-9 and 11 to 65535.
	
	`access-list acl_dmz1 deny tcp any host 192.168.1.3 neq 10`
	
	Use **range** and a port range to permit or deny access to only those ports named in the range. For example, use **range 10 1024** to permit or deny access only to ports 10 through 1024. All other ports are unaffected. The use of port ranges can dramatically increase the number of IPSec tunnels. For example, if a port range of 5000 to 65535 is specified for a highly dynamic protocol, up to 60,535 tunnels can be created.

permit	When used with the **access-group** command, the **permit** option selects a packet to traverse the PIX Firewall. By default, PIX Firewall denies all inbound or outbound packets unless you specifically permit access. When used with a **crypto map** command statement, **permit** selects a packet for IPSec protection. The **permit** option causes all IP traffic that matches the specified conditions to be protected by IPSec using the policy described by the corresponding **crypto map** command statements.
port	Services you permit or deny access to. Specify services by the port that handles it, such as **smtp for port 25**, **www** for port 80, and so on. You can specify ports by either a literal name or a number in the range of 0 to 65535. You can view valid port numbers online at the following website: http://www.iana.org/assignments/port-numbers See "Ports" in Chapter 2, "Using PIX Firewall Commands" for a list of valid port literal names in port ranges; for example, **ftp h323**. You can also specify numbers.
protocol	Name or number of an IP protocol. It can be one of the keywords **icmp**, **ip**, **tcp**, or **udp**, or an integer in the range 1 to 254 representing an IP protocol number. To match any Internet protocol, including ICMP, TCP, and UDP, use the keyword **ip**.

RQS nº 03/2005 - CN
CPMI CORREIOS
Fls Nº 203
Doc 3702

source_addr	Address of the network or host from which the packet is being sent. Use this field when an **access-list** command statement is used in conjunction with an **access-group** command statement, or with the **aaa match access-list** command and the **aaa authorization** command.
source_mask	Netmask bits (mask) to be applied to *source_addr*, if the source address is for a network mask.
remote_addr	IP address of the network or host remote to the PIX Firewall. Specify a *remote_addr* when the **access-list** command statement is used in conjunction with a **crypto access-list** command statement, a **nat 0 access-list** command statement, or a **vpdn group split-tunnel** command statement.
remote_mask	Netmask bits (mask) to be applied to *remote_addr*, if the remote address is a network mask.

Usage Guidelines

The **access-list** command lets you specify if an IP address is permitted or denied access to a port or protocol. In this document, one or more **access-list** command statements with the same access list name are referred to as an "access list." Access lists associated with IPSec are known as "crypto access lists."

By default, all **access-list** commands have an implicit **deny** unless you explicitly specify **permit**. In other words, by default, all access in an access list is denied unless you explicitly grant access using a **permit** statement.

Note Do not use the string "multicastACL" following the name of a PIX Firewall interface in an access-list name because this is a reserved keyword used by PIX Device Manager (PDM).

Additionally, you can use the **object-group** command to group access lists like any other network object.

Use the following guidelines for specifying a source, local, or destination address:

- Use a 32-bit quantity in four-part, dotted-decimal format.
- Use the keyword **any** as an abbreviation for an address and mask of 0.0.0.0 0.0.0.0. This keyword is normally not recommended for use with IPSec.
- Use **host** *address* as an abbreviation for a mask of 255.255.255.255.

Use the following guidelines for specifying a network mask:

- Do not specify a mask if the address is for a host; if the destination address is for a host, use the **host** parameter before the address.

  For example:

  ```
  access-list acl_grp permit tcp any host 192.168.1.1
  ```

- If the address is a network address, specify the mask as a 32-bit quantity in four-part, dotted-decimal format. Place zeros in the bit positions you want to ignore.
- Remember that you specify a network mask differently than with the Cisco IOS software **access-list** command. With PIX Firewall, use 255.0.0.0 for a Class A address, 255.255.0.0 for a Class B address, and 255.255.255.0 for a Class C address. If you are using a subnetted network address, use the appropriate network mask.

  For example:

  ```
  access-list acl_grp permit tcp any 209.165.201.0 255.255.255.224
  ```

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 204
Doc. 3702

If appropriate, after you have defined an access list, bind it to an interface using the **access-group** command. For IPSec use, bind it with a **crypto ipsec** command statement. In addition, you can bind an access list with the RADIUS authorization feature (described in the next section).

The **access-list** command supports the **sunrpc** service.

The **show access-list** command lists the **access-list** command statements in the configuration and the hit count of the number of times each element has been matched during an **access-list** command search. Additionally, it displays the number of access list statements in the access list and indicates whether or not the list is configured for TurboACL. (If the list has less than eighteeen access control entries then it is marked to be turbo-configured but is not actually configured for TurboACL until there are 19 or more entries.)

The **clear access-list** command removes all **access-list** command statements from the configuration or, if specified, access lists by their *acl_ID*. The **clear access-list** *acl_ID* **counters** command clears the hit count for the specified access list.

The **no access-list** command removes an **access-list** command from the configuration. If you remove all the **access-list** command statements in an access list, the **no access-list** command also removes the corresponding **access-group** command from the configuration.

Note The **aaa**, **crypto map**, and **icmp** commands make use of the **access-list** command statements.

RADIUS Authorization

PIX Firewall allows a RADIUS server to send user group attributes to the PIX Firewall in the RADIUS authentication response message. Additionally, the PIX Firewall allows downloadable access lists from the RADIUS server. For example, you can configure an access list on a Cisco Secure ACS server and download it to the PIX Firewall during RADIUS authorization.

After the PIX Firewall authenticates a user, it can then use the CiscoSecure **acl** attribute returned by the authentication server to identify an access list for a given user group. To maintain consistency, PIX Firewall also provides the same functionality for TACACS+.

To restrict users in a department to three servers and deny everything else, the **access-list** command statements are as follows:

```
access-list eng permit ip any server1 255.255.255.255
access-list eng permit ip any server2 255.255.255.255
access-list eng permit ip any server3 255.255.255.255
access-list eng deny ip any any
```

In this example, the vendor specific attribute string in the CiscoSecure configuration has been set to **acl=eng**. Use this field in the CiscoSecure configuration to identify the **access-list** identification name. The PIX Firewall gets the **acl=***acl_ID* from CiscoSecure and extracts the ACL number from the attribute string, which it places in a user's uauth entry. When a user tries to open a connection, PIX Firewall checks the access list in the user's uauth entry, and depending on the permit or deny status of the access list match, permits or denies the connection. When a connection is denied, PIX Firewall generates a corresponding syslog message. If there is no match, then the implicit rule is to deny.

Because the source IP of a given user can vary depending on where they are logging in from, set the source address in the **access-list** command statement to **any**, and the destination address to identify which network services the user is permitted or denied access to. If you want to specify that only users logging in from a given subnet may use the specified services, specify the subnet instead of using **any**.

ECS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 205
Doc. 3702

Note An access list used for RADIUS authorization does not require an **access-group** command to bind the statements to an interface.

There is *not* a **radius** option to the **aaa authorization** command.

Configure the access list specified in Attribute 11 to specify a per-user access list name. Otherwise, remove Attribute 11 from the aaa RADIUS server configuration if no access list is intended for user authentication. If the access list is not configured on the PIX Firewall when the user attempts to login, the login will fail.

For more information on how to use RADIUS server authorization, refer to the *Cisco PIX Firewall and VPN Configuration Guide*, version 6.2 or higher.

TurboACL

On the PIX Firewall, TurboACL is turned on globally with the command **access-list compiled** (and turned off globally by the command **no access-list compiled**).

The PIX Firewall default mode is TurboACL off (**no access-list compiled**), and TurboACL is active only on access lists with 19 or more entries.

The minimum amount of Flash memory required to run TurboACL is 2.1 MB. If memory allocation fails, the TurboACL lookup tables will not be generated.

Note Use TurboACL only on PIX Firewall platforms that have 16MB or more of Flash memory. Consequently, TurboACL is not supported on PIX 501 because it has 8MB of Flash memory.

If TurboACL is configured, some access control list or access control list group modifications can trigger regeneration of the TurboACL internal configuration. Depending on the extent of TurboACL configuration(s), this could noticeably consume CPU resources. Consequently, we recommend modifying turbo-complied access lists during non-peak system usage hours.

For more information on how to use TurboACL, refer to the *Cisco PIX Firewall and VPN Configuration Guide*, version 6.2 or higher.

Usage Notes

1. The **clear access-list** command automatically unbinds an access list from a **crypto map** command or interface. The unbinding of an access list from a **crypto map** command can lead to a condition that discards all packets because the **crypto map** command statements referencing the access list are incomplete. To correct the condition, either define other **access-list** command statements to complete the **crypto map** command statements or remove the **crypto map** command statements that pertain to the **access-list** command statement. Refer to the **crypto map** command for more information.
2. Access control lists that are dynamically updated on the PIX Firewall by an AAA server can only be shown using the **show access-list** command. The **write** command does not save or display these updated lists.
3. The **access-list** command operates on a first match basis.
4. If you specify an **access-list** command statement and bind it to an interface with the **access-group** command statement, by default, all traffic inbound to that interface is denied. You must explicitly permit traffic. Note that "inbound" in this context means traffic passing through the interface, rather than the more typical PIX Firewall usage of inbound meaning traffic passing from a lower security level interface to a higher security level interface.

ECT nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 206
Nº Doc 3702

16 485

5. Always permit access first and then deny access afterward. If the host entries match, then use a **permit** statement, otherwise use the default **deny** statement. You only need to specify additional **deny** statements if you need to deny specific hosts and permit everyone else.
6. You can view security levels for interfaces with the **show nameif** command.
7. The ICMP message type (*icmp_type*) option is ignored in IPSec applications because the message type cannot be negotiated with ISAKMP.
8. Only one access list can be bound to an interface using the **access-group** command.
9. If you specify the **permit** option in the access list, the PIX Firewall continues to process the packet. If you specify the **deny** option in the access list, PIX Firewall discards the packet and generates the following syslog message.

   ```
   %PIX-4-106019: IP packet from source_addr to destination_addr, protocol protocol
   received from interface interface_name deny by access-group acl_ID
   ```

   The **access-list** command uses the same syntax as the Cisco IOS software **access-list** command *except* that PIX Firewall uses a subnet mask, whereas Cisco IOS software uses a wildcard mask. (In Cisco IOS software, the mask in this example would be specified with the 0.0.0.255 value.) For example, in the Cisco IOS software **access-list** command, a subnet mask of 0.0.0.255 would be specified as 255.255.255.0 in the PIX Firewall **access-list** command.
10. We recommend that you do not use the **access-list** command with the **conduit** and **outbound** commands. While using these commands together will work, the way in which these commands operate may cause debugging issues because the **conduit** and **outbound** commands operate from one interface to another whereas the **access-list** command used with the **access-group** command applies only to a single interface. If these commands must be used together, PIX Firewall evaluates the **access-list** command before checking the **conduit** and **outbound** commands.
11. Refer to the Chapter 3, "Managing Network Access and Use" in the *Cisco PIX Firewall and VPN Configuration Guide* for a detailed description about using the **access-list** command to provide server access and to restrict outbound user access.
12. Refer to the **aaa-server radius-acctport** and **aaa-server radius-authport** commands to verify or change port settings.

ICMP Message Types

For non-IPSec use only, if you prefer more selective ICMP access, you can specify a single ICMP message type as the last option in this command. Table 3-1 lists possible ICMP types values.

Table 3-1 ICMP Type Literals

ICMP Type	Literal
0	echo-reply
3	unreachable
4	source-quench
5	redirect
6	alternate-address
8	echo
9	router-advertisement
10	router-solicitation
11	time-exceeded

RQS nº 03/2005 CN
CPMI - CORREIOS
207
Fls Nº
Doc 3702

16484

Table 3-1 ICMP Type Literals (continued)

ICMP Type	Literal
12	parameter-problem
13	timestamp-reply
14	timestamp-request
15	information-request
16	information-reply
17	mask-request
18	mask-reply
31	conversion-error
32	mobile-redirect

If you specify an ICMP message type for use with IPSec, PIX Firewall ignores it.

For example:

```
access-list 10 permit icmp any any echo-reply
```

IPSec is enabled such that a **crypto map** command references the *acl_ID* for this **access-list** command, then the **echo-repy** ICMP message type is ignored.

Using the access-list Command with IPSec

If an access list is bound to an interface with the **access-group** command, the access list selects which traffic can traverse the PIX Firewall. When bound to a **crypto map** command statement, the access list selects which IP traffic IPSec protects and which traffic IPSec does not protect. For example, access lists can be created to protect all IP traffic between Subnet X and Subnet Y or traffic between Host A and Host B. More information is available in the **crypto map** command section of this guide.

The access lists themselves are not specific to IPSec. It is the **crypto map** command statement referring to the specific access list that defines whether IPSec processing is applied to the traffic matching a permit in the access list.

Crypto access lists associated with the IPSec **crypto map** command statement have these primary functions:

- Select outbound traffic to be protected by IPSec (permit = protect).
- Indicate the data flow to be protected by the new security associations (specified by a single permit entry) when initiating negotiations for IPSec security associations.
- Process inbound traffic to filter out and discard traffic that IPSec protects.
- Determine whether or not to accept requests for IPSec security associations on behalf of the requested data flows when processing IKE negotiation from the IPSec peer. (Negotiation is only done for **crypto map** command statements with the **ipsec-isakmp** option.) For a peer's initiated IPSec negotiation to be accepted, it must specify a data flow that is permitted by a crypto access list associated with an **ipsec-isakmp** crypto map entry.

You can associate a crypto access list with an interface by defining the corresponding **crypto map** command statement and applying the crypto map set to an interface. Different access lists must be used in different entries of the same crypto map set. However, both inbound and outbound traffic will be

RQS nº 03/2005 - CN
CPMI CORREIOS
Fls Nº 208
Nº Doc 3702

evaluated against the same "outbound" IPSec access list. Therefore, the access list's criteria are applied in the forward direction to traffic exiting your PIX Firewall and the reverse direction to traffic entering your PIX Firewall.

If you want certain traffic to receive one combination of IPSec protection (for example, authentication only) and other traffic to receive a different combination of IPSec protection (for example, both authentication and encryption), you need to create two different crypto access lists to define the two different types of traffic. These different access lists are then used in different crypto map entries that specify different IPSec policies.

We recommend that you configure "mirror image" crypto access lists for use by IPSec and that you avoid using the **any** keyword. See the *Cisco PIX Firewall and VPN Configuration Guide* for more information.

If you configure multiple statements for a given crypto access list, in general, the first **permit** statement matched, will be the statement used to determine the scope of the IPSec security association. That is, the IPSec security association will be set up to protect traffic that meets the criteria of the matched statement only. Later, if traffic matches a different **permit** statement of the crypto access list, a new, separate IPSec security association will be negotiated to protect traffic matching the newly matched **access list** command statement.

Some services such as FTP require two **access-list** command statements, one for port 10 and another for port 21, to properly encrypt FTP traffic.

Examples

The following example creates a numbered access list that specifies a Class C subnet for the source and a Class C subnet for the destination of IP packets. Because the **access-list** command is referenced in the **crypto map** command statement, PIX Firewall encrypts all IP traffic that is exchanged between the source and destination subnets.

```
access-list 101 permit ip 172.21.3.0 255.255.0.0 172.22.2.0 255.255.0.0
access-group 101 in interface outside
crypto map mymap 10 match address 101
```

The next example only lets an ICMP message type of echo-reply be permitted into the outside interface:

```
access-list acl_out permit icmp any any echo-reply
access-group acl_out interface outside
```

activation-key

Updates the activation key on your PIX Firewall and checks the activation key running on your PIX Firewall against the activation key stored in the Flash memory of the PIX Firewall. (Configuration mode.)

Configure with the command...	Remove with the command...
activation-key *activation-key-four-tuple*	N/A

Show command options	Show command output
show activation-key	Displays the results of checking the activation key running on the PIX Firewall against the activation key stored in the Flash memory of the PIX Firewall.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 209
Doc 3702

Syntax Description

activation-key	Updates the PIX Firewall activation key unless there is a mismatch between the Flash memory and running PIX Firewall software versions.
activation-key-four-tuple	A four-element hexidecimal string with one space between each element. For example: `0xe02888da 0x4ba7bed6 0xf1c123ae 0xffd8624e` (The leading 0x specfier is optional; all values are assumed to be hexadecimal.)

Usage Guidelines

Use the **activation-key** *activation-key-four-tuple* command to change the activation key on your PIX Firewall.

Caution Use only an activation key valid for your PIX Firewall software version and platform or your system may not reload after rebooting.

The **activation-key** *activation-key-four-tuple* command output indicates the status of the activation key as follows:

- If the PIX Firewall Flash memory software image version is the same as the running PIX Firewall software version, and the PIX Firewall Flash memory activation key is the same as the running PIX Firewall software activation key, then the **activation-key** command output reads as follows:

```
The flash activation key has been modified.
The flash activation key is now the SAME as the running key.
```

- If the PIX Firewall Flash memory image version is the same as the running PIX Firewall software, and the PIX Firewall Flash memory activation key is different from the running PIX Firewall activation key, then the **activation-key** command output reads as follows:

```
The flash activation key has been modified.
The flash activation key is now DIFFERENT from the running key.
The flash activation key will be used when the unit is reloaded.
```

- If the PIX Firewall Flash memory image version is not the same as the running PIX Firewall software, then the **activation-key** command output reads as follows:

```
The flash image is DIFFERENT from the running image.
The two images must be the same in order to modify the flash activation key.
```

- If the PIX Firewall Flash memory image version is the same as the running PIX Firewall software, and the entered activation key is not valid, then the **activation-key** command output reads as follows:

```
ERROR: The requested key was not saved because it is not valid for this system.
```

- If the PIX Firewall Flash memory activation key is the same as the entered activation key, then the **activation-key** command output reads as follows:

```
The flash activation key has not been modified.
The requested key is the SAME as the flash activation key.
```

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 210
Doc 3702

The **show activation-key** command output indicates the status of the activation key as follows:

- If the activation key in the PIX Firewall Flash memory is the same as the activation key running o the PIX Firewall, then the **show activation-key** output reads as follows:

```
The flash activation key is the SAME as the running key.
```

- If the activation key in the PIX Firewall Flash memory is the different from the activation key running on the PIX Firewall, then the **show activation-key** output reads as follows:

```
The flash activation key is DIFFERENT from the running key.
The flash activation key takes effect after the next reload.
```

- If the PIX Firewall Flash memory software image version is not the same as the running PIX Firewall software image, then the **show activation-key** output reads as follows:

```
The flash image is DIFFERENT from the running image.
The two images must be the same in order to examine the flash activation key.
```

Usage Notes

1. The PIX Firewall must be rebooted for a new activation key to be enabled.
2. If the PIX Firewall software image is being upgraded to a higher version and the activation key is being updated at the same time, we recommend that you first install the software image upgrade an reboot the PIX Firewall unit, and then update the activation key in the new image and reboot the uni again.
3. If you are downgrading to a lower PIX Firewall software version, we recommend that you ensure that the activation key running on your system is not intended for a higher version before installin the lower version software image. If this is the case, you must first change the activation key to on that is compatible with the the lower version before installing and rebooting. Otherwise, your system may refuse to reload after installation of the new software image.

Examples

The following example shows sample out from the **show activation-key** command:

```
pixfirewalll(config)# show activation-key
Serial Number: 480221353 (0x1c9f98a9)

Running Activation Key: 0x36df4255 0x246dc5fc 0x39d2ec4d 0x09f6288f
Licensed Features:
Failover:           Enabled
VPN-DES:            Enabled
VPN-3DES:           Enabled
Maximum Interfaces: 6
Cut-through Proxy:  Enabled
Guards:             Enabled
URL-filtering:      Enabled
Inside Hosts:       Unlimited
Throughput:         Unlimited
IKE peers:          Unlimited

The flash activation key is the SAME as the running key.
pixfirewall(config)#
```

RQS nº 03/2005 - CN
CPMI - CORREIOS
211
Doc 3702

alias

Administer overlapping addresses with dual NAT. (Configuration mode.)

Configure with the command...	Remove with the command...
alias [(*if_name*)] *dnat_ip foreign_ip* [*netmask*]	**no alias** [[(*if_name*)] *dnat_ip foreign_ip* [*netmask*]] **clear alias**

Show command options	Show command output
show alias	Displays the **alias** command statements in the configuration.

Syntax Description

dnat_ip	An IP address on the internal network that provides an alternate IP address for the external address that is the same as an address on the internal network.
foreign_ip	IP address on the external network that has the same address as a host on the internal network.
if_name	The internal network interface name in which the *foreign_ip* overlaps.
netmask	Network mask applied to both IP addresses. Use 255.255.255.255 for host masks.

Usage Guidelines

The **alias** command translates one address into another. Use this command to prevent conflicts when you have IP addresses on a network that are the same as those on the Internet or another intranet. You can also use this command to do address translation on a destination address. For example, if a host sends a packet to 209.165.201.1, you can use the **alias** command to redirect traffic to another address, such as, 209.165.201.30.

Note For DNS **fixup** to work properly, **proxy-arp** has to be disabled. If you are using the **alias** command for DNS **fixup**, disable **proxy-arp** with the following command after the **alias** command has been executed:

```
sysopt noproxyarp internal_interface
```

If the **alias** command is used with the **sysopt ipsec pl-compatible** command, a static **route** command statement must be added for each IP address specified in the **alias** command statement. There must be an A (address) record in the DNS zone file for the "dnat" address in the **alias** command.

Use the **no alias** command to disable a previous **set alias** command statement. Use the **show alias** command to display **alias** command statements in the configuration. Use the **clear alias** command to remove all **alias** commands from the configuration. After changing or removing an **alias** command statement, use the **clear xlate** command.

The **alias** command changes the default behavior of the PIX Firewall in three ways:

- When receiving a packet coming in through the interface identified by *if_name*, destined for the address identified by *dnat_ip*, PIX Firewall sends it to the address identified by *foreign_ip*.

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 212
Nº Doc 3702

- When receiving a DNS A response, containing the address identified by *foreign_ip*, coming from lower security interface, and destined for the host behind the inteface identified by *if_name*, PIX Firewall changes *foreign_ip* in the reply to *dnat_ip*. This can be turned off by using the command **sysopt nodnsalias inbound**.
- When receiving a DNS A response, containing the address identified by *dnat_ip*, coming from a DNS server behind the interface, *if_name*, and destined for a host behind the lower security interface, PIX Firewall changes *dnat_ip* address to *foreign_ip*. This can be turned off using the command **sysopt nodnsalias outbound**.

The **alias** command is applied on a per-interface basis, while the **sysopt nodnsalias** changes the behaviour for all interfaces. Also, note that addresses in the zone transfers made across the PIX Firewal are not changed.

You can specify a net alias by using network addresses for the *foreign_ip* and *dnat_ip* IP addresses. Fo example, the **alias 192.168.201.0 209.165.201.0 255.255.255.224** command creates aliases for each I address between 209.165.201.1 and 209.165.201.30.

Note ActiveX blocking does not occur when users access an IP address referenced by the **alias** command. ActiveX blocking is set with the **filter activex** command.

Usage Notes

- To access an **alias** *dnat_ip* address with **static** and **access-list** command statements, specify the *dnat_ip* address in the **access-list** command statement as the address from which traffic is permitte from. The following example illustrates this note.

```
alias (inside) 192.168.201.1 209.165.201.1 255.255.255.255
static (inside,outside) 209.165.201.1 192.168.201.1 netmask 255.255.255.255
access-list acl_out permit tcp host 192.168.201.1 host 209.165.201.1 eq ftp-data
access-group acl_out in interface outside
```

  An alias is specified with the inside address 192.168.201.1 mapping to the foreign address 209.165.201.1.

- You can use the **sysopt nodnsalias** command to disable inbound embedded DNS A record fixups according to aliases that apply to the A record address and outbound replies.

Examples

In the following example, the inside network contains the IP address 209.165.201.29, which on the Internet belongs to example.com. When inside clients try to access example.com, the packets do not g to the PIX Firewall because the client assumes 209.165.201.29 is on the local inside network.

To correct this, use the **alias** command as follows:

```
alias (inside) 192.168.201.0 209.165.201.0 255.255.255.224

show alias
alias 192.168.201.0 209.165.201.0 255.255.255.224
```

When the inside network client 209.165.201.2 connects to example.com, the DNS response from an external DNS server to the internal client's query would be altered by the PIX Firewall to be 192.168.201.29. If the PIX Firewall uses 209.165.200.225 through 209.165.200.254 as the global poo IP addresses, the packet goes to the PIX Firewall with SRC=209.165.201.2 and DST=192.168.201.29. The PIX Firewall translates the address to SRC=209.165.200.254 and DST=209.165.201.29 on the outside.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 213
Nº - Doc 3702

In the next example, a web server is on the inside at 10.1.1.11 and a **static** command statement was created for it at 209.165.201.11. The source host is on the outside with address 209.165.201.7. A DNS server on the outside has a record for www.example.com as follows:

```
www.example.com. IN A 209.165.201.11
```

The period at the end of the www.example.com. domain name must be included.

The **alias** command follows:

```
alias 10.1.1.11 209.165.201.11 255.255.255.255
```

PIX Firewall doctors the nameserver replies to 10.1.1.11 for inside clients to directly connect to the web server.

The **static** command statement is as follows:

```
static (inside,outside) 209.165.201.11 10.1.1.11
```

The **access-list** command statement you would expect to use follows:

```
access-list acl_grp permit tcp host 209.165.201.7 host 209.165.201.11 eq telnet
```

But with the **alias** command, use this command:

```
access-list acl_grp permit tcp host 209.165.201.11 eq telnet host 209.165.201.7
```

You can test the DNS entry for the host with the following UNIX **nslookup** command:

```
nslookup -type=any www.example.com
```

arp

Change or view the ARP cache, and set the timeout value. (Configuration mode.)

Configure with the command...	Remove with the command...
arp *if_name ip_address mac_address* [**alias**]	**no arp** *if_name ip_address* **clear arp**
arp timeout *seconds*	**no arp timeout**

Show command options	Show command output
show arp [*if_name*] [*ip_address mac_address* **alias**]	Displays the entries in the ARP table.
show arp timeout	Displays the current timeout value.

Syntax Description

alias	Make this entry permanent. Alias entries do not time out and are automatically stored in the configuration when you use the **write** command to store the configuration.
if_name	The internal or external interface name specified by the **nameif** command.
ip_address	Host IP address for the ARP table entry.
mac_address	Hardware MAC address for the ARP table entry; for example, 00e0.1e4e.3d8b.
seconds	Duration that an ARP entry can exist in the ARP table before being cleared.

PQS nº 03/2665 CN
CPMI CORREIOS
Fls Nº 214
Doc 3702

Usage Guidelines

The **arp** command adds an entry to the PIX Firewall ARP cache. ARP is a low-level TCP/IP protocol that resolves a node's physical address from its IP address through an ARP request asking the node with a particular IP address to send back its physical address. The presence of entries in the ARP cache indicates that the PIX Firewall has network connectivity. The **clear arp** command clears the ARP table but not the **alias** (permanent) entries. Use the **no arp** command to remove these entries. The **show arp** command lists the entries in the ARP table.

Note You can use the **sysopt noproxyarp** command to disable proxy-arps on an interface.

Use the **arp** command to add an entry for new hosts you add on your network or when you swap an existing host for another. Alternatively, you can wait for the duration specified with the **arp timeout** command to expire and the ARP table rebuilds itself automatically with the new host information.

The **no arp timeout** command sets the timer to its default value. The **show arp timeout** command displays the current timeout value.

Defaults

The **arp timeout** command sets the duration that an ARP entry can stay in the PIX Firewall ARP table before expiring. The timer is known as the ARP persistence timer. The default value is 14,400 seconds (4 hours).

Examples

The following examples illustrate use of the **arp** and **arp timeout** commands:

```
arp inside 192.168.0.42 00e0.1e4e.2a7c
arp outside 192.168.0.43 00e0.1e4e.3d8b alias
show arp
    outside 192.168.0.43 00e0.1e4e.3d8b alias
    inside 192.168.0.42 00e0.1e4e.2a7c

clear arp inside 192.168.0.42

arp timeout 42
show arp timeout
arp timeout 42 seconds

no arp timeout
show arp timeout
arp timeout 14400 seconds
```

auth-prompt

Change the AAA challenge text for through the firewall user sessions. (Configuration mode.)

Configure with the command...	Remove with the command...
auth-prompt [accept | reject | prompt] *string*	**no auth-prompt [accept | reject | prompt]** *string* **clear auth-prompt**

ROS nº 03/2005 - CN
CPMI - CORREIOS
215
Fls. Nº
Doc: 3702

Show command options	Show command output
show auth-prompt	Displays the AAA challenge text.

Syntax Description

accept	If a user authentication via Telnet is accepted, display the prompt *string*.
prompt	The AAA challenge prompt string follows this keyword. This keyword is optional for backward compatibility.
reject	If a user authentication via Telnet is rejected, display the prompt *string*.
string	A string of up to 235 alphanumeric characters or 31 words, limited by whichever maximum is first reached. Special characters should not be used; however, spaces and punctuation characters are permitted. Entering a question mark or pressing the **Enter** key ends the string. (The question mark appears in the string.)

Usage Guidelines

The **auth-prompt** command lets you change the AAA challenge text for HTTP, FTP, and Telnet access through the firewall requiring user authentication from TACACS or RADIUS servers. This text is primarily for cosmetic purposes and displays above the username and password prompts that users view when logging in. If the user authentication occurs from Telnet, you can use the **accept** and **reject** options to display different status prompts to indicate that the authentication attempt is accepted or rejected by the AAA server.

Following is the authentication sequence showing when each **auth-prompt** string is displayed:

1. A user initiates a telnet session from the **inside** interface through the firewall to the **outside** interface.
2. The user receives the **auth-prompt** challenge text, followed by the **username** prompt.
3. The user enters the AAA username/password username and password, or in the formats **aaa_user@outside_user** and **aaa_pass@outside_pass**.
4. The firewall sends the **aaa_user/aaa_pass** to the TACACS or RADIUS AAA server.
5. If the AAA server authenticates the user, the firewall displays the **auth-prompt accept** text to the user, otherwise the **reject** challenge text is displayed. Authentication of http and ftp sessions displays only the challenge text at the prompt. The **accept** and **reject** text are not displayed.

If you do not use this command, FTP users view `FTP authentication`, HTTP users view `HTTP Authentication`, and challenge text does not appear for Telnet access.

Note Microsoft Internet Explorer only displays up to 37 characters in an authentication prompt. Netscape Navigator displays up to 120 characters, and Telnet and FTP display up to 235 characters in an authentication prompt.

Examples

The following example shows how to set the authentication prompt and how users view the prompt:

```
auth-prompt XYZ Company Firewall Access
```

After this string is added to the configuration, users view the following:

```
Example.com Company Firewall Access
User Name:
Password:
```

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 216
Doc 3702

The **prompt** keyword can be included or omitted.

For example:

```
auth-prompt prompt Hello There!
```

This command statement is the same as the following:

```
auth-prompt Hello There!
```

auto-update

Specifies how often to poll an Auto Update Server. (Configuration mode.)

Configure with the command...	Remove with the command...
auto-update device-id hardware-serial | hostname | ipaddress [*if_name*] **| mac-address** [*if_name*] **| string** *text*	**no auto-update device-id hardware-serial | hostname | ipaddress** [*if_name*] **| mac-address** [*if_name*] **| string** *text*
auto-update poll-period *poll_period* [*retry_count* [*retry_period*]]	**no auto-update** *poll_period* **poll-period** [*retry_count* [*retry_period*]] **clear auto-update**
auto-update server *url* [*verify_certificate*]	**no auto-update server** *url* [*verify_certificate*] **clear auto-update**
auto-update timeout *period*	**no auto-update timeout** *period* **clear auto-update**

Show command options	Show command output
show auto-update	Displays the Auto Update Server, poll time, and timeout period.

Syntax Description

device-id	The device ID of the PIX Firewall.
hardware-serial	Specifies to use the hardware serial number of the PIX Firewall to uniquely identify the firewall.
hostname	Specifies to use the host name of the PIX Firewall to uniquely identify the firewall.
if_name	Specifies the interface to use (with its corresponding IP or MAC address) to uniquely identify the PIX Firewall.
ipaddress	Specifies to use the IP address of the specified PIX Firewall interface to uniquely identify the firewall.
mac-address	Specifies to use the MAC address of the specified PIX Firewall interface to uniquely identify the firewall.
period	Specifies how long to attempt to contact the Auto Update Server, after the last successful contact, before stopping all traffic passing through the PIX Firewall.

RQS nº 03/2005 - CN
CPMI - CORREIOS
217
Doc 3702

poll_period	Specifies how often, in minutes, to poll an Auto Update Server. The default is 720 minutes (12 hours).
retry_count	Specifies how many times to try reconnecting to the Auto Update Server if the first attempt fails. The default is 0.
retry_period	Specifies how long to wait, in minutes, between connection attempts. The default is 5 minutes and the valid range of values is from 1 to 35791.
text	Specifies the text string to uniquely identify the PIX Firewall to the Auto Update Server.
url	Specifies the location of the Auto Update Server using the following syntax: **http**[**s**]:[[*user:password@*] *location* [*:port*]] */ pathname* See the **copy** command for variable descriptions.
verify_certificate	Specifies to verify the certificate returned by the Auto Update Server.

Usage Guidelines

The **clear auto-update** command removes the entire auto-update configuration.

The **auto-update poll-period** command specifies how often to poll the Auto Update Server for configuration or software image updates. The **no auto-update poll-period** command resets the poll period to the default.

The **auto-update server** command specifies the URL of the Auto Update Server. Only one server can be configured. The **no auto-update server** command disables polling for auto-update updates (by terminating the auto-update daemon).

The **auto-update timeout** command is used to stop all new connections to the PIX Firewall if the Auto Update Server has not been contacted for *period* minutes. This can be used to ensure that the PIX Firewall has the most recent image and configuration.

Examples

The **show auto-update** command displays the Auto Update Server, poll time, and timeout period. The following is sample output from the command:

```
Server: https:pix:********@172.23.58.115:1742/management.cgi?1276 (verify)
Poll period: 720, retry count: 2, retry period: 5
Timeout: none
```

Commands

There are no commands that start with the letter B in PIX Firewall software version 6.2.

ROS nº 03/2005 CN
CPMI CORREIOS
218
Fls Nº
Doc 3702

1647

Segurança Tipo 1 doc 8

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 219
Doc. 3702

1647

Cisco – Using and Configuring PIX Object Groups

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 220
Doc 3702

Table of Contents

Using and Configuring PIX Object Groups **1**
- Introduction 1
- Before You Begin 1
  - Conventions 1
  - Prerequisites 1
  - Components Used 1
  - Network Diagram 2
- Using Object Groups 2
- Configuring Object Groups 2
  - ICMP-Type Configuration 2
  - Network Configuration 3
  - Protocol Configuration 3
  - Service Configuration 4
  - Object-Group Nesting Configuration 4
- Verify 4
- Related Information 5

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 221
Doc 3702

Using and Configuring PIX Object Groups

Introduction
Before You Begin
Conventions
Prerequisites
Components Used
Network Diagram
Using Object Groups
Configuring Object Groups
ICMP–Type Configuration
Network Configuration
Protocol Configuration
Service Configuration
Object–Group Nesting Configuration
Verify
Related Information

Introduction

This document discusses object groups, a feature introduced in PIX code version 6.2. Object grouping allows objects such as IP hosts or networks, protocols, ports, and Internet Control Message Protocol (ICMP) types to be collected into object groups. Once configured, an object group can then be used with the standard **conduit** or **access–list** PIX commands to reference all objects within that group. This will reduce the configuration size.

Before You Begin

Conventions

For more information on document conventions, see the Cisco Technical Tips Conventions.

Prerequisites

There are no specific prerequisites for this document.

Components Used

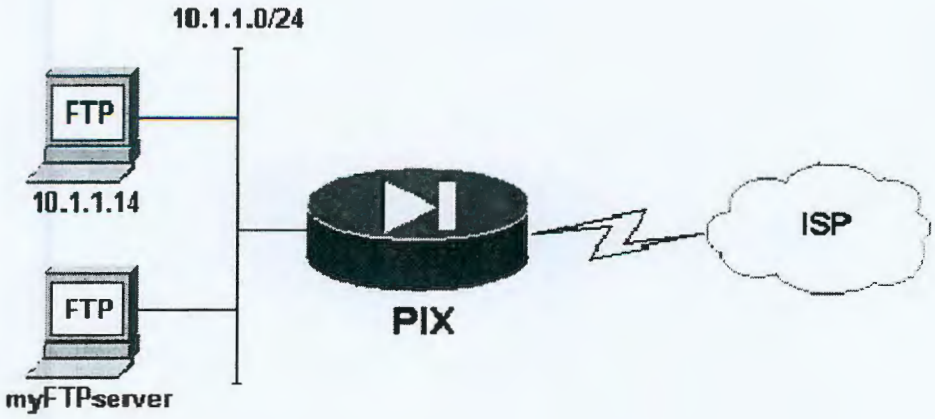
The information in this document is based on the software and hardware versions below.

- Cisco PIX Software Release 6.2(2)
- Cisco 515 PIX Firewall (any PIX model will work with these configurations)

The information presented in this document was created from devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If you are working in a live network, ensure that you understand the potential impact of any command before using it.

RQS nº 03/2005 - CN
CPMI CORREIOS
Fls Nº 222
Doc 3702

Network Diagram



Using Object Groups

When using an object group within a command, the keyword **object-group** must be used before the group name, as shown in the following example.

```
access-list 100 permit object-group protocols object-group
   remotes object-group locals object-group services
```

In this example, protocols, remotes, locals, and services are previously defined object group names. Object groups can also be nested, where one object group can be included as a subset of another object group.

The command set is shown below.

```
object-group grp_id
object-group description description_text
group-object object_grp_name

object-group icmp-type grp_id
icmp-object icmp_type

object-group network grp_id
network-object host host_addr
network-object net_addr netmask

object-group protocol grp_id
protocol-object protocol

object-group service grp_id {tcp|udp|tcp-udp}
port-object eq service
port-object range begin_service end_service
```

Configuring Object Groups

ICMP-Type Configuration

The ICMP-type object group is used to specify specific ICMP types for use only with ICMP access control lists (ACLs) and conduits. A full listing of ICMP types can be found in the PIX command reference for the

Fls. Nº 223
Doc 3702

object–group command.

```
(config)# object-group icmp-type icmp-allowed
(config-icmp-type)# icmp-object echo
(config-icmp-type)# icmp-object time-exceeded
(config-icmp-type)# exit

(config)# access-list 100 permit icmp any any object-group icmp-allowed
```

Network Configuration

The network object group is used to specify host IP addresses or subnet ranges to be defined in an ACL or conduit. Host IP addresses are prefixed with the keyword **host**, and can be either an IP address or a hostname already defined with the **name** command. This object group can be used as either the source or destination in the associated ACL/conduit.

```
(config)# names
(config)# name 10.1.1.10 myFTPserver

(config)# object-group network ftp_servers

(config-network)# network-object host 10.1.1.14
(config-network)# network-object host myFTPserver

(config-network)# network-object 10.1.1.32 255.255.255.224
(config-network)# exit

(config)# access-list 101 permit ip any object-group ftp_servers
```

If this list consists only of FTP servers, the following specific example applies.

```
(config)# access-list 101 permit tcp any object-group ftp_servers eq ftp
```

Protocol Configuration

The protocol object group is used to specify a protocol(s) to be defined in an ACL or conduit. This object group can be used as the protocol type only in the associated ACL or conduit. Note that the allowed protocols for this object group are only the standard PIX protocol names allowed in an **access–list** or **conduit** command, such as Transmission Control Protocol (TCP), User Datagram Protocol (UDP), Generic Routing Encapsulation (GRE), Enhanced Interior Gateway Routing Protocol (EIGRP), Encapsulating Security Payload (ESP), Authentication Header (AH), and so on. Protocols that sit on top of TCP or UDP cannot be specified with a protocol object group. Instead, these protocols will use an object group, as shown in the following example.

```
(config)# object-group protocol proto_grp_1

(config-protocol)# protocol-object udp
(config-protocol)# protocol-object tcp
(config-protocol)# protocol-object esp
(config-protocol)# exit

(config)# access-list 102 permit object-group proto_grp_1 any any
```


ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 224
Doc 3702

Service Configuration

The service object group is used to specify specific or ranges of TCP and/or UDP ports to be defined in an ACL or conduit. This object group can be used as either the source port(s) or destination port(s) in the associated ACL/conduit, as shown in the following example.

```
(config)# object-group service allowed_prots tcp
(config-service)# port-object eq ftp
(config-service)# port-object range 2020 2021
(config-service)# exit

(config)# object-group service high_ports tcp-udp
(config-service)# port-object range 1024 65535
(config-service)# exit

(config)# access-list 103 permit tcp any object-group
          high_ports any object-group allowed_prots
```

Object–Group Nesting Configuration

Only object groups of the same type can be nested within another. For example, you cannot nest a protocol–type object group within a network–type object–group.

To nest a group within a group, issue the **group–object** subcommand. In the following example, you could use the all_hosts group in an ACL or conduit to specify all four hosts. Or, you could use either host_grp_1 or host_grp_2 to specify only the two hosts within each group.

```
(config)# object-group network host_grp_1

(config-network)# network-object host 10.1.1.10
(config-network)# network-object host 10.1.1.14
(config-network)# exit

(config)# object-group network host_grp_2

(config-network)# network-object host 172.16.10.1
(config-network)# network-object host 172.16.10.2
(config-network)# exit


(config)# object-group network all_hosts

(config-network)# group-object host_grp_1

(config-network)# group-object host_grp_2

(config-network)# exit
```

Verify

This section provides information you can use to confirm your configuration is working properly.

Certain **show** commands are supported by the Output Interpreter Tool (registered customers only) , which allows you to view an analysis of **show** command output.

- **show object–group** – Shows the currently defined ACLs.

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 225
Doc 3702

- **show access-list** *<acl>* – Shows the ACL and the associated hit counter for each line. This command shows the expanded ACL entries for each object group defined.

Related Information

- **Documentation for PIX Firewall**
- **PIX Command Reference**
- **PIX Support Page**
- **Requests for Comments (RFCs)**
- **Technical Support – Cisco Systems**

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 226
Doc 3702

roriz 7NYWD1

16.465

Job Title: doc1.pdf

Time Queued: [illegible] 02:55 [illegible] 2003
Time Printed: [illegible] 03.23.[illegible] 2003

Submitted By: [illegible] 297NYWD11S3

297NYWD11S3

Need help? Call your local NCO HelpDesk.

PIO_DEV: [illegible] brbrap7a#ibmNetPrinter (ibm4320) @ brbraprt01

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 227
Doc 3702

Data Sheet

Cisco Catalyst **6500** Series Switch

The Catalyst 6500 Series sets the new standard for IP communications and application delivery in enterprise campus and service provider networks by maximizing user productivity and enhancing operational control while providing unprecedented investment protection. As Cisco's premier intelligent multilayer modular switch, the Catalyst® 6500 Series delivers secure, converged services, end-to-end, from the wiring closet to the core, to the data center, to the WAN edge.

Ideal for enterprises and service providers seeking to reduce their total cost of ownership, the Cisco Catalyst 6500 Series delivers scalable performance and port density across a range of chassis configurations and LAN/WAN/MAN interfaces. Available in 3-, 6-, 9-, and 13-slot chassis, Cisco Catalyst 6500 Series switches feature an unparalleled range of integrated services modules, including multigigabit network security, content switching, telephony, and network analysis modules.

By taking advantage of a forward-thinking architecture that uses a common set of modules and operating system software across all Cisco Catalyst 6500 Series chassis, the Catalyst 6500 Series delivers a high level of operational consistency that optimizes IT infrastructure usage and enhances return on investment. From 48-port to 576-port 10/100/1000 Ethernet wiring closets to hundreds-of-Mpps network cores supporting up to 192 1-Gbps or 32 10-Gbps trunks, the Cisco Catalyst 6500 Series provides an optimal platform that maximizes network uptime with stateful failover capability between redundant routing and forwarding engines.

With numerous industry-firsts and industry-leading features to its credit, the Catalyst 6500 Series supports three generations of modules that continue to demonstrate the Catalyst 6500 value and Cisco's commitment to innovation. Cisco's new generation of Catalyst 6500 Series modules and Supervisor Engine 720 incorporate 11 new Cisco-developed application specific integrated circuits (ASICs)—extending Cisco's leadership in networking while providing unparalleled investment protection.

Figure 1
Cisco Catalyst 6500 Series Chassis

POS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 228
Nº - 1 Doc 3702

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Cisco Catalyst 6500 Series Benefits

The Cisco Catalyst 6500 Series provides market-leading services, performance, port densities, and availability with investment protection for enterprise and service provider markets. These include:

- *Maximum network uptime*—With platform, power supply, supervisor engine, switch fabric, and integrated network services redundancy provides one- to three-second stateful failover and delivers application and services continuity in a converged network environment, minimizing disruption of mission-critical data and services
- *Comprehensive network security*—Integrates proven, multigigabit Cisco security solutions, including intrusion detection, firewall, VPN, and SSL into existing networks
- *Scalable performance*—Provides up to 400 Mpps performance with distributed forwarding architecture
- *Forward-Thinking architecture with investment protection*—Supports three generations of interchangeable, hot-swappable modules in the same chassis, optimizing IT infrastructure usage, maximizing return on investment, and reducing total cost of ownership
- *Operational consistency*—Features 3-, 6-, 9-, and 13-slot chassis configurations sharing a common set of modules, Cisco IOS Software, Cisco Catalyst Operating System Software, and network management tools that can be deployed anywhere in the network
- *Unparalleled services integration and flexibility*—Integrates advanced services such as security and content with converged networks, provides the widest range of interfaces and densities, from 10/100 and 10/100/1000 Ethernet to 10 Gigabit and from DS0 to OC-48, and performs in any deployment end to end

Operational Consistency in End-to-End Cisco Catalyst 6500 Series Deployments

- Features 3-, 6-, 9-, and 13-slot chassis configurations that share a common set of modules, software, and network management tools
- Deploys anywhere in the network—from the wiring closet to the core, to the data center, to the WAN edge
- Shares WAN port adapters with Cisco 7xxx router Series for reduced sparing and training costs
- Offers choice of Cisco IOS Software and Cisco Catalyst Operating System Software supported on all supervisor engines, providing smooth migration from Cisco Catalyst 5000 Series and Cisco 7500 Series deployments

Maximum Network Uptime and Network Resiliency

- Provides packet-loss protection and the fastest recovery from network disruption
- Features fast, one- to three-second stateful failover between redundant supervisor engines
- Offers optional, redundant high-performance Cisco Catalyst 6500 Series Supervisor Engine 720, passive backplane, multimodule Cisco EtherChannel® technology, IEEE 802.3ad link aggregation, IEEE 802.1s/w, and Hot Standby Router Protocol/Virtual Router Redundancy Protocol (HSRP/VRRP) high-availability features

Integrated High-performance Security and Network Management

Integrated gigabit-per-second services modules, deployed where external devices would not be feasible, simplify network management and reduce total cost of ownership. These include:

- Gigabit firewall—provides access protection
- High-performance intrusion detection system (IDS)—provides intrusion detection protection
- Gigabit Network Analysis Module—provides a more manageable infrastructure and full Remote Monitoring (RMON) support
- High-performance SSL—provides high-performance, secure e-commerce traffic termination
- Gigabit VPN and standards-based IP Security (IPSec)—support lower cost Internet and intracampus connections

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Fls. Nº 229
Doc 3702

16.46.2

Content-and Application-Aware Layers 2 Through 7 Switching Services

- Integrated content switching module (CSM) brings high-performance, feature-rich server and firewall load balancing to the Cisco Catalyst 6500 Series, ensuring a safer and more manageable infrastructure with unprecedented control
- Integrated multigigabit SSL acceleration combined with CSM provides a high-performance e-commerce solution
- Integrated multigigabit firewall and CSM provide a secure, high-performance, data-center solution
- Software features such as Network Based Application Recognition (NBAR) enhance network management and control of bandwidth utilization

Scalable Performance

- Delivers the industry's highest LAN switch performance, 400 Mpps, using the distributed Cisco Express Forwarding dCEF720 platform
- Supports a mix of Cisco Express Forwarding (CEF) implementations and switch fabric speeds for optimal wiring closet, core, data center, and WAN edge deployments, as well as service provider networks

Rich Layer 3 Services

- Multiprotocol Layer 3 routing supports traditional network requirements and provides a smooth transition mechanism in the enterprise
- Provides hardware support for enterprise-class and service-provider-scale routing tables
- Provides IPv6 support in hardware (using Supervisor Engine 720) with an unparalleled high-performance suite of services
- Provides hardware support for large enterprise-class and service-provider-scale routing tables
- Provides MPLS support in hardware to enable VPN services within the enterprise and facilitate smooth integration with new high-speed service provider core infrastructures and Metro Ethernet deployments

Enhanced Data Voice, and Video Services

- Provides integrated IP communications throughout all Cisco Catalyst 6500 Series platforms
- Provides 10/100 and 10/100/1000 line cards, field upgradable with inline power using a daughter card and offering future support for IEEE 802.3af to protect today's investments
- Provides dense T1/E1 and foreign Exchange Station (FXS) voice-over-IP (VoIP) gateway interfaces for public switched telephone network (PSTN) access and traditional phone, fax, and private branch exchange (PBX) connections
- Supports high-performance IP multicast video and audio applications
- Provides integrated management necessary to effectively deploy a scalable enterprise-converged network

Highest Level of Interface Flexibility, Scalability, and Density

- Provides the port densities and interface choices that large mission-critical wiring closets, enterprise core, and distribution networks require
- Supports up to 576 voice 10/100/1000 Gigabit-over-copper ports with inline power per system
- Provides up to 192 Gigabit Ethernet ports

ECT nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 230
Doc 3702

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

16.461

- Features the industry's first 10 Gigabit Ethernet, Channelized OC-48 dense OC-3 Packet over Synchronous Optical Network (SONET) (PoS)
- Provides investment protection by using Cisco 7xxx Series port adapters on the Cisco Catalyst 6500 Series FlexWAN Line Card, supporting T1/E1 through OC-48 WAN interfaces
- Chassis sizes range from 3-slot (Cisco Catalyst 6503 Switch) to 13-slot (Cisco Catalyst 6513 Switch)

High-Speed WAN Interfaces

- Provides high-speed WAN, ATM, and SONET interfaces compatible with other core routers
- Provides single-device management for WAN aggregation and for campus and metro connectivity

Maximum Investment Protection

- Highly flexible modular architecture supports multiple generations of modules that are fully interoperable with each other in the same chassis
- Upgradable supervisor engines can add Layer 3 routing or forwarding capabilities over time
- Cisco IOS Software and Cisco Catalyst Operating System Software are supported across all supervisor engines
- Field-upgradable inline power for 10/100 Mbps and 10/100/1000 Mbps Ethernet modules for "pay as you go" IP telephony and wireless computing
- A steady stream of new services modules adds to the deployment options
- Includes Cisco Catalyst 6500 Series network security, content switching, and voice capabilities
- Future modules will increase performance, port density, and include additional services

Ideal for Metro Ethernet WAN Services

- 802.1Q and 802.1Q tunneling (QinQ) providing point-to-point and multipoint Ethernet services
- EoMPLS in MPLS backbones for superior network scaling providing virtual LAN (VLAN) translation capability
- Layer 2 and Layer 3 QoS enables tiered Ethernet service offerings through rate limiting and traffic shaping
- Superior high-availability features include enhanced Spanning Tree Protocol, IEEE 802.1s, IEEE 802.1w, and Cisco EtherChannel IEEE 802.3ad link aggregation

Table 1 Catalyst 6500 Series at a Glance

Feature	Catalyst 6500 Series
System Feature	
Chassis Configurations	3-slot 6-slot 9-slot 9 vertical slots 13-slot
Backplane Bandwidth	32Gbps shared bus 256Gbps switch fabric 720Gbps switch fabric
L3 Forwarding Performance	Supervisor 1 MSFC: 15 Mpps Supervisor 2 MSFC: up to 210 Mpps Supervisor 720: up to 400 Mpps

Cisco Systems, Inc.
All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

ANATEL nº 03/2005 - CN
CPMI - CORREIOS
231
Fls. Nº
Nº Doc 3702

Table 1 Catalyst 6500 Series at a Glance

Feature	Catalyst 6500 Series
Operating System	Catalyst OS (CatOS) Cisco IOS CatOS/IOS Hybrid Configuration
Redundant Supervisors	Yes, with stateful failover
Redundant Components	Power supplies (1+1) Switch fabric (1+1) Replaceable clock Replaceable fan tray
High Availability Features	Gateway Load Balancing Protocol Hot Standby Router Protocol Multimodule EtherChannel Rapid Spanning Tree Multiple Spanning Tree Per VLAN Rapid Spanning Tree Rapid Convergence L3 Protocols
Maximum System Port Densities	
10/100/1000 Ethernet	576 ports, all support Inline Power
10/100 Fast Ethernet	576 ports, all support Inline Power
100-Base-FX	288 ports
Gigabit Ethernet (GBIC)	194 ports (2 ports provided on supervisor engine)
10 Gigabit Ethernet (XENPAK)	32 ports
Integrated WAN Modules	
FlexWAN (DS0 to OC-3)	12 modules with 24 port adapters
OC-3 POS ports	192
OC-12 POS ports	48
OC-12 ATM ports	24
OC-48 POS/DPT ports	24
PSTN Interfaces	
Digital T1/E1 Trunk ports	216
FXS Interfaces	864
Advanced Services Modules	Gigabit Firewall Gigabit VPN High Performance Intrusion Detection Gigabit Content Switching Module High Performance SSL Termination Gigabit Content Services Gateway

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Fls. Nº 232
Nº Doc 3702

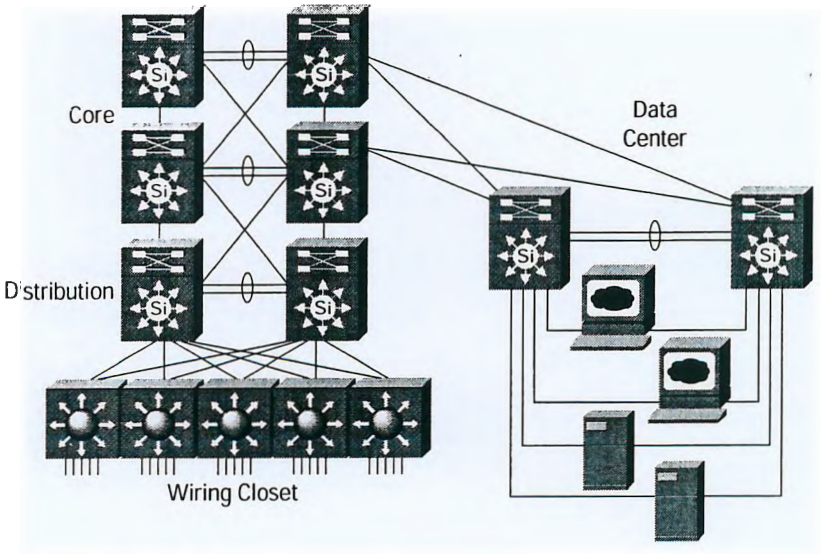
Deployment Scenarios

The Cisco Catalyst 6500 Series delivers secure converged services for campus, Internet service provider (ISP), metro edge, and research and grid computing networks.

- *Campus networks*—Features 10/100 and 10/100/1000 autosensing modules that provide inline power for the wiring closet, along with robust high availability, security, and manageability features; world-class networking software; high-performance Gigabit and 10 Gigabit interface modules; and network management for the distribution and core

Figure 2

Deployment Scenarios for Catalyst 6500 Series Switches in Campus Networks

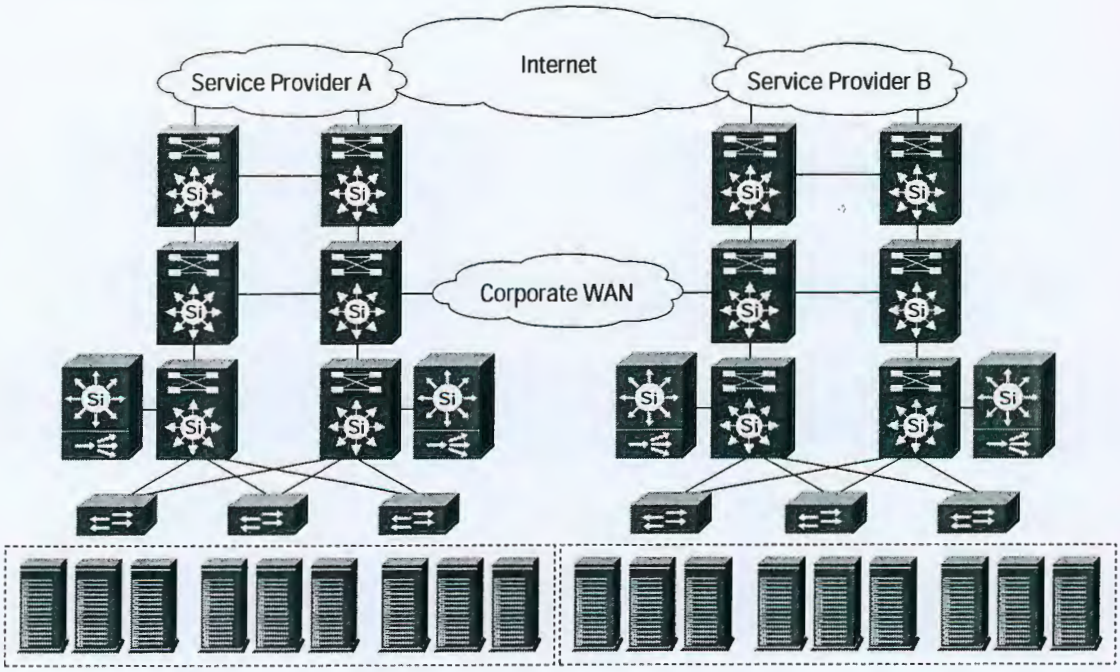


ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 233
Doc 3702

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

- [*ISP network*—Provides robust high-availability, security, and manageability features; world-class networking software; high-performance Gigabit and 10 Gigabit interface modules; and network management for the most demanding service provider networking environments requiring Multiprotocol Label Switching (MPLS), Multicast, IP Version 6 (IPv6), an extensive set of WAN interfaces, and hierarchical traffic shaping.

Figure 3
Deployment Scenarios for Catalyst 6500 Series Switches in ISP Networks

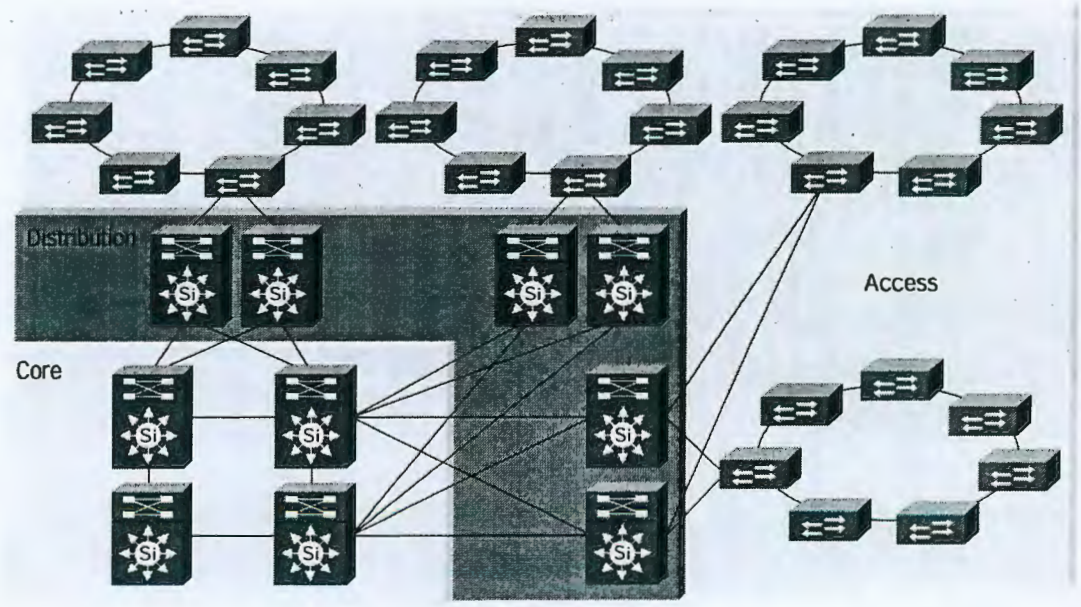


Cisco Systems, Inc.
All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RCS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 234
Doc. 3702

- *Metro edge*—Features edge-, distribution-, and core-layer interfaces for point-to-point and multipoint Ethernet services for metro and inter-metro network deployments with the following features:
  - High-performance 10-Gigabit Ethernet uplinks
  - 802.1Q tunneling
  - Ethernet over MPLS (EoMPLS)
  - Layer 2 and Layer 3 QoS
  - Network Equipment Building Standards (NEBS) compliance
  - Security, high availability, and manageability

Figure 4
Deployment Scenarios for Catalyst 6500 Series Switches in Metro Edge

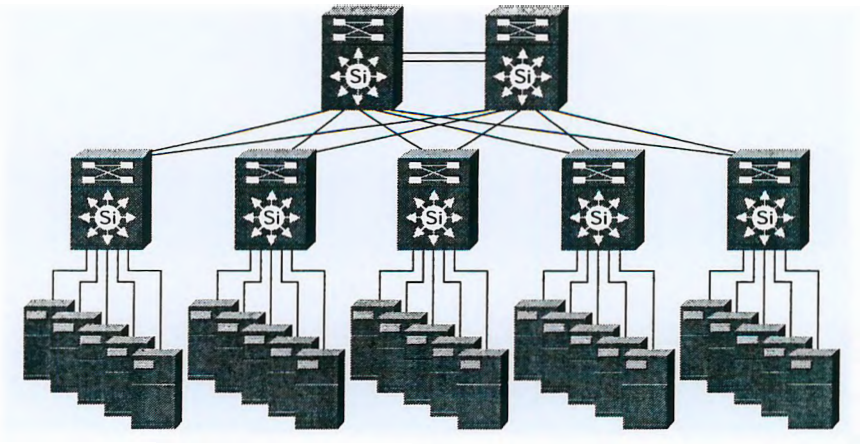


Cisco Systems, Inc.
All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Fls. Nº 235
Doc 3702

- *Grid computing network*—Provides high-speed optical interface modules and world-class software required to handle high-volume traffic and build and manage large-scale networks

Figure 5
Deployment Scenarios for Catalyst 6500 Series Switches in Grid Computing Network



Cisco Systems, Inc.
All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Nº 236
Doc. 3702

1645

System Overview

Modular Architecture

The Cisco Catalyst 6500 Series is a modular system that can grow as customer requirements expand and technology evolves, allowing customers to upgrade and reconfigure systems by adding new modules, replacing existing modules, and adding and redeploying systems. Throughout the Cisco Catalyst 6500 Series, modules are:

- *Configurable*—Separately, simplifying the addition of new services
- *Interoperable*—In the same chassis, providing flexible design options
- *Interchangeable*—Among Cisco Catalyst 6500 Series systems, simplifying sparing and network expansion
- *Hot-swappable*—Without requiring a chassis to be powered off, providing fast upgrade and repair
- *Upgradable*—As newer modules come along, providing investment protection

Cisco Catalyst 6500 Series Hardware-Forwarding Architectures

Cisco Catalyst 6500 Series modules use one of three forwarding technologies, each having a different architecture with different characteristics and capabilities:

- *Cisco Express Forwarding (CEF)*—Scaling to 30 Mpps, this technology uses a central CEF Cisco Express Forwarding engine located on the supervisor engine's policy feature card (PFC) daughter and CEF forwarding tables located on the supervisor engine. The supervisor engine makes all forwarding decisions for all interface modules centrally. For more information see *How Cisco Express Forwarding Works.*
- *Accelerated Cisco Express Forwarding (aCEF)*—Suited for high-performance enterprise environments, this technology uses the aCEF engine and aCEF tables located on the interface module, along with the central CEF engine located on the supervisor engine's PFC daughter card and central CEF forwarding tables located on the supervisor engine. The interface module makes high-volume forwarding decisions locally, and the supervisor engine makes the rest of the forwarding decisions centrally. For more information see *How Accelerated Cisco Express Forwarding (aCEF) Works.*
- *Distributed Cisco Express Forwarding (dCEF)* —Suited for the most demanding environments, this technology uses the dCEF engine located on the interface module's distributed forwarding card (DFC) daughter card and the dCEF table, a local copy of the supervisor engine's central CEF table located on the interface module's DFC. The interface module makes all the forwarding decisions locally, and provides maximum performance and scalability. For more information see *How Distributed Cisco Express Forwarding (dCEF) Works*

Cisco Catalyst 6500 Series Switching Architectures

Cisco developed the following switching architectures for Cisco Catalyst 6500 modules to allow platforms to scale in any deployment:

- 32-Gbps bus—Allowing access to a central shared bus
- 256-Gbps switch fabric—Located on the switch fabric module (SFM)
- 720 Gbps switch fabric—Located on Cisco Catalyst 6500 Series Supervisor Engine 720

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 237
Doc 3702

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Cisco Catalyst 6500 Series Modules

Cisco Catalyst 6500 Series interfacecmodules support the following forwarding technology and switch fabric combinations:

- *Classic Interface Modules*—Use the centralized CEF engine located on the supervisor engine's PFC, connect to the 32-Gbps switching bus only, and forward packets at up to 15 Mpps
- *CEF256 Interface Modules*—Use the centralized CEF engine located on the supervisor engine's PFC, connect to both the 256-Gbps fabric located on the supervisor engine with a single 8-Gbps full-duplex fabric connection and the 32-Gbps switching bus, and forward packets at up to 30 Mpps
- *dCEF256 Interface Modules*—Use the distributed CEF engine on the DFC (located on the interface module), connect to a 256-Gbps fabric located on the supervisor engine or a Switch Fabric Module with 16-Gbps full-duplex fabric connections, and forward packets at up to 210 Mpps
- *aCEF720 Interface Modules*—Use the accelerated CEF engine on the DFC3 (located on the interface module), connect to the 720-Gbps fabric located on the supervisor engine with 40-Gbps full-duplex fabric connections, and forward packets at up to 400 Mpps, peak performance
- *dCEF720 Interface Modules*—Use the distributed CEF engine on the DFC3 (located on the interface module), connect to the 720-Gbps fabric located on the supervisor engine with dual 20-Gbps full-duplex fabric connections, and forward packets at up to 400 Mpps, sustained performance

Note: All Performance numbers refer to IPv4 forwarding.

Cisco Catalyst 6500 Series Module Types

In the Cisco Catalyst 6500 Series architecture, special-purpose modules perform separate tasks—allowing the feature set to evolve quickly and allowing customers to add new features and enhanced performance by adding new modules. The Cisco Catalyst 6500 Series features the following types of special-purpose modules:

- *Supervisor engines*—Perform the control functions and make the forwarding decisions for packets routed to other networks
- *Ethernet interface modules*—Provide IEEE-standard receive and forwarding interfaces and forward packets within the defined network
- *WAN interface modules*—Provide the receive and forwarding interface at the WAN edge
- *Services modules*—Support multigigabit security, application-aware Layer 4 through 7 content switching, network management, and voice gateway services to traditional phones, fax machines, PBXs, and the PSTN
- *Switch Fabric Modules (SFMs)*—Pass network traffic from interface module to the supervisor engine or to another interface

Cisco Catalyst 6500 Series Supervisor Engines

The supervisor engines for the Cisco Catalyst 6500 Series support different forwarding technologies and achieve different forwarding rates, depending on the configuration of the supervisor engine and the capability of a particular interface module.

Supervisor engines can be configured with optional factory-installed daughter cards—a Policy Feature Card (PFC) providing hardware-based Layer-2 forwarding, and a Multilayer Switch Feature Card (MSFC) providing Layer 3 capabilities.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

CPMI - CORREIOS
Fls. Nº 238
Doc 3702

A supervisor engine performs control operations centrally on processors that run either Cisco IOS Software or Cisco Catalyst Operating System Software while special-purpose application-specific integrated circuits (ASICs) perform bridging and routing (based on Cisco Express Forwarding), QoS marking and policing, and access control. The same ASICs are used on the DFCs, daughter cards that can be installed on certain interface modules to distribute forwarding in a decentralized fashion to achieve system forwarding rates of up to 400 Mpps (Table 2).

For additional information about the following Cisco Catalyst 6500 Series supervisor engines visit: http://www.cisco.com/en/US/products/hw/switches/ps708/products_data_sheets_list.html

- Cisco Catalyst 6500 Series Supervisor Engine 720 Data Sheet
- Cisco Catalyst 6500 Series Supervisor Engine 1A and Supervisor Engine 2 Data Sheet

Table 2 Cisco Catalyst 6500 Supervisor Engines

Feature	Supervisor Engine 1	Supervisor Engine 2	Supervisor Engine 720
Solution and market	Wiring closet	Enterprise distribution, core, and WAN edge; service provider WAN and Internet edge	Enterprise core and data center; service provider metro; wireless; national research networks; grid computing
Fabric architectures supported	Centralized forwarding only—engine located on supervisor engine's PFCx daughter card	Centralized CEF—engine located on supervisor engine's PFCx daughter card; Distributed CEF—engine located on interface module's DFC daughter card	Centralized CEF—engine located on Supervisor Engine 720's PFC3 daughter card; Distributed CEF—engine located on interface module's DFC3 daughter card; Accelerated CEF—engine located on interface module's ASICs
Fabric connections	32-Gbps shared bus connection to modules	16 Gbps per slot; Dual-fabric connection to modules at 8 Gbps full duplex per channel	40 Gbps per slot; Dual-fabric connection to modules at 20 Gbps full duplex per channel
Performance maximum (Mpps)	15 Mpps	210 Mpps	Sustained 400 Mpps—dCEF720 Peak 400 Mpps—aCEF720
DFC modules	Not supported	DFC	DFC3

RQS nº 03/2005 - CN -
CPMI - CORREIOS
239

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Nº Doc 3702

Table 2 Cisco Catalyst 6500 Supervisor Engines

Feature	Supervisor Engine 1	Supervisor Engine 2	Supervisor Engine 720
Route processor	On MSFC2 daughter card (optional)	On MSFC2 daughter card (optional)	MSFC3 integrated
PFC modules	PFC daughter card (optional)	PFC2 integrated	PFC3 integrated

Ethernet Interface Modules

Cisco Catalyst 6500 Series Ethernet interface modules, designed for wiring closet, distribution and core, and data center applications, as well as service provider and Metro Ethernet environments, use one of the following types o Ethernet interfaces:

- *10/100 Mbps over copper and 10/100/1000 Mbps Ethernet over copper*—For wiring closets providing 10/100- and 10/100/1000-Mbps performance with auto-negotiation and inline power for voice; up to 48 ports/module; includes Classic and CEF256 interface modules.
- *100 Mbps over fiber*—For secure wiring closets and long-haul router and switch interconnects; up to 24 ports pe module; includes Classic and CEF256 interface modules.
- *1 Gbps*—For distribution and core layers and for data centers providing 1-Gbps performance in a 48-port module; includes Classic CEF256, and dCEF256 interface modules.
- 10 Gbps—For distribution and core layers providing 10-Gbps performance in 1-port or 2-port module; includes CEF256, aCEF720, and dCEF720 interface modules.

For more information, visit:
http://www.cisco.com/en/US/products/hw/switches/ps708/products_data_sheets_list.html

WAN Interface Modules

The Cisco Catalyst 6500 Series and Cisco 7600 Series support several WAN interfaces using two technologies:

- *FlexWAN module*—Accepts up to two plug-in port adapters that provide numerous WAN/MAN protocols and features
- *Optical Services Module (OSM)*—A dedicated line card that provides several interfaces, including OC-3/STM-1, OC-12/STM-4, OC-48/STM-16, Channelized T3, Channelized OC-12/STM-4 PoS, Gigabit Ethernet, OC-12/STM-4 ATM, and OC-48/STM-16 Dynamic Packet Transport (DPT)

FlexWAN Module

The FlexWAN module fits inside Cisco Catalyst 6500 Series and Cisco 7600 Series systems and uses Cisco 7200 and 7500 Series port adapters for a wide range of WAN/MAN protocols, including Frame Relay, ATM, PoS, Point-to-Point Protocol (PPP), and High-Level Data Link Control (HDLC). Additionally, the FlexWAN module provides media options such as clear channel and Channelized T1/E1, T3/E3, High-Speed Service Interface (HSSI), OC-3 PoS, and ATM.

- For information about the Cisco Catalyst 6500 Series and Cisco 7600 Series FlexWAN Module, visit: http://www.cisco.com/en/US/products/hw/routers/ps368/products_data_sheet09186a00800923bf.html

RQS nº 03/2005 - CN
CPMI - CORREIOS
240
3702

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Optical Services Modules

OSMs are line cards that provide high-speed WAN connectivity with onboard network processors for distributed-line-rate IP service applications. For more information about OSMs, see the following data sheets:

- Cisco 7600 Series 4-, 8-, and 16-Port OC-3c/STM-1 PoS/SDH OSM: http://www.cisco.com/en/US/products/hw/routers/ps368/products_data_sheet09186a0080092249.html
- Cisco 7600 Series 4-Port Gigabit Ethernet OSM: http://www.cisco.com/en/US/products/hw/routers/ps368/products_data_sheet09186a008009223d.html
- Cisco 7600 Series 1-Port Channelized OC-12/STM-4 to DS3/E3 OSM: http://www.cisco.com/en/US/products/hw/routers/ps368/products_data_sheet09186a0080092250.html
- Cisco 7600 Series 1-Port OC-48c/STM-16 PoS/SDH/OSM: http://www.cisco.com/en/US/products/hw/routers/ps368/products_data_sheet09186a0080092241.html
- Cisco 7600 Series 2- and 4-Port OC-12c/STM-4 PoS/SDH OSM: http://www.cisco.com/en/US/products/hw/routers/ps368/products_data_sheet09186a008009223e.html
- Cisco 7600 Series 2-Port ATM OSM: http://www.cisco.com/en/US/products/hw/routers/ps368/products_data_sheet09186a008008876f.html
- Cisco 7600 Series 2-Port OC-48c/1-Port OC-48c DPT OSM: http://www.cisco.com/en/US/products/hw/routers/ps368/products_data_sheet09186a0080088774.html

Layer 4 Through 7 Services Modules

The Cisco Catalyst 6500 Series offers an extensive set of services modules for Layer 4 through 7 applications, including content services, network monitoring, security, and telephony.

Content Services Modules

- *Content Services Gateway (CSG)*—Enables differentiated billing, user balance enforcement, and activity tracking for customer billing systems. For more information, visit: http://mobiletraining.cisco.com/csg/CSGe_ds_0211.pdf
- *Content Switching Module (CSM)*—Integrates advanced content switching into the Cisco Catalyst 6500 Series to provide high-performance, high-availability load balancing of caches, firewalls, Web servers, and other network devices. For more information, visit: http://www.cisco.com/en/US/products/hw/modules/ps2706/products_data_sheet09186a00800887f3.html

Network Monitoring

- *Network Analysis Module (NAM 1 and 2)*—Provides application-level visibility into the network infrastructure for real-time traffic analysis, performance monitoring, and troubleshooting; performs traffic monitoring with embedded Web-based traffic analyzer. For more information, visit: http://www.cisco.com/en/US/products/hw/modules/ps2706/products_data_sheet09186a00800a2c89.html

Security Services Modules

- *Firewall Services Module (FWSM)*—The FWSM allows any port in the chassis to operate as a firewall port and integrates stateful firewall security inside the network infrastructure. For more information, visit: http://www.cisco.com/en/US/products/hw/modules/ps2706/products_data_sheet09 186a00800c4fe7.html

Intrusion Detection System Module (IDSM and IDSM-2)—Takes traffic from the switch backplane at wire speed, integrating IDS functions directly into the switch. For more information, visit: http://www.cisco.com/en/US/products/hw/modules/ps2706/products_data_sheet09186a0080092341.html

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

ECT/TP 241
Nº 3702
Doc

- *IPSec VPN Module (IVSM)*—Provides infrastructure-integrated IPSec VPN services capable of 1.9-Gbps Triple Data Encryption Standard (3DES) performance, 8000 active tunnels, and up to 60 tunnels per second. For more information, visit: http://www.cisco.com/en/US/products/hw/modules/ps2706/products_data_sheet09 186a00800c4fe2.html
- *SSL Services Module (SSM)*—Offloads processor-intensive tasks related to securing traffic with SSL accelerating the performance and increasing the security of Web-enabled applications. For more information, visit: http://www.cisco.com/en/US/products/hw/modules/ps2706/products_data_sheet09186a00800c4fe9.html

Telephony Services Modules

- *Communications Media Module (CMM)*—Provides flexible, high-density T1 and E1 gateways, allowing organizations to connect their existing time-division multiplexing (TDM) networks to their IP communications networks, and providing connectivity to the PSTN. For more information, visit: http://www.cisco.com/en/US/products/hw/modules/ps3115/products_data_sheet09 186a00800e9c1f.html

Switch Fabric Modules

Designed to support distributed forwarding for interface modules that have distributed forwarding capability, the Cisco Catalyst 6500 Series SFM or SFM2, in combination with the Cisco Catalyst 6500 Series Supervisor Engine 2-MSFC2 and DFCs on interface modules, increases available system bandwidth from 32 to 256 Gbps. The SFM/SFM2 supports the Cisco Catalyst 6500 CEF256 and dCEF256 interface modules.

Designed to support new interface modules with 720 Gbps forwarding capabilities, the Supervisor Engine 720's onboard switch fabric increases available bandwidth to 720 Gbps and enables packet forwarding rates up to 400 Mpps. By using auto-sensing and auto-negotiation, the Supervisor 720 switch fabric is fully interoperable with the 8- and 16-Gbps switch fabric interconnections used by the CEF256 and dCEF256 interface modules. When a CEF256 or dCEF256 interface module is detected, the switch fabric will automatically connect those modules by offering 8-16 Gbps of bandwidth to each module, as applicable.

How Cisco Express Forwarding Works

Cisco Express Forwarding (CEF) is a Layer 3 technology that provides increased forwarding scalability and performance to handle many short-duration traffic flows common in today's enterprise and service provider networks. To meet the needs of environments handling large amounts of short-flow, Web-based, or highly interactive types of traffic, CEF forwards all packets in hardware, and maintains its forwarding rate completely independent of the number of flows going though the switch.

On the Cisco Catalyst 6500 Series, the CEF Layer 3 forwarding engine is located centrally on the supervisor engine's PFC2 or PFC3—the same device that performs hardware-based Layer 2 and 3 forwarding, ACL checking, QoS policing and marking, and NetFlow statistics gathering.

Using the routing table that Cisco IOS Software builds to define configured interfaces and routing protocols, the CEF architecture creates CEF tables and downloads them into the hardware-forwarding engine before any user traffic is sent through the switch. The CEF architecture places only the routing prefixes in its CEF tables—the only information it requires to make the Layer 3 forwarding decisions—relying on the routing protocols to do route selection. By performing a simple CEF table lookup, the switch forwards packets at wire-rate, independent of the number of flows transiting the switch.

POS nº 03/2003 - CN
CPMI - CORREIOS
Fls. Nº 242
Nº Doc 3702

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

CEF-based forwarding requirements: Requires a Cisco Catalyst Supervisor Engine 2 or Catalyst Supervisor Engine 720.

How Accelerated Cisco Express Forwarding (aCEF) Works

Accelerated Cisco Express Forwarding (aCEF) technology uses two forwarding engines working together in a master-slave relationship to accelerate high-rate traffic flows through the switch—a central CEF engine located on the Supervisor Engine 720's PFC3 and a scaled-down distributed aCEF engine located on the interface module.

The central PFC3 makes the initial forwarding decision, with the aCEF engine storing the result and making subsequent packet-forwarding decisions locally. aCEF forwarding works like this:

- As in standard CEF forwarding, the central PFC3 is loaded with the necessary CEF information before any user traffic arrives at the switch.
- As traffic arrives on an aCEF720 interface module, the aCEF engine inspects the packet, and finding that no specific packet forwarding information exists, consults the central PFC3.
- The PFC3 makes a hardware-based forwarding decision for this packet (including Layer 2, Layer 3, ACLs, and QoS).
- The aCEF engine stores the forwarding decision results and makes forwarding decisions locally for subsequent packets based on packet-flow history.
- The aCEF engine handles hardware-based Layer 2 and Layer 3 forwarding, ACLs, QoS marking, and NetFlow.
- The central PFC3 processes any forwarding decisions that the interface module's aCEF engine cannot handle.

aCEF-based forwarding requirements: Requires a Cisco Catalyst Supervisor Engine 720 and aCEF720 (WS-X67xx) class modules.

How Distributed Cisco Express Forwarding (dCEF) Works

With Distributed Cisco Express Forwarding (dCEF), forwarding engines located on the interface modules make forwarding decisions locally and in parallel, allowing the Cisco Catalyst 6500 Series to achieve the highest forwarding rates in the industry. With dCEF, forwarding occurs on the interface modules in parallel and system performance scales up to 400 Mpps—the aggregate of all forwarding engines working together.

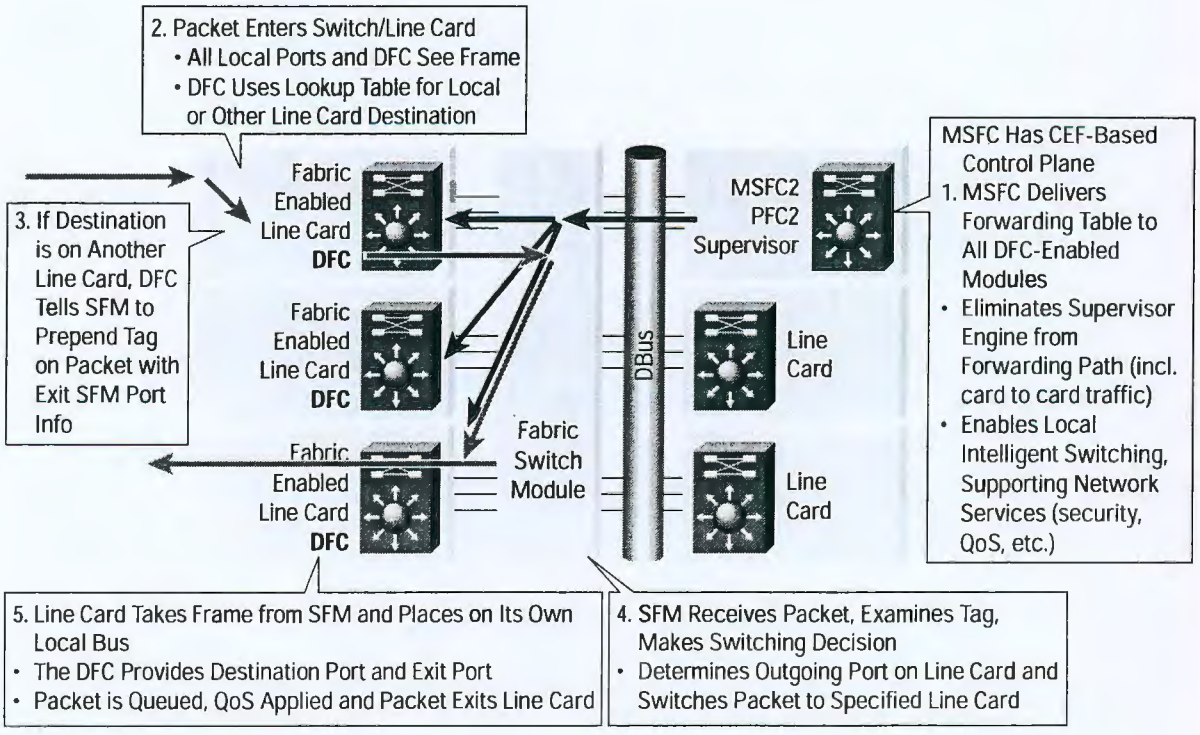
RDS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 243
Nº Doc 3702

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Using the same ASIC engine design as the central PFCx, DFCs located on the interface modules forward packets between two ports, directly or across the switch fabric, without involving the supervisor engine. With the DFC, each interface module has a dedicated forwarding engine complete with the full forwarding tables. dCEF forwarding works like this:

- As in standard CEF forwarding, the central PFC3 located on the supervisor engine and the DFC engines located on the interface modules are loaded with the same CEF information derived from the forwarding table before any user traffic arrives at the switch.
- As a packet arrives at an interface module, its DFC engine inspects the packet and uses the information in the CEF table (including Layer 2, Layer 3, ACLs, and QoS) to make a completely hardware-based forwarding decision for that packet.
- The dCEF engine handles all hardware-based forwarding for traffic on that module, including Layer 2 and Layer 3 forwarding, ACLs, QoS policing and marking, and NetFlow.
- Because the DFCs make all the switching decisions locally, the supervisor engine is freed from all forwarding responsibilities and can perform other software-based functions, including routing, management, and network services.

Figure 6
Distributed Cisco Express Forwarding Packet Flow



dCEF-based forwarding requirements: Requires a Cisco Catalyst Supervisor Engine 720 for the dCEF720 interface module; requires either a Catalyst Supervisor Engine 720 or a Catalyst Supervisor Engine 2-MSFC2 and a SFM for the dCEF256 interface module.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Fls nº 03/2005 CN
CPMI - CORREIOS
0244
3702
Doc

Cisco IOS Software and Catalyst Operating System Software

Cisco Catalyst 6500 Series switches offer two operating modes of software, the Cisco Catalyst Operating System Software with optional Cisco IOS Software on the MSFC, and Cisco IOS Software for the supervisor engines. Eacl operating mode can be deployed at different hierarchies of the network, depending on the network's requirements These software solutions for the Cisco Catalyst 6500 Series switches provide full Layer 2 through 4 switching and routing functions at high performances.

Today, either of these operating modes can be deployed in an entire network environment, or the operating modes can vary within an environment to meet different requirements. One operating mode is not a replacement for anothei but is recommended for varying feature requirements.

- Cisco IOS Software for the Cisco Catalyst 6500 Series
- Cisco Catalyst Operating System Software with optional Cisco IOS Software on the MSFC

Cisco IOS Software for the Cisco Catalyst 6500 Series

Cisco IOS Software for the Cisco Catalyst 6500 Series supervisor engines requires the MSFC on the supervisor engine. It provides integrated multilayer functions in a single image and is optimized for core, distribution, Interne access, and data center deployments. Cisco IOS Software combined with the performance of the Cisco Catalyst 650(Series offers the necessary features for a high-performance Layer 3-enabled deployment, including support for a distributed architecture with the ability to scale the switch to 400 Mpps throughput. Additionally, Cisco IOS Software provides operational ease of use by offering a single image and configuration file to be deployed across the Cisco Catalyst 6500 Series switches.

Cisco Catalyst Operating System Software with Optional Cisco IOS Software on the MSFC

Cisco Catalyst Operating System Software is the premier software for the wiring closet on Cisco Catalyst 6500 Series switches offering high-performance Layer 2 forwarding. It is optimized to deliver the high availability, enhanced security, and integrated inline power support necessary for mission-critical wiring closet deployments. Cisco Catalyst Operating System Software can also be extended to the distribution and core layers of the network when coupled with Cisco IOS Software on the MSFC, providing robust and advanced Layer 3 and Layer 4 functions. This operating mode is often referred to as "hybrid mode." See Table 3 for software and hardware deployment options.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 245
Doc. 3702

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Table 3 Software and Hardware Deployment Options

Network Performance	Wiring Closet	Distribution/ Data Center	Core	WAN Edge
Highest-performance Cisco IOS Software end-to-end	Cisco IOS Software; Supervisor Engine 2-MSFC2; CEF256 interface modules	Cisco IOS Software; Supervisor Engine 720; dCEF720 and aCEF720 interface modules	Cisco IOS Software; Supervisor Engine 720; dCEF720 interface modules	Cisco IOS Software; Supervisor Engine 2-MSFC2; dCEF720 and aCEF720 interface modules
Higher-performance mixed operating system	Cisco Catalyst Operating System Software; Supervisor Engine 2-PFC2; CEF256 and Classic interface modules	Cisco IOS Software; Supervisor Engine 2-MSFC2; dCEF256 and CEF256 interface modules	Cisco IOS Software; Supervisor Engine 720; dCEF720 and aCEF720 interface modules	Cisco IOS Software; Supervisor Engine 2-MSFC2; dCEF256 and, CEF256 interface modules
High-performance Cisco Catalyst Operating System Software end-to-end	Cisco Catalyst Operating System Software; Supervisor Engine 1-2GE; CEF256 and Classic interface modules	Hybrid mode; Supervisor Engine 2-MSFC2; CEF256 and Classic interface modules	Hybrid mode; Supervisor Engine 2-MSFC2; dCEF720 Series and aCEF720 interface modules	Hybrid mode; Supervisor Engine 2-MSFC2; CEF256 and Classic interface modules

Cisco IOS Software and Cisco Catalyst Operating System Software Shared Features

All Cisco Catalyst 6500 Series supervisor engines, including the new Supervisor Engine 720, take advantage of the industry-leading software and management capabilities of the Cisco Catalyst 6500 Series. Customers can apply thei knowledge of Cisco Catalyst Operating System Software, Cisco IOS Software, CiscoWorks, and other graphical and Web-based network management tools without the need to learn a new command-line interface (CLI) or management system.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

ECT nº 03/2005 - CN
CPMI - CORREIOS
246
3702
Doc

Cisco Catalyst 6500 Series Chassis

Cisco Catalyst 6500 Series chassis can be deployed in the wiring closet, the distribution and core layers, the data center, and the WAN edge, providing the power and features required for end-to-end deployment for the enterprise campus, the ISP network, metro, and research computing networks.

Chassis Applications

The Cisco Catalyst 6500 Series provides a selection of chassis, including 3-, 6-, 9-, and 13-slot models with slots arranged horizontally and a 9-slot model with slots arranged vertically, with front-to-back airflow. Typical applications for Cisco Catalyst 6500 Series chassis include:

- *3-slot chassis*—Low-density, wiring-closet chassis sharing interface modules and supervisor engines with larger chassis for common sparing; low-density, high-performance specialized services modules chassis for network security and management; low-density, high-end chassis providing connectivity to the WAN edge
- *6- and 9-slot chassis*—Traditional chassis for the wiring closet, distribution and core, data center, and WAN edge
- *13-slot chassis*—Highest-capacity chassis for Ethernet connectivity, with slots to spare for services modules providing network security and management

Chassis Configuration

All Cisco Catalyst 6500 Series chassis are NEBS Level-3 compliant and use common power supplies. The 6- and 9-slot chassis require a 1000W or 1300W power supply and the 13-slot chassis requires a 2500W or 4000W power supply. The 3-slot chassis requires a 950W power supply. When ordering a Cisco Catalyst 6500 Series switch, use the online Cisco Dynamic Configuration Tool to assist you in selecting the chassis, power supplies, power cables, and fan trays that will meet your requirements. The tool is available at:
http://www.cisco.com/appcontent/apollo/configureHomeGuest.html

Power

All Cisco Catalyst 6500 chassis hold up to two load-sharing, fault-tolerant, hot-swappable AC or DC power supplies. Only one supply is required to operate a fully loaded chassis. If a second supply is installed, it operates in a load-sharing capacity. The power supplies are hot-swappable—a failed power supply can be removed without powering off the system.

Cisco Catalyst 6500 Series switch power supplies are available in five power ratings:

- 950W AC input (Cisco Catalyst 6503 chassis)
- 1000W AC input
- 1300W AC and DC input
- 2500W AC and DC input
- 4000W AC input

Table 4 outlines the power requirements and heat dissipation for the three different models of power supplies available for the Cisco Catalyst 6500 Series switch.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

ECT nº 03/2005 - CN
CPMI - CORREIOS
247
Doc 3702

16.442
L.

Table 4 Power Supply VAC and VDC requirements

Power Supply	AC Input Voltage/Current	DC Input Voltage/Current
950W	100 to 240 VAC (10% for full range); 15 A	-48 VDC to -60 VDC continuous; 38 A @ -48 VDC, 30 A @ -60 VDC
1000W	100 to 240 VAC (10% for full range); 12 A @ 100 VAC, 6 A @ 240 VAC	Not supported
1300W	100 to 240 VAC (10% for full range); 17.25 A @ 100 VAC, 8 A @ 200 VAC	-48 VDC to -60 VDC continuous; 38 A @ -48 VDC, 30 A @ -60 VDC
2500W	100 to 120 VAC, 200 to 240 VAC (10% for full range); 16 A maximum at 200 VAC at 2500 W output; 16 A maximum at 100 VAC at 1300 W output	-48 VDC to -60 VDC continuous; 80 A @ -40.5 VDC, 70 A @ -48 VDC, 55 A @ -60 VDC
4000W	100 to 240 VAC (10% for full range); 23 A	Not supported

Fan Trays

Chassis that have a Supervisor Engine 720 installed require a high-speed fan tray. See Table 5 for part number information.

Table 5 Catalyst 6500 Chassis Fan Tray Part Numbers

Catalyst 6500 Chassis	Normal Speed Fan— Fan Tray Part Number	High Speed Fan— Fan Tray Part Number
6503	FAN-MOD-3	FAN-MOD-3-HS(=)
6506	WS-C6K-6SLOT-FAN	WS-C6K-6SLOT-FAN2
6509	WS-C6K-6SLOT-FAN	WS-C6K-9SLOT-FAN2
6509-NEB	WS-C6509-NEB-FAN	WS-C6509-NEB-FAN2
6509-NEB-A	N/A	FAN-MOD-09(=)
6513	WS-C6K-13SLOT-FAN	WS-C6K-13SLOT-FAN2

Dimensions

Table 6 provides Catalyst 6500 Series chassis dimensions.

Table 6 Catalyst 6500 Series Chassis Dimensions

Dimension	Cisco Catalyst 6503	Cisco Catalyst 6506	Cisco Catalyst 6509	Cisco Catalyst 6509-NEB	Cisco Catalyst 6513
H x W x D (in.)	7 x 17.37 x 21.75 in.	20.1 x 17.2 x 18.1 in.	25.2 x 17.2 x 18.1 in.	33.3 x 17.2 x 18.1 in.	33.3 x 17.3 x 18.1 in.
H x W x D (cm)	17.8 x 44.1 x 55.2 cm	51.1 x 43.7 x 46.0 cm	64.0 x 43.7 x 46.0 cm	84.6 x 43.7 x 46.0 cm	84.6 x 43.7 x 46.0 cm

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

CPMI
File N° 248
Doc 3702

Table 6 Catalyst 6500 Series Chassis Dimensions

Dimension	Cisco Catalyst 6503	Cisco Catalyst 6506	Cisco Catalyst 6509	Cisco Catalyst 6509-NEB	Cisco Catalyst 6513
Rack units (RU); 1.75 in., 4.4 cm	4 RU	12 RU	15 RU	20 RU	20 RU

Weight

Table 7 provides the weight information for empty and fully configured Catalyst 6500 Series chassis.

Table 7 Catalyst 6500 Series Chassis Weights

Weight	Cisco Catalyst 6503	Cisco Catalyst 6506	Cisco Catalyst 6509	Cisco Catalyst 6509-NEB	Cisco Catalyst 6513
Chassis only (lb)	27	45	55	55	98
Fully configured (lb)	83	115	135	135	240
Chassis only (kg)	12	20	25	25	45
Fully configured (kg)	38	52	61	61	109

Cisco Systems, Inc.
All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

FOLHA Nº 03/2005 - CPMI CORREIOS
Nº 3702 Doc 249

Ordering Information

Table 8 provides part number information for Catalyst 6500 Series chassis

Table 8 Catalyst 6500 Series Chassis Part Numbers

Part Number	Chassis
WS-C6503	Cisco Catalyst 6503 chassis (three slots)
WS-C6506	Cisco Catalyst 6506 chassis (six slots)
WS-C6509	Cisco Catalyst 6509 chassis (nine slots)
WS-C6509-NEB	Cisco Catalyst 6509-NEB chassis (nine vertically oriented slots)
WS-C6509-NEB-A	Cisco Catalyst 6509-NEB chassis (nine vertically oriented slots)–enhanced
WS-C6513	Cisco Catalyst 6513 chassis (13 slots)

Environmental Conditions

Table 9 provides environmental information for Catalyst 6500 Series Chassis.

Table 9 Catalyst 6500 Series Chassis Environmental Conditions

Parameter	Performance Range
Operating temperature	32 to 104 F (0 to 40 C)
Storage temperature	–4 to 149 F (–20 to 65 C)
Relative humidity	10 to 90%, noncondensing
Operating altitude	3000 meters
Mean time between failure (MTBF)	7 years for system configuration

RQS nº 03/2005 - CN
CPMI CORREIOS
Fls. Nº 250
Doc 3702

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Regulatory Compliance

Safety

- UL 1950
- EN 60950
- CSA C22.2 no. 950
- IEC 60950
- AS/NZA 3260
- 21 CFR 1040
- EN 60825-1
- IEC 60825-1
- TS 001

EMC

- FCC (CFR 47, Part 15) Class A
- VCCI
- CE Marking
- EN 55022
- EN 55024
- CISPR 22
- AS/NZS 3548
- NEBS Level 3 (GR-1089-CORE, GR-63-CORE)
- ETSI ETS-300386-2

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 251
Doc 3702

Specifications

Table 10 provides an overview of Catalyst 6500 Series switches specifications, additional information can be found in software release notes.

Table 10 Catalyst 6500 Series Specifications

Specification	Number	Description
IEEE Compliance		
802.1	802.1d	Bridging
	802.1p, q	VLAN tagging
	802.1s	Per-VLAN Group Spanning Tree Protocol
	802.1w	Rapid Spanning Tree Protocol
	802.1x	
802.1	802.3	10BASE-T, 10BASE-FL
	802.3ad	Link aggregation
	802.3ab	1000BASE-T
	802.3ae	10 Gigabit Ethernet
	802.3u	100BASE-TX, 100BASE-FX
	802.3x	Flow control
	802.3z	1000BASE-SX, 1000BASE-LX
RFC Compliance		
ATM	1483, 2584	Protocol encapsulation over ATM AAL-5
		ATM permanent virtual circuit (PVC) to 802.1q tagging
BGP4	1269	Definitions of Managed Objects for the Border Gateway Protocol (Version 3)
	1745	Border Gateway Protocol/Open Shortest Path First (BGP/OSPF) interactions
	1771	BGPv4
	1965	BGP4 autonomous system confederations
	1966	BGP4 route reflection
	1997	Communities attribute
	2385	Transmission Control Protocol (TCP) MD5 authentication for BGP
	2439	Route flap dampening
	2796	Route reflection
	2842	Capabilities advertisement
General routing protocols	768	User Datagram Protocol (UDP)
	783	Trivial File Transfer Protocol (TFTP)
	791	IP

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Fls Nº
Doc 3702

Table 10 Catalyst 6500 Series Specifications

Specification	Number	Description
	792	Internet Control Message Protocol (ICMP)
	793	TCP
	826	Address Resolution Protocol (ARP)
	854	Telnet
	894	IP over Ethernet
	903	Reverse Address Resolution Protocol (RARP)
	906	TFTP Bootstrap
	951, 1542	BootP, BootP extensions
	1027	Proxy ARP
	1122	Host requirements
	1256	ICMP Router Discovery Protocol (IRDP) IPv4 router discovery
	1519	Classless interdomain routing (CIDR)
	1541	Dynamic Host Control Protocol (DHCP)
	1591	Domain Name System (DNS) client
	1619	PPP over SONET
	1662	PPP HDLC-like framing
	1812	IPv4
	2131	BootP/DHCP
	2338	VRRP
		Internetwork Packet Exchange Routing Information Protocol/ Service Advertising Protocol (IPX RIP/SAP)
		Software-controlled redundant ports
IP multicast	1112	Internet Group Management Protocol (IGMP)
	1122	Host extensions, Distance Vector Multicast Routing Protocol (DVMRP)
	2236	IGMP v1, v2, v3 IGMP v1, v2, v3 Snooping
	2283	Multicast Border Gateway Protocol (MBGP)
	2362	Protocol-Independent Multicast (PIM)-SM
		DVMRP v3-07 Multicast Source Discovery Protocol (MSDP)
		PIM-Dense Mode (PIM-DM) v1

BOS nº 03/2005 - FN
CPMI - CORREIOS
Fls. Nº 252
Doc. 3702

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Table 10 Catalyst 6500 Series Specifications

Specification	Number	Description
		PIM-DM v2 Bidirectional PIM (Supervisor Engine 720 only)
Intermediate system to Intermediate system (IS-IS)	1195	TCP
	1377	PPP
	2763	Dynamic host name exchange
	2966	Domain-wide prefixes
LSP tunnels	2211	Controlled load network element service
	2702	Traffic engineering over MPLS
MPLS	2547	MPLS VPN
	2961	Resource Reservation Protocol (RSVP) refresh
	3031	MPLS architecture
	3032	MPLS label stack encoding
	3036	Label Distribution Protocol (LDP)
OSPF	1583	OSPF v2
	1587	OSPF NSSA
	1745	OSPF interactions
	1765	OSPF database overflow
	1850	OSPF v2 Management Information Base (MIB), traps
	1997	Communities and attributes
	2154	OSPF digital signatures, MD5
	2178	OSPF v2 (superceded by RFC 2328)
	2328	OSPF v2
	2370	OSPF opaque link-state advertisement (LSA) option
	2385	TCP M5
	2439	Route flap damping
	2842	Capabilities advertisement
	2918	Route refresh capability
RIP	1058	RIP v1
	1723	RIP v2
	2453	RIP v2

Cisco Systems, Inc.
All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Table 10 Catalyst 6500 Series Specifications

Specification	Number	Description
Miscellaneous protocols	1866	HTML
	2030	Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI
	2068	HTTP
Denial of service (DoS) protection	2267	Network Ingress Filtering
		ACLs: wire-speed
		ICMP and IP-option control
		IP broadcast forwarding control
		Rate limiting using ACLs
		Unicast Reverse Path Forwarding (RPF)
		Server load balancing with Layer 3 and Layer 4 protection
		SYN attack protection
		Session control
Network management	782	VLAN Trunking Protocol (VTP)
	783	TFTP
	854	Telnet
	951	BOOTP
	1155	Structure of Management Information (SMIv1)
	1156	TCP/IP MIB
	1157	Simple Network Management Protocol (SNMP)v1
	1212	MIB definitions
	1213	SNMP MIB II
	1215	SNMP traps
	1256	ICMP router discovery
	1285	Station management (SMT) 7.3
	1354	IP forwarding table MIB
	1493	Bridge MIB
	1516	Ethernet repeater MIB
	1573	Interface table MIB
	1643	Ethernet MIB
	1650	Ether-like MIB

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

CPMI CORREIOS
Fls Nº 254
Doc 3702

Table 10 Catalyst 6500 Series Specifications

Specification	Number	Description
	1657	BGPv4 MIB
	1724	RIPv2 MIB
	1757	RMON MIB
	1850	OSPFv2 MIB
	1901, 1907	SNMPv2c
	1908	SNMPv1/v2 coexistence
	2021	RMON2 probes
	2037	ENTITY-MIB
	2096	IP forwarding
	2233	Interface MIB
	2613	RMON analysis for switched networks (SMON) MIB
	2668	802.3 media attachment unit (MAU) MIB
	2787	VRRP MIB
	2925	Ping/Traceroute/NS Lookup MIB
		Sampled Netflow
		999 local messages
		BSD Syslog with multiple servers
		Configuration logging
		CISCO-CDP-MIB
		CISCO-COPS-CLIENT-MIB
		Cisco Discovery Protocol
		CISCO-ENTITY-FRU-CONTROL-MIB
		CISCO-PAGP-MIB
		CISCO-STACK-MIB
		CISCO-STP-Extensions-MIB
		Cisco Traffic Director Software
		CISCO-UDLDP-MIB
		CiscoView
		CISCO-VLAN-Bridge-MIB
		Cisco VLAN Director Software
		CISCO-VLAN-Membership-MIB

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN
Fls. Nº 255
Doc 3702

Table 10 Catalyst 6500 Series Specifications

Specification	Number	Description
		CISCO-VTP-MIB
		Cisco Workgroup MIB
		SPAN and Remote SPAN (RSPAN)
		Hot Standby Routing Protocol (HSRP)
		HC-RMON
		HTML/HTTP management
		NetFlow v1 export
		RMON HP Open View
		SMON-MIB
		Standard Cisco IOS Software security capabilities: passwords and TACACS+
		Telnet client
		Telnet management
		Text-based CLI
		Web-based GUI Management Tools (CiscoWorks)
Security	1492	Terminal Access Controller Access Control System Plus (TACACS+)
	2138	Remote Authentication Dial-In User Service (RADIUS) authentication
		ACLs for Layers 2, 3, 4, and 7
		Access profiles on all routing protocols
		Access profiles on all management methods
		Media Access Control (MAC) address security/lockdown
		Network Address Translation (NAT)
		Network login (including DHCP/RADIUS integration)
		RADIUS accounting
		RADIUS per-command authentication
		Secure Copy Protocol (secure file transfer)

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 256
Doc 3702

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Technical Support Services

Whether your company is a large organization, a commercial business, or a service provider, Cisco is committed tc maximizing the return on your network investment. Cisco offers a portfolio of technical support services to help ensure that your Cisco products operate efficiently, remain highly available, and benefit from the most up-to-date system software.

The Cisco Technical Support Services organization offers the following features, providing network investment protection and minimal downtime for systems running mission-critical applications:

- Provides Cisco networking expertise online and on the telephone
- Creates a proactive support environment with software updates and upgrades as an ongoing integral part of your network operations, not merely a remedy when a failure or problem occurs
- Makes Cisco technical knowledge and resources available to you on demand
- Augments the resources of your technical staff to increase productivity
- Complements remote technical support with onsite hardware replacement

Cisco Technical Support Services include:

- Cisco SMARTnet™ support
- Cisco SMARTnet Onsite support
- Cisco Software Application Services, including Software Application Support and Software Application Support plus Upgrades

For more information, visit:
http://www.cisco.com/en/US/products/svcs/ps3034/serv_category_home.html

Additional Cisco Catalyst 6500 Series Information

For additional information about the following data sheets that describe Cisco Catalyst 6500 Series, supervisor engines, interface modules, SFM, and services modules, visit:

http://www.cisco.com/en/US/products/hw/switches/ps708/products_data_sheets_list.html

- Cisco Catalyst 6500 Series Supervisor Engine 1A and Supervisor Engine 2 Data Sheet
- Cisco Catalyst 6500 Series Supervisor Engine 720 Data Sheet
- Cisco Catalyst 6500 Series 10/100 and 10/100/1000 Ethernet Interface Modules Data Sheet
- Cisco Catalyst 6500 Series Gigabit Ethernet Interface Modules Data Sheet
- Cisco Catalyst 6500 Series 10 Gigabit Ethernet Interface Modules Data Sheet
- Cisco Catalyst 6500 Series FlexWAN Interface Modules Data Sheet
- Cisco Catalyst 6500 Series Switch Fabric Interface Modules Data Sheet
- Cisco Catalyst 6500 Series Content Services Module Data Sheet
- Cisco Catalyst 6500 Series Firewall Services Module Data Sheet
- Cisco Catalyst 6500 Series Network Application Module (NAM) Data Sheet
- Cisco Catalyst 6500 Series Intrusion Detection (IDS) Module Data Sheet
- Cisco Catalyst 6500 Series IPSec VPN Services Module Data Sheet
- Cisco Catalyst 6500 Series SSL Services Module Data Sheet

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 257
Doc 3702

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

16433

CISCO SYSTEMS

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the

Cisco Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland
Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland
Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Catalyst, Cisco, Cisco Systems, Cisco IOS, the Cisco Systems logo, EtherChannel, and SMARTnet are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0304R)

MH/LW4273 0403

CPMI - CORREIOS
258
Doc 3702

16.932
L

Segurança Tipo 1 doc 9

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 259
Doc. 3702

Cisco Systems

16 931

White Paper

CiscoWorks **VPN/Security Management Solution** (VMS) 2.1 Deployment Guide

Introduction

The Challenge

One of the challenges of network management is the ability to have a solution that is flexible and can adapt to the changing needs of a network. While it makes sense to have applications that provide basic network management functionality regardless of function, the network environment must also be considered. In this case, it makes more sense to have a focused set of tools for management. For example, a tool that focuses on managing Quality of Service (QoS) levels is not necessarily (and most likely not) going to be very good at managing a server farm topology.

Growth and Enhancements in Network Security

If we look at the network as a strategic asset to the enterprise, network management clearly becomes an important factor in the success of the company. When we consider the evolution of business applications running across the traditional data network including e-commerce, business-to-business transactions, voice over IP (VoIP), the need to provide secure network connections grows. As a result, we have witnessed a proliferation in virtual private networks (VPNs) and an enhanced awareness of network security, setting the stage for reliable security management.

Paper Objective

The purpose of this paper is to provide guidance on how to effectively deploy CiscoWorks VPN/Security Management Solution (VMS). Covered topics include: server, installation, and operating system requirements; reference topology; metrics to monitor; and device configuration considerations. This is intended to supplement the CiscoWorks VMS Quick Start Guide and User Manual. We address such questions as: Which products are included and what are they used for? How many servers will be needed? What devices can be managed with this application? By answering these questions, we can provide some basic best practices for managing specific Cisco security technology.

What It Does Not Do

This paper does not replace User Guides (and other product documentation). It does not go into comprehensive detail about the various features or capabilities of the products.

Intended Audience

This paper is intended for audiences who are already familiar with network security, VPNs, firewalls, and intrusion detection. The audience should already have a basic understanding of these concepts and tools; our goal is to show how best to deploy CiscoWorks VMS in a production environment.

ECT Nº 03/2005 - CN
CPMI CORREIOS
Fls. Nº 260
Doc 3702

Cisco Systems, Inc.
All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

High-level Overview of CiscoWorks VMS 2.1

What Does It Do?

The CiscoWorks VMS solution is a set of integrated tools that provide a comprehensive solution for VPN and security management. CiscoWorks VMS features are positioned for configuring, monitoring, and troubleshooting enterprise VPNs, firewalls, and network- and host-based intrusion detection systems (IDS). VMS provides key features to assist customers in the deployment, monitoring, and management of their security-specific hardware. It also provides the operational management support, software distribution, configuration archive, change-audit, and syslog management for different elements of a Cisco security infrastructure. VMS provides a scalable solution that addresses the needs of small- and large-scale VPN and security deployments.

CiscoWorks VMS 2.1 Components

The CiscoWorks VPN/Security Management Solution (CiscoWorks VMS) consists of installable software components for flexible deployment options. Table 1 lists the different CiscoWorks VMS modules and their basic usages.

Table 1 CiscoWorks VMS 2.1 Modules

VMS Module	Usage
Auto Update Server	Permits configurations to be pulled from update server
CD-One/CiscoView	Provides graphical device management
Cisco IDS Host Sensor and Console	Configures host-based IDS to protect critical servers
Cisco Secure Policy Manager	Configures Cisco PIX Firewall, Cisco IOS Software firewall, and VPN
Common services	Provides a set of common software and services for the Management Centers
Management Center for IDS Sensor	Configures network-based IDS
Management Center for PIX Firewalls	Configures PIX Firewalls
Management Center for VPN routers	Configured VPN routers
Monitoring Center for Security	Monitors network and host-based IDS events, IOS and PIX syslog
Resource Manager essentials	Provides operational management, such as software distribution, change audit, syslog analysis
VPN Monitor	Monitors IPSec-based site-to-site and remote access VPN

These components can be classified into three distinct categories: Core asset management applications, monitoring applications, and security configuration applications. This section details some of the basic features associated with each product.

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

16.429
L.

Core Asset Management Applications

CD-One (CiscoView)

CD-One software provides the Common Management Foundation (CMF) for CiscoWorks. This includes basic components on the management server such as the web server, common database, polling engine, and so forth. In many deployments, this is the first CD to be installed from CiscoWorks VMS since it is the prerequisite for other applications. In addition to the CMF, CD-One provides the web-based CiscoView application. CiscoView provides graphical browser-based access to real-time devices status and simple network management protocol (SNMP) configuration capabilities.

CiscoWorks Resource Manager Essentials

CiscoWorks Resource Manager Essentials (RME) provides the basic network management tools for day-to-day network management, including inventory, configuration, change audit, and syslog. RME also provides additional VPN management capabilities. Network administrators can now produce device configuration, software image, and syslog reports specific for VPN environments.

Security Monitoring Applications

CiscoWorks VPN Monitor

CiscoWorks VPN Monitor allows users to monitor the status of their VPN devices and tunnels. This application collects, stores, and reports statistics for VPN-capable devices, including Cisco VPN routers, and the Cisco VPN 3000 Series Concentrator. The VPN Monitor supports the two major classes of VPNs (site-to-site and remote access) as well as multiple tunneling protocols, including Layer 2 Tunneling Protocol, Point-to-Point Tunneling Protocol (PPTP), and IP security (IPsec).

CiscoWorks Monitoring Center for Security

The CiscoWorks Monitoring Center for Security, or Security Monitor, monitors IDS events from various Cisco devices. These include network IDS sensor appliances, Cisco Catalyst® 6000 IDS modules, Cisco IOS® Software IDS syslog messages, Cisco PIX® Firewall syslog messages, and Cisco host IDS events.

Security Configuration Applications

CiscoWorks Common Services Software

CiscoWorks Common Services Software includes basic components of the management server such as the Web server, common database, polling engine, and so forth. In many deployments, this is the first CD to be installed because it is the prerequisite for the Management Center tools in the CiscoWorks VMS bundle.

CiscoWorks Management Center for VPN Routers

CiscoWorks Management Center for VPN Routers (Router MC) is a VPN configuration and deployment tool for Cisco VPN routers with Cisco IOS Software. Router MC is a Web-based application installed on top of Common Services.

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 261
Doc 3702

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

CiscoWorks Management Center for PIX Firewalls

Management Center for PIX Firewalls (PIX MC) is a complete firewall and access rule policy configuration tool for Cisco PIX Firewalls. You can configure new Firewalls and import configurations from existing firewalls. PIX MC also provides a powerful tool for controlling changes made to your network, showing configuration and status changes. PIX MC is a Web-based application installed on top of CiscoWorks Common Services.

CiscoWorks Auto Update Server

The CiscoWorks Auto Update Server (AUS) is used to store and upgrade device configuration files and software images. Cisco PIX Firewall devices periodically contact the AUS to request configuration and software updates. In this way, PIX Firewall devices are actively kept up to date. AUS is a Web-based application installed on top of CiscoWorks Common Services.

CiscoWorks Management Center for IDS Sensors

CiscoWorks Management Center for IDS sensors (IDS MC) is an IDS configuration and deployment tool for Cisco IDS sensor appliances and Cisco IDS Modules. IDS MC is a web-based application installed on top of Common Services.

Cisco IDS Host Sensor

Working as a complementary technology to IDS MC and Security Monitor, the Cisco Host Intrusion Detection System (HIDS) application protects critical servers and hosts by integrating with the operating system. By intercepting system calls to the kernel, Cisco HIDS software can protect the users' hosts by identifying attacks and preventing access to resources and unauthorized transactions.

Cisco Secure Policy Manager

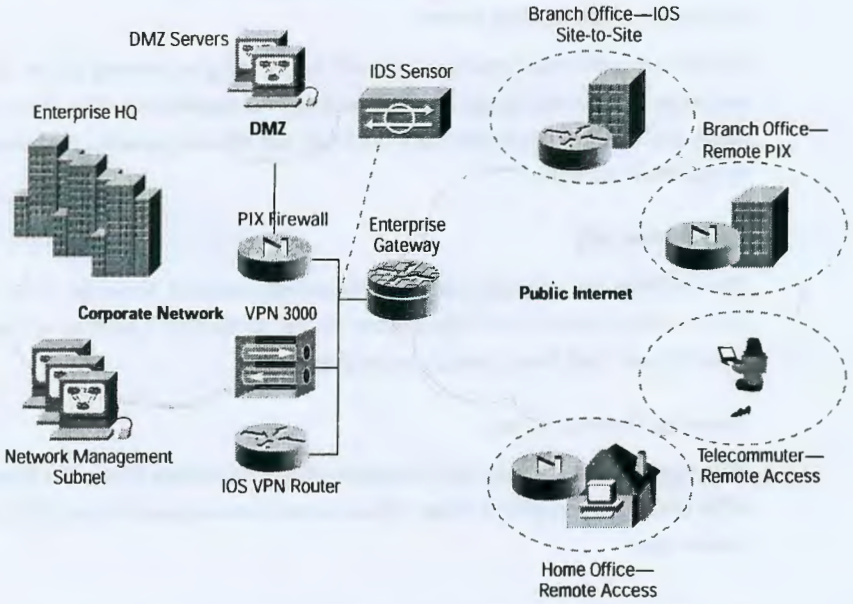
Cisco Secure Policy Manager (CSPM) is a policy-based application that allows network and security administrators to define and deploy perimeter security policies on mixed Cisco PIX Firewalls and Cisco IOS routers with the firewall feature set. CSPM also facilitates the deployment of site-to-site, mixed-environment VPN topologies.

Reference Topology

In order to describe how best to deploy the CiscoWorks VMS, we will use a reference network topology that sh the different aspects of VPN and network security (Figure 1). While obviously not identical to most customer environments, it does serve to provide a holistic view of a secure network. The intent is that by providing this reference, readers will be able to select the different components that best represent their topology and hence, understand how best to deploy CiscoWorks VMS in their environment.

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Figure 1
Reference Security Topology



The infrastructure involved:

a. Enterprise Gateway: This is a Cisco IOS router with the firewall feature set. The main purpose of this device is to perform the gateway routing and the basic frontline firewall functionality.

b. Cisco PIX Firewall: The Cisco PIX Firewall provides the comprehensive firewall functionality for this enterprise network. By strategically placing these devices at network access points, the corporate network resources are protected as a result of this firewall.

c. Cisco 800, 1700, 2600, 3600, 7100 or 7200 Series routers: Cisco routers act as site-to-site VPN termination points. In a hub-and-spoke VPN topology, the high-end VPN routers act as hubs, and the small- to medium-sized routers act as spokes.

d. Cisco VPN 3000 Series Concentrator: The VPN 3000 Series Concentrator is designed to provide scalable remote access VPN termination. In this topology the concentrator terminates VPN connections with a variety of remote access environments, VPN client software, and tunneling protocols (IPSec, L2TP, PPTP).

e. Cisco VPN remote-access client software: This software allows remote access users to connect to the corporate network via VPNs.

f. Cisco IDS Network Sensor: This device sits on a network segment and passively "listens" to the traffic, inspecting it against a database of common attack signatures. It forwards IDS event information to the monitoring station.

g. Cisco host-based IDS agents: Software that sits on critical network servers that protect individual hosts from intrusion and attacks. Events are forwarded to a central monitoring console.

h. Network Management Subnet: This subnet represents a dedicated network segment for the network management servers. The components of CiscoWorks VMS will reside in this subnet to manage the different pieces of the infrastructure.

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

i. Demilitarized zone (DMZ) Servers: This subnet represents a dedicated network segment for publicly accessible network servers. Generally, this includes e-mail, Web, File Transfer Protocol (FTP) servers, and in our case will include the Auto Update Server.

Within our reference topologies, we will be focusing on several pieces of the infrastructure that CiscoWorks VMS manages. That is not to say that the network management applications within VMS cannot manage other pieces (such as Cisco Catalyst switches), but these are the components that should be the focal point of VMS. These components include:

Enterprise HQ

This includes the network management servers, internal firewalls, VPN termination points (both hub routers and VPN concentrators), and IDS sensors. Access to the DMZ portion of the network will be controlled by internal firewalls and also have publicly accessible servers.

Remote Access Sites

The remote access sites in our topology contain the remote Cisco PIX Firewalls, remote IOS VPN routers, and remote VPN clients. These pieces of the infrastructure are responsible for VPN termination and firewall access policy at the remote site.

Software Requirements for CiscoWorks VMS

CiscoWorks VMS is composed of a series of tools that reside on a network management server (or servers). This section covers the prerequisite software needed in order to install and run the components within VMS. Primarily, this refers to operating system (OS) support. For almost every application in the VMS bundle, the supported OS is Windows 2000 Professional or Server. This is summarized in Table 2.

Table 2 Supported OS for CiscoWorks VMS Modules

CiscoWorks VMS Module	Windows Support	Solaris Support
CD-One	X	X
Resource Manager Essentials	X	X
VPN Monitor	X	X
Common Services	X	
Management Center for PIX Firewalls	X	
Auto Update Server	X	
Management Center for VPN routers	X	
Management Center for IDS Sensor	X	
Monitoring Center for Security	X	
Cisco IDS Host Sensor and Console	X[1]	
Cisco Secure Policy Manager	X	

1. Windows NT 4.0 Server, Enterprise Server (SP4 or later), Windows 2000 Advanced Server

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

16425

To run the CiscoWorks VMS components on a Windows 2000 system, the following requirements must be considered.

- Windows 2000 (Service Pack 2 or later)
- IE 5.5 SP2 or later
- ODBC Driver Manager 3.510 or later
- NTFS File System
- Do not install VMS on a server that is a:
  - Primary domain controller
  - Backup domain controller
  - Terminal server

Mitigating Threats

Now that we have the basic hardware and software requirements, we must consider how to configure the servers themselves to be ready for management. As a general security axiom, to secure hosts, pay careful attention to each of the components within the systems. Keep all systems up to date with the latest patches, fixes, and so forth. In the particular case of VMS, it is important to have the latest Windows 2000 patches and hot-fixes for security. Following is a detailed checklist of items to make sure the Windows 2000 server is ready to be used as a management server:

- Install the operating system on its own partition
- Use strong passwords
- Avoid creating network shares
- Disable unnecessary accounts
- Secure the Registry
- Apply all hot-fixes and security patches
- Disable unused and unneeded services (at a minimum, Windows requires the following services to run: DNS Client, Event Log, Plug & Play, Protected Storage, and Security Accounts Manager. Do not install IIS.)
- Disable all network protocols except Internet Protocol (TCP/IP)
- Monitor the security of your system regularly
- Limit physical access to your server
- Do not install remote access or administration tools on the server
- Periodically run a virus scanning application on the server

Hardware Considerations for CiscoWorks VMS

Along with the software requirements, be aware of the hardware requirements for the CiscoWorks VMS bundle. Then the inherent challenge is deciding how best to deploy the different applications in the solution. Since there are eleven installable software applications, there are numerous combinations in which to deploy them.

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 263
Doc 3702

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Platform and Specs

The following server system requirements are specified in the VMS bundle documentation:

- Pentium III 1GHz CPU
- 1 GB RAM
- 2 GB virtual memory
- 9 GB free hard disk space

These are minimum requirements, and consideration should be given to the difference in recommended system specifications based upon different sized networks and configurations. For example, consider three different sized configurations: small, medium, and large. The first thing to think about is scalability. In other words, how many devices equate to a small, medium, and large configuration?

Scaling

Each application within CiscoWorks VMS has a different scalability metric. Table 3 provides the theoretical maximum for each of the applications.

Table 3 Theoretical Scale Limits for CiscoWorks VMS Applications

CiscoWorks VMS Module	Scalability Metric (tested up to[1])
IDS MC	300 IDS sensors
Security Monitor	500 events/sec[2]
PIX MC	1000 PIX Firewalls
AUS	1000 PIX Firewalls
Router MC	1000 VPN routers
CSPM	200 devices
RME	5000 devices inventory, 1000 devices availability
VPN Monitor	30 devices on dashboard (hard limit)
Cisco IDS Host Console	300 host agents

1. The theoretical scale limits define what the tools have been tested up to. The numbers are stated as a guideline to guarantee reasonable performance and user experience. Although possible, it is not recommended to exceed these metrics.
2. If the volume of security events exceeds 500/second for extended periods of time, it is recommended that users consider a monitoring product from a partner-vendor that can handle higher event volumes.

These are not software-imposed limits, but rather the scale limitations based on testing maximums. For example, if a user wants to add device number 1001 to Router MC, the software will allow it. However, from a support standpoint, we do not recommend doing this.

Also note that the specifications for the minimum recommended hardware system for CiscoWorks VMS are based on testing and performance statistics for ONE (not all) of the applications in the bundle. For example, if you are using IDS MC to manage 300 sensors (the theoretical maximum), we do NOT recommend using any other applications on that server. If you plan to heavily use more than one application within VMS, it is highly recommended to put them on separate servers.

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

16.4.2.3

The following tables list some of the more resource-intensive applications within the bundle, and configuration is broken down into small, medium, and large configuration metrics in Tables 4-6, respectively.

Table 4 Small Configuration Metrics (reflects restricted CiscoWorks VMS license model)

CiscoWorks VMS Module	Scalability Metric (up to)
IDS MC	20 IDS sensors
Security Monitor	200 events/sec
PIX MC	20 PIX Firewalls
AUS	20 PIX Firewalls
Router MC	20 VPN routers
CSPM	20 devices

Table 5 Medium Configuration Metrics (This configuration represents the majority of the CiscoWorks VMS customer base):

CiscoWorks VMS Module	Scalability Metric (up to)
IDS MC	100 IDS sensors
Security Monitor	300 events/sec
PIX MC	100 PIX Firewalls
AUS	100 PIX Firewalls
Router MC	100 VPN routers
CSPM	50 devices

Table 6 Large Configuration (Reflects the theoretical maximum scalability metrics.)

CiscoWorks VMS Module	Scalability Metric (up to)
IDS MC	300 IDS sensors
Security Monitor	500 events/sec
PIX MC	1000 PIX Firewalls
AUS	1000 PIX Firewalls
Router MC	1000 VPN routers
CSPM	200 devices

Fls Nº 264
3702

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Server Sizing

Based on these factors, a closer examination of the recommended server sizing for each configuration is now possible. It is important to note that these specifications are minimum requirements for individual applications and are frequently exceeded in many deployments. The general rule of thumb here is, if it is necessary to choose one metric that will have the greatest affect on performance, then increase the amount of RAM. It is also important to pay attention to the scale limits of each application. If you are approaching some of those theoretical limits, it might be a good idea to increase the horsepower of your VMS server(s). For example, it is not out of the question to see a P4 2.2GHz CPU with 4 GB of RAM running VMS applications. For a general guideline, please see Table 7.

Table 7 Server Recommendations for CiscoWorks VMS Configurations

Configuration	Small	Medium	Large
CPU	PIII 1GHz	PIII 1.4GHz	P4 2.0GHz
RAM	1 GB	1.5 GB	2 GB
Virtual memory	2 GB	3 GB	4 GB
Hard disk space	9 GB	20 GB	40 GB

Server Deployment Rules of Thumb

In terms of application compatibility, there are several rules to follow:

- CD-One, RME, and VPN Monitor MUST reside on the same server.
- Router MC, IDS MC, Security Monitor, PIX MC, and AUS must be installed on top of Common Services. However, since more than one instance of Common Services can be installed, these can still be deployed across different servers.
- CD-One MUST be installed before Common Services.

Given these conditions, CiscoWorks VMS can have extremely flexible deployments. All of the components can be installed and run on a single server. On the other side of the spectrum, each of these components can be installed on its own individual server. This extreme is not practical and deployment will generally depend on a number of factors including the following four:

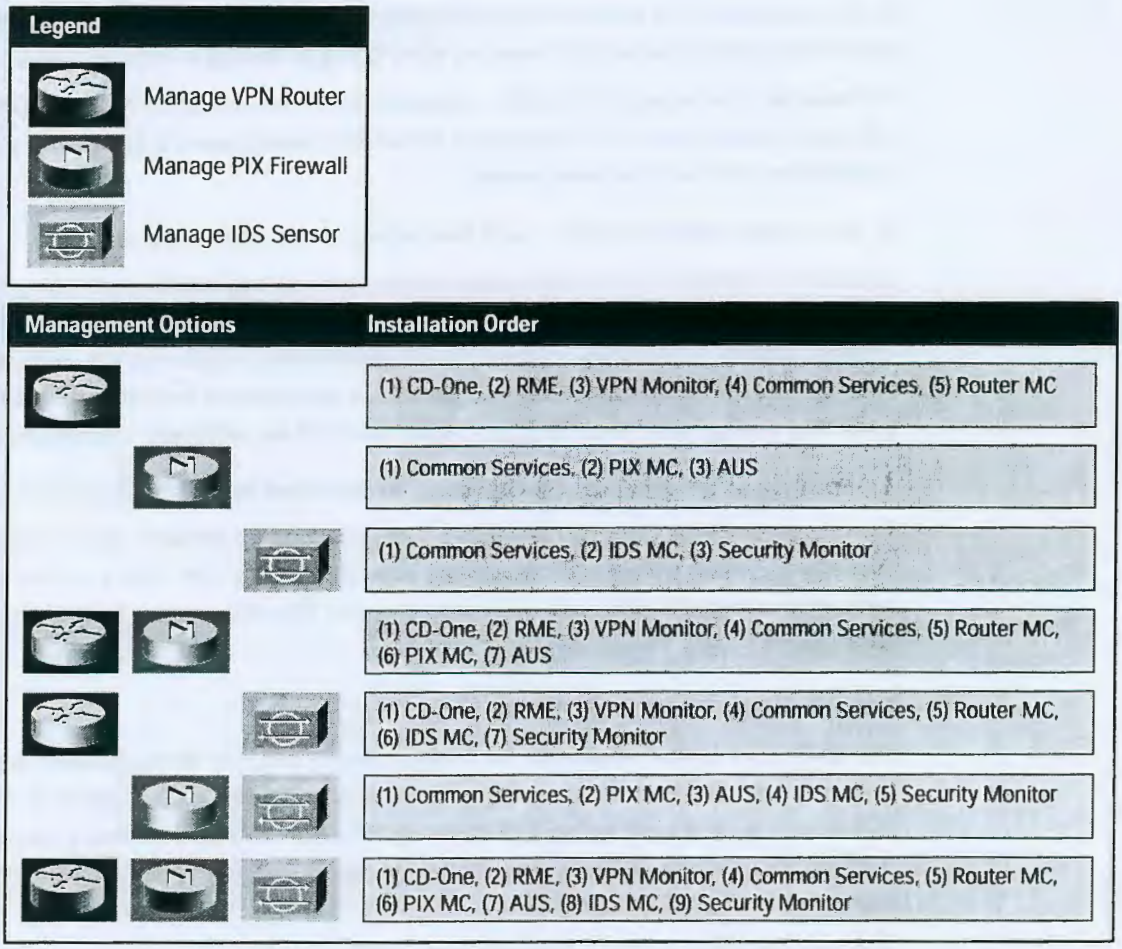
1. Which applications do you actually need?

Although VMS provides a rich, comprehensive management solution, it is possible (and perhaps even probable) that users will not need every single tool. The first question that should be asked is: Which applications do I actually need? Once this has been determined, users can choose to install only the modules that are needed. Figure 2 shows a table that provides the installation order based upon the different management options provided they are installed on a single server.

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

16.423

Figure 2
CiscoWorks VMS Module Installation Matrix



Note: This table provides basic guidelines. Obviously, not all the combinations and tools within VMS are covered—just those with installation order dependencies.

- Installation Option 1: For VPN management, it is the monitoring component that is covered by CD-One, RME, and VPN Monitor. If monitoring is not necessary, these modules do not need to be installed.
- Installation Option 2: For PIX management, AUS is only necessary in order to take advantage of the auto-update feature for PIX configuration and software deployment.

RGS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 265
Doc. 3702

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

2. How many devices will each application manage?

If one of the applications being used is approaching its theoretical scale limits, it is a good idea to dedicate a server to that application. For obvious reasons of resource allocation and task distribution, it is best not to have other applications using valuable CPU resources when trying to manage a large number of devices.

For example, if an instance of PIX MC is installed that is managing 800 PIX Firewalls, and the user is also trying to roll out a hub and spoke VPN deployment across 600 router spokes, it is probably a good idea to break these applications apart onto dedicated servers.

3. How many administrators will me using these applications?

In some multi-administrator environments, it makes sense to explore different deployment options for VMS. Because there are so many applications involved, and they each have a very distinct purpose, it is possible that there will be different security administrators using different applications. In this case, it is probably better to split these applications onto dedicated servers. This way, if one application is busy with a resource-intensive task such as generating configuration files, the second application will not suffer any degradation in performance.

4. What types of cost restrictions exist in terms of server procurement?

Does the organization using CiscoWorks VMS have (or have the ability to get) multiple servers? In some cases, there may only be enough budget to allocate to one server. If this is the case, then it is always better to shoot for a high-end server that exceeds the minimum system requirements. This allows room for growth, as well as improved performance.

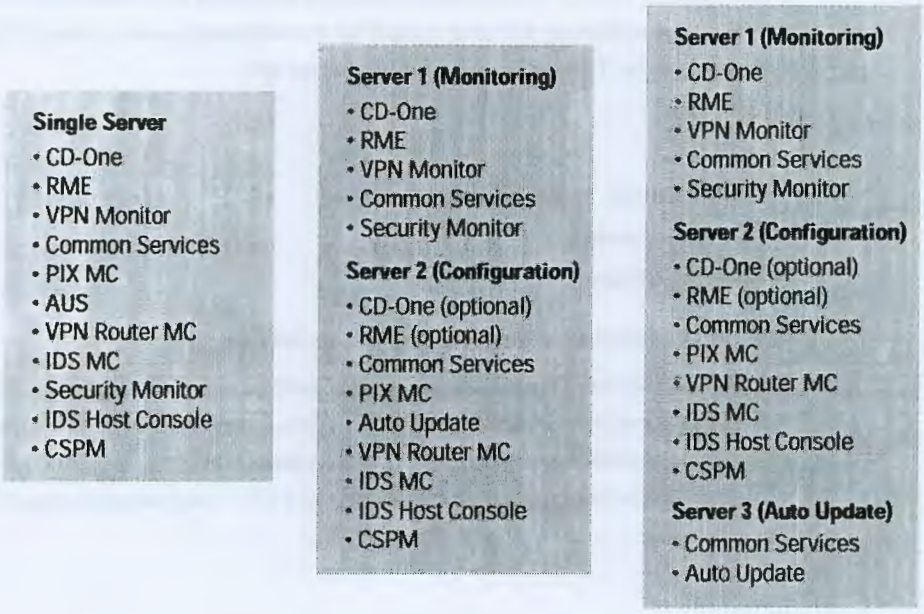
More is Better

The bottom line is, if at all possible, use multiple servers and split the applications across them as they make sense. Generally, for better scalability, resource allocation, task distribution, and room for growth, more is better as long as it doesn't become cumbersome and unmanageable. Also keep in mind that if you decide to combine multiple applications onto a single server, you will need to pay special attention to the hardware requirements of each application and adjust accordingly.

The following figure and section breaks down some basic deployment options and provides some general guidelines covering most customer scenarios (Figure 3). Note that these are simply recommendations, and do not necessarily indicate that CiscoWorks VMS must be deployed in this manner.

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Figure 3
Server Deployment Options



Option 1: Single Server Deployment

For small-scale security environments with a single network security administrator, a single server deployment is recommended. This has the benefit of being low cost to the organization and guarantees ease of administration.

Option 2: 2 Servers: Configuration and Monitoring

This deployment option breaks down the VMS applications across function. One server is dedicated for monitoring and the second server is dedicated for configuration.

Server 1: Configuration

This security management server is designed to combine all of the CiscoWorks VMS applications that assist in configuration. Whether the infrastructure is VPN Router, PIX Firewall, IDS Sensor, or Host IDS Agent, this server's primary function will be configuration. The relevant applications are:

- Common Services
- PIX MC
- AUS[1]
- VPN Router MC
- IDS MC
- Cisco Host IDS Console
- Cisco Secure Policy Manager (CSPM)

1. AUS primarily provides configuration and software updates to remote PIX Firewalls. For this reason, it is frequently recommended to place the AUS within the organization's DMZ. If this is the case, we recommend using a dedicated server for AUS.

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 266
Doc 3702

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Server 2: Monitoring

The second server in this deployment option is dedicated for monitoring. VPN Monitor is used for IPsec MIB monitoring and Security Monitor is used for consolidated event viewing of Post Office IDS, Host IDS, PIX, and IOS Syslog messages. The applications for this server are:

- CD-One
- RME
- VPN Monitor
- Common Services
- Security Monitor

Option 3: 3 Servers: Security Application Function

The third deployment option centers around splitting up the CiscoWorks VMS application according to security technology (or infrastructure) managed. The first server deals with VPNs, and generally this covers IOS-based VPN routers. The second server contains the applications used to manage the PIX Firewall. Finally, the third server is dedicated to the management and monitoring of IDS—both network-based and host-based IDS.

Server 1: VPN

- CD-One
- RME
- VPN Monitor
- Common Services
- VPN Router MC

Server 2: Firewall

- Common Services
- PIX MC
- AUS
- CSPM

Server 3: IDS

- Common Services
- IDS MC
- Security Monitor
- Cisco Host IDS Console

Option 4: 4 Servers: Granular Management Control

For greater granularity and scalability benefits, further divide the deployment. The main difference with this option is the use of a dedicated server for AUS, since it is placed within a different subnet of the network. The other difference is the use of a dedicated server for the policy management tool CSPM. This makes sense because CSPM does not have any natural integration with the other products in the bundle and it is also resource intensive. As such, it is recommended to split it up and have a dedicated system for policy management across mixed environments.

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

16417
L

Server 1: Configuration

- Common Services
- PIX MC
- VPN Router MC
- IDS MC
- Cisco Host IDS Console

Server 2: Monitoring

- CD-One
- RME
- VPN Monitor
- Common Services
- Security Monitor

Server 3: Remote Management (placed in DMZ)

- Common Services
- AUS

Server 4: Policy

- CSPM

Again, keep in mind that these are only recommendations. There are numerous combinations and deployment options available and each case should be considered on an individual basis. There will likely be many cases where customers don't even want to use all of the possible applications within VMS.

CiscoWorks VMS Applied

Now that we have determined how to deploy the components of CiscoWorks VMS from an installation perspective, we need to take a look at how these applications should be deployed from a functional standpoint. Three basic questions will be addressed in this section:

1. What is the management function of each application?
2. What devices can I manage?
3. What types of services do I need to enable?

The first question requires a detailed look into the capabilities of each product. This information is used to figure out what aspects of security management can and should be managed by each of the components within VMS. Answering the second question will clarify confusion surrounding the variances in device support by the component applications. Finally, the last question looks at how each application touches the device(s) that it manages. By examining the communication protocols being used, we can compile a list of requirements that ensures a successful deployment of VMS. For the sake of clarity, we will examine each of the questions on a product/server basis.

Note: The components of a Cisco network infrastructure are diverse and varied; however, for this discussion surrounding security, we will focus on five classes of objects: IOS routers, PIX Firewalls, VPN concentrators, IDS sensors, and IDS host agents. This does not imply that VMS is not able to manage other elements, simply that these are the pieces we must pay special attention to for security issues.

CPMI – CORREIOS
Fls. Nº 267
Doc 3702

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

A Word About Management Subnets (Out-of-Band Management)

In many networks, it is desirable to design a separate management subnet. This is commonly referred to as out-of-band management and describes a situation where the management stations reside on an isolated subnet separate from the network elements they are trying to manage. This is attractive to many network administrators due to the inherent higher level of security and clear functional division within their network.

As is the case with all network management tools, however, CiscoWorks VMS requires network access to the devices that it is trying to manage. So when making this decision, consider that, while it might be desirable to have a completely isolated management subnet, it will do no good unless there is IP connectivity to the rest of the network. This must be carefully planned out when deploying VMS in such an environment.

CD-One (CiscoView)

What is the management function?

CiscoView provides graphical Web-based device management. Users of CiscoView see a graphical representation on their computer screen and are able to monitor real-time device status, and in certain cases make configuration changes to those devices. From a CiscoWorks VMS perspective, CiscoView is positioned as a troubleshooting tool. If there is a problem within the network, and that problem has been isolated to a single device or interface, then CiscoView can be used to take a look at the statistics associated with that device and potential configure variable(s) to solve the problem.

What devices does it manage?

CiscoView provides support for the majority of the Cisco IOS routers, Cisco VPN 3000 Series Concentrators, and the Cisco PIX Firewall 501 and 506 Series.

Which services do I need to enable? (Application protocol requirements)

CiscoView relies entirely on SNMP get/set operations (UDP port 161) for its functionality. From the CiscoView server to the device, you need to enable SNMP traffic. Furthermore, the devices that you are managing must be configured to support SNMP. The Cisco IOS Software devices can support both get and set operations (for both monitoring and configuration), so both read and write community strings are configured separately to provide this level of granularity. For the VPN 3000 Concentrators and the PIX Firewalls, only SNMP read operations are supported—while you can monitor these devices, configuration using CiscoView is not possible.

Resource Manager Essentials

What is the management function?

Describing the functions of Resource Manager Essentials (RME) would take an entire paper by itself. In general (and from a security perspective), this application provides basic network management operations and administration. Basically, this tool provides:

- Inventory management to keep track of the devices within the infrastructure
- Configuration management to manage configuration of the network devices
- Change audit control to keep track of any changes (configuration or otherwise) occurring in the network
- Software image management to facilitate the maintenance of software versions
- Syslog management to receive and analyze syslog messages sourced from the network devices

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

16 415

This list confirms that RME functionality provides benefits beyond the scope of security infrastructure management. For the purposes of this discussion, focus is on the benefits it provides to our reference environment. Of special interest is the fact that RME can generate configuration reports, software image upgrade analysis, and syslog reports specific to VPN-related infrastructure and environments.

What devices does it manage?

RME provides support for Cisco IOS routers, VPN 3000 Concentrators, and PIX Firewalls (506, 515, 520, and 525 Series). For the concentrators, RME does NOT support configuration management and only provides limited support for software image management. For the PIX Firewalls, RME provides limited support for syslog management. Refer to the diagram of our reference topology and notice this covers all aspects of our network with the exception of the IDS sensor. For this reason, RME is frequently referred to as our "core" management application.

Which services do I need to enable? (Application protocol requirements)

RME depends on several protocols to manage its devices. These include SNMP, Telnet, TFTP, and Syslog, among others. Because the subcomponents of RME are so varied, along with the different devices, we've summarized the application protocol requirements for this tool in Table 8.

Table 8 CiscoView and RME Protocol Requirements

Application	Traffic Flow	Service(s)	TCP/UDP Port Number
CiscoView		SNMP	UDP 161
Inventory Manager		SNMP	UDP 161
Configuration Manager		Telnet TFTP SNMP	TCP 23 UDP 69 UDP 161
Software Image Manager		Telnet TFTP SNMP	TCP 23 UDP 69 UDP 161
Change Audit Services		Syslog	UDP 514
Availability Manager		Telnet SNMP ICMP	TCP 23 UDP 161 N/A
Syslog Analyzer		Syslog	UDP 514

RQS nº 03/2005 - CPMI - CORREIOS
Fls. Nº 268
Doc 3702

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Based on this matrix, it is necessary to make sure the devices being managed with RME are configured to provide the proper information. SNMP read (and write where applicable) community strings need to be configured. The Telnet service, along with a login password, needs to be enabled. Finally, the devices need to be configured to point their syslog messages at the RME server.

Common Services

What is the management function?

Common Services is a server environment that provides a common set of services and management functions to a suite of client applications—the Management Centers. These services and functions include the following:

- Data storage and management
- A web infrastructure
- Session management
- User authentication/permission management
- Common environment for multiple client applications

Common Services must be installed on the server before any of the MCs, Security Monitor, or AUS can be installed. These applications integrate with Common Services and use the services and management functions provided by Common Services.

Note: To install Common Services and CD-One on the same system, CD-One MUST be installed first! Common Services can be installed on top of an existing CD-One Edition 5 installation, which allows the user to install and access applications such as RME and Router MC from a single server.

What devices does it manage?

Common Services provides the server environment, and does not directly manage any particular network devices. The management is typically handled by the applications that sit on top of Common Services.

Which services do I need to enable? (Application protocol requirements)

Common Services is responsible for the web infrastructure of the VMS MC applications, so in terms of application protocols, it is important to maintain the connection from the Web client to the Web server. Typically this will be HTTP and HTTPS traffic through pre-assigned port numbers:

- TCP 1741
- TCP 1742
- TCP 1751

For a comprehensive list of TCP and UDP port numbers used by Common Services, please consult the product documentation "Installing CiscoWorks Common Services on Windows 2000."

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Management Center for VPN Routers

What is the management function?

Management Center for VPN Routers (Router MC) provides an easy management interface to set up and maintain VPN connections between multiple supported Cisco IOS Software devices in a hub-and-spoke topology. Router MC allows network managers to quickly and easily provision all critical connectivity, security, and performance parameters for a site-to-site, large-scale VPN. Utilizing a point-and-click web-based interface and preconfigured components for VPN creation, Router MC also allows the quick configuration of smaller, simpler VPNs. In addition to configuring hub and spoke VPNs, Router MC also lets users replace leased line connections with VPN connections, or prepare VPN configurations for routers not yet on the network

What devices does it manage?

Router MC is used to manage VPNs across Cisco IOS Routers. In general, the application is hardware-platform agnostic. It only cares about the version of Cisco IOS Software and the supported feature set. The basic rule is that the routers have to support IPsec, SSH, and named access lists. Table 9 lists the Cisco IOS Software versions that have been tested with Router MC.

Table 9 Supported Cisco IOS Software Versions in Router MC

Cisco IOS Software Platform	Minimum Cisco IOS Software Version
7100, 7200 (Hub)	12.1(9)E
3640/60 (Hub)	12.2(2)T, 12.2(3)
7100, 7200 (Spoke)	12.2(2)T, 12.2(3)
2610/20/50 and 3620/40/60	12.2(2)T, 12.2(3)
1720/50	12.2(2)T, 12.2(3)
806	12.2(1)XE
803	12.2(2)XH

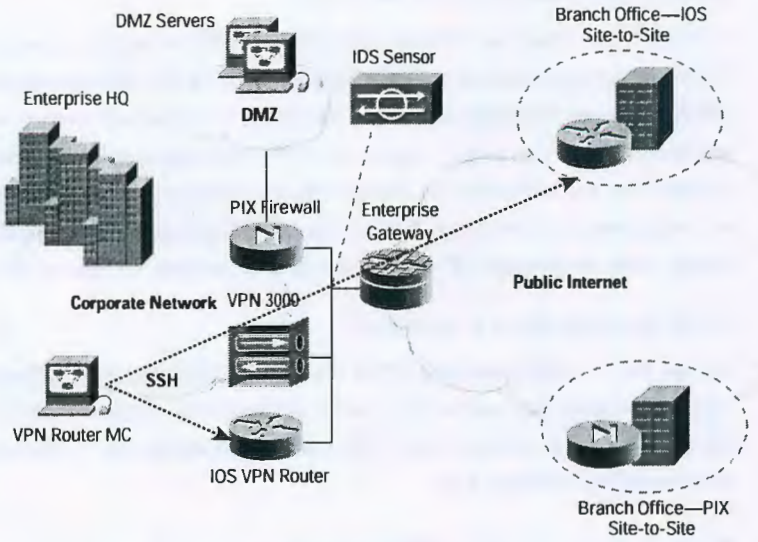
Which services need to be enabled? (Application protocol requirements)

Router MC uses SSH (TCP port 22) to configure the IOS routers. The SSH session is established when devices are initially imported into Router MC. Then when configurations are pushed out to the devices, this session is also encrypted via SSH. Figure 4 shows how Router MC is applied to our reference topology.

RGS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 269
Doc 3702

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Figure 4
Router MC Applied



Management Center for PIX Firewalls

What is the management function?

Management Center for PIX Firewalls (PIX MC) enables Cisco PIX Firewall infrastructure management by configuring new firewalls and importing configurations from existing firewalls. Firewall device settings, access rules, and translations rules can be configured, and these configuration changes can then be deployed to the firewalls on the network. PIX MC also provides a powerful tool for controlling changes made to the network, showing configuration and status changes.

What devices does it manage?

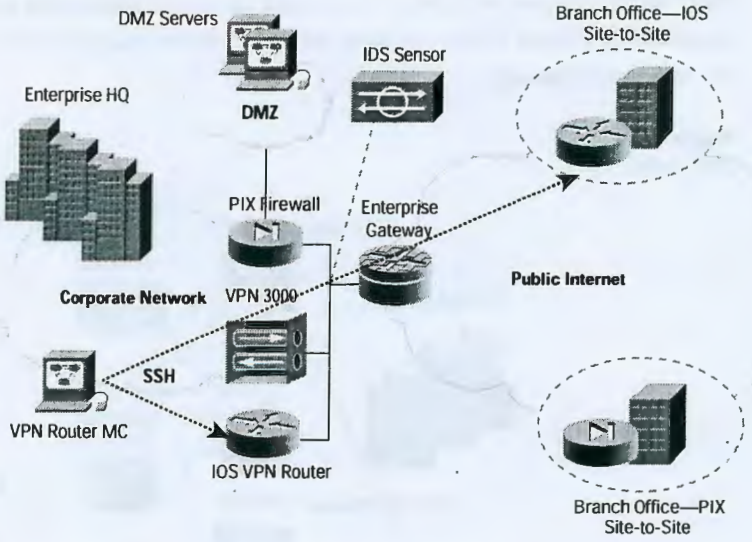
PIX MC is used to manage the PIX Firewall deployed throughout the network. These include all the PIX platforms: 501, 506E, 515E, 525, and 535 Series. The PIX MC supports the command sets for PIX OS version 6.1, and supports the Auto Update and the Easy VPN command sets found in version 6.2.

Which services must be enabled? (Application protocol requirements)

PIX MC uses an encrypted session to manage its PIX Firewall devices. The protocol that it uses is SSL (or HTTPS) and the port number assigned for this connection is TCP port 443. Therefore, it is necessary to permit TCP 443 to a PIX Firewall (from the management interface) in order for PIX MC to properly manage the device. Figure 5 shows how PIX MC is applied to our reference topology.

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Figure 5
PIX MC Applied



Auto Update Server

What is the management function?

AUS is responsible for storing configurations and software images for PIX Firewalls. Firewalls operating in auto-update mode periodically contact AUS to upgrade software images, configurations, and versions of PDM, and to pass device information and status to AUS. Using AUS also facilitates managing devices that obtain their addresses through Dynamic Host Configuration Protocol (DHCP) or that sit behind Network Address Translation (NAT) boundaries. Typically, because of this management function, the AUS is deployed in a publicly accessible DMZ which the remote side PIX Firewalls can contact directly.

What devices does it manage?

PIX MC is used to manage the PIX Firewalls deployed throughout your network. These include all the PIX platforms: 501, 506E, 515E, 525, and 535 Series. AUS requires that PIX Firewalls run OS version 6.2 since it requires the Auto Update feature.

Which services need to be enabled? (Application protocol requirements)

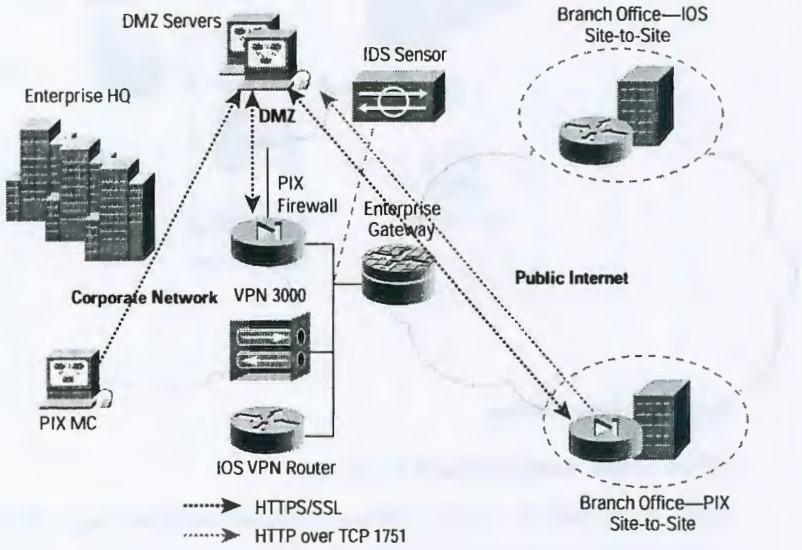
AUS talks to two different pieces in our topology diagram. The first piece it talks to is the PIX MC server. If these two applications are installed on the same system, no changes are necessary to the communication architecture. However, if they are installed on different servers, the PIX MC server will push configuration files to AUS using SSL, making it necessary to open up TCP 443 to the AUS system.

ECT nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 270
Doc 3702

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

The second piece is the actual communication between the AUS and the PIX Firewall itself. In this scenario, there is two-way communication and both occur via SSL. Therefore, it is not only necessary to open up TCP 443 to the AUS from the PIX, but also vice versa. For transfer of binary images (PIX and PDM software), this will be transferred via standard HTTP over TCP 1751 (this can optionally be changed to SSL). Figure 6 illustrates how AUS is applied to our reference topology.

Figure 6
AUS Applied



Management Center for IDS

What is the management function?

Management Center for IDS (IDS MC) manages configurations for Cisco Intrusion Detection System Sensors. All aspects of sensor configuration can be managed through a series of Web-based screens, including individual sensors or a group of sensors having a common configuration. The sensor configuration data resides in a database. IDS MC can also perform signature updates by downloading the update archives from the Cisco web location and then distributing these signature updates to the appropriate sensor groups.

A separate but closely related product, Monitoring Center for Security (Security Monitor), provides event collection, viewing, and reporting capability for network devices. This is covered in the next section.

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

What devices does it manage?

IDS MC manages the Cisco IDS appliance sensors as well as the Cisco IDS Module for the Catalyst 6500. The IDS software required for the application depends on the platform (See Table 10).

Table 10 Required IDS Sensor Software for IDS MC

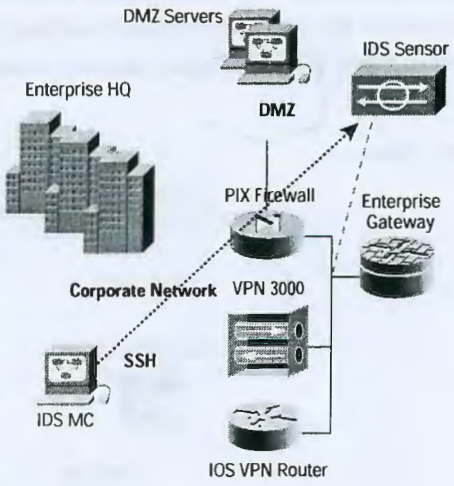
IDS Sensor Platform	Minimum Required Software
Cisco IDS Appliance Sensor	3.0.1[1]
Catalyst 6000 IDS Module	3.0.5[1]

1. IDS 4.0 software will be supported in a future release of IDS MC and Security Monitor.

Which services need to be enabled? (Application protocol requirements)

IDS MC uses two protocols to manage the IDS sensors: First, it uses Secure Shell (SSH) to secure remote login to the sensors. Second, it uses SCP to secure the transfer of the actual sensor configuration files. Session-Control Protocol (SCP) uses SSH for data transfer, so TCP 22 needs to be allowed to the sensors. Figure 7 illustrates how IDS MC is applied to our reference topology.

Figure 7
IDS MC Applied



Security Monitor

What is the management function?

Monitoring Center for Security (Security Monitor) provides a Web-based interface for event collection, viewing, and monitoring for the following devices:

- Cisco Intrusion Detection System Sensor running Post Office software
- Cisco IOS router running IDS software
- Host IDS Sensor via the Console
- PIX Firewall

RGS nº 33/2005 - CN
CPMI - CORREIOS
Fls: Nº 271
Doc 3702

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

The Security Monitor displays events on a customizable event viewer, and allows the user to write some basic event correlation rules to consolidate events. These rules can also be set up to kick off real time notifications.

What devices does it manage?

Security Monitor can receive security events from five sources with the following software requirements:

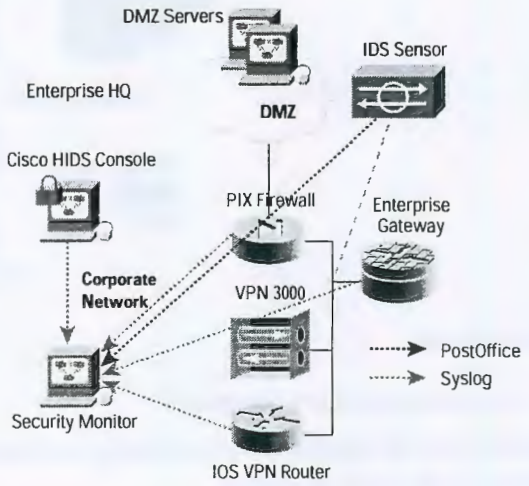
Table 11 Required Software for Security Monitor Devices

Security Event Source	Minimum Software Required
Cisco IDS Appliance Sensor	3.0.1
Catalyst 6000 IDS Module	3.0.5
IOS router	IOS with IDS features set
PIX Firewall	Any version that supports syslog
Host IDS Console	2.5 or later with integrator software

Which services do I need to enable? (Application protocol requirements)

Because of the number of data inputs, consider each of these individually in terms of application protocol requirements. For the Post Office devices (sensor appliance and IDS module), Security Monitor uses Post Office protocol to forward events. For the other data sources (Cisco IOS Software, PIX and Host IDS), the events are sent to Security Monitor via syslog. So make sure to allow Post Office (UDP 45000) and syslog (UDP 514) to the Security Monitor server. Figure 8 illustrates how Security Monitor is applied to our reference topology.

Figure 8
Security Monitor Applied



All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

16.407
L.

VPN Monitor

What is the management function?

VPN Monitor provides monitoring statistics for the enterprise head-end VPN devices—this means the "hubs" of a hub-and-spoke VPN topology. In our reference topology, this refers to both the Cisco 7X00 Series Router and the VPN 3000 Concentrator, so proper connectivity from the VPN Monitor server to those devices is necessary. This application provides statistical VPN information in both graphical and tabular format. It can also be used as a graphical notification tool when certain VPN-related thresholds (that are user configurable) are violated. With VPN Monitor, network administrators can get an overall view of how their VPNs are doing by looking at metrics that include encrypted traffic statistics, secure handshake negotiations, packet replays, and so on.

What devices does it manage?

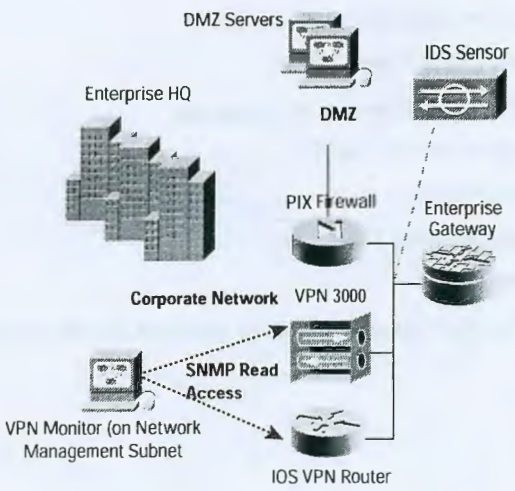
VPN Monitor supports Cisco IOS VPN routers with the necessary IPSec MIB support as well as VPN 3000 Concentrators. Currently, the application supports the Cisco1700, 2600, 3600, 7100, and 7200 Series routers. The software image version requirements are:

- 1700, 2600, or 3600 IOS Router—12.2(4)T or later
- 7100 or 7200 IOS Router—12.1(5a)E or later
- VPN Concentrator 3000 Series—2.5.2f or later

Which services do I need to enable? (Application protocol requirements)

Much like CiscoView, VPN Monitor requires SNMP (UDP port 161) to function. The VPN Monitor server periodically polls the devices to retrieve the IPSec MIB information. Since this is purely a monitoring tool, it is only necessary to consider SNMP get operations on these two classes of devices. This corresponds to configuring the SNMP read community string on the network devices that need to be managed with VPN Monitor. Figure 9 illustrates how VPN Monitor is applied to our reference topology.

Figure 9
VPN Monitor Applied



ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 272
Doc. 3702

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Note: Given these requirements, it IS possible to use VPN Monitor on a remote VPN device. However, this is not entirely practical for two reasons: First, this type of monitoring does not scale as well. Second, in most cases it is sufficient to view the VPN metrics from one end of the tunnel (and not both).

Cisco IDS Host Sensor

What is the management function?

The Cisco IDS Host Sensor (Cisco HIDS) application is a product that complements the network-based IDS management provided in IDS MC and Security Monitor, and gives CiscoWorks VMS a truly comprehensive solution to manage intrusion detection. The basic premise of Cisco HIDS is to protect individual host systems from intrusion detection. The software (agent) sits on the host itself and examines system calls to the OS kernel, comparing these to a database of well-known signatures. Events are reported back to a central Cisco HIDS Console system, which consolidates the information from the agents it is managing. If a signature match is found, Cisco HIDS will prevent the operation and shoot off a real-time notification.

This protection model is proven to mitigate well-known threats such as the NIMDA and Code-Red worms without any user configuration. This means the Cisco HIDS agent software is especially important to use on important network hosts, at the user's discretion. In our reference topology, the Cisco HIDS agent code is installed on all the network management servers that comprise the VMS solution, thus protecting the important network management systems. These servers report IDS events back to the HIDS Console system, which are then forwarded to Security Monitor, provided the integrator software is installed on the HIDS Console. Users are asked to provide the IP address and syslog listening port of Security Monitor during the installation of the integrator.

What devices does it manage?

The Cisco HIDS application does not directly interact with Cisco network devices. It interacts with network hosts with the Cisco HIDS Agent code installed. At present, the following server OS versions are protected:

- Windows NT 4.x Server
- Windows NT Enterprise Server (SP 3 or later)
- Windows 2000 Server
- Windows 2000 Advanced Server
- Solaris 2.6, 2.7, and 2.8

The following Web servers are protected:

- Windows IIS Web Server
- Solaris Apache
- Solaris Netscape Enterprise
- Solaris iPlanet

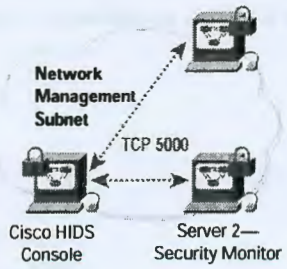
Consult product documentation to verify the current available option of the Cisco HIDS Agent software.

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Which services do I need to enable? (Application protocol requirements)

For Cisco HIDS to work properly, the agents must be able to communicate with the console. This is necessary so that the agents can report IDS events to the console, and just as importantly, the console can push configuration changes out to the agents. This communication is accomplished through a proprietary protocol that travels on TCP port 5000. This port number is actually a configurable option upon install, but TCP port is the default value. Figure 10 illustrates how the Cisco HIDS application is applied to our reference topology.

Figure 10
Cisco HIDS Console and Agents Applied



Cisco Secure Policy Manager

What is the management function?

Cisco Secure Policy Manager (CSPM) is an end-to-end security policy tool. Network administrators use CSPM to define and deploy security policies for their networks. This can be something as simple as what hosts or networks are allowed to access their network, or it can be something much more complex involving encryption, access methods, and other variables. The point is that, using CSPM, network administrators can implement policy management across their mixed network infrastructures.

From the perspective of our reference topology, the role of CSPM is twofold: 1. It manages traffic encryption policy by handling the VPN configuration that allows the user to configure the hub and spoke VPN tunnels between the 7X00 Series Router on the corporate network to the endpoints on the branch sites (both IOS and PIX devices). 2. It allows the user to configure security policies on the PIX Firewall(s) and also the firewall feature set on the IOS enterprise gateway, defining basic firewall policy distribution.

What devices does it manage?

As can be inferred from the previous paragraph, CSPM is able to manage the Cisco IOS routers and PIX Firewalls. The software image version requirements are:

- Cisco IOS Router—12.0(5) or later with the FW-DES feature set
- PIX Firewall—4.2.4 or later with the Data Encryption Standard (DES) feature set

Other versions can be added and managed as well, using the version management utility in CSPM.

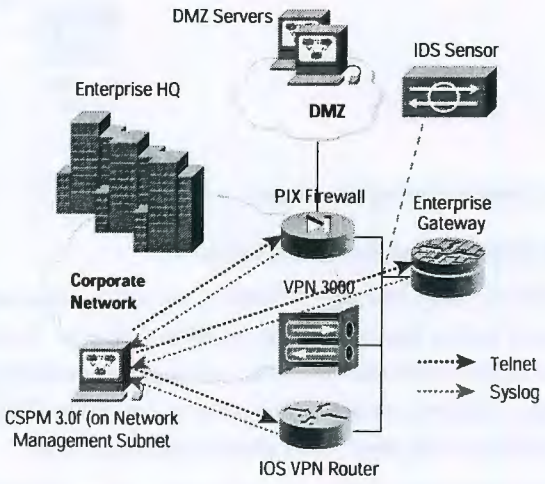
RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 273
Doc 3702

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Which services do I need to enable? (Application protocol requirements)

CSPM requires several protocols in order to function. First, when applying a security policy across the network, CSPM will use Telnet (TCP port 23) to connect to the device(s) and make configuration changes. The second protocol is syslog (UDP port 514). The CSPM has the ability to receive and consolidate syslog messages from the Cisco devices that it is managing. The application keeps an archive of these syslog messages and can use them to generate reports based upon the information they provide. Based on these requirements, the devices must then be configured to support these services. For both Cisco IOS Software and PIX, the telnet service along with a login password must be enabled. These devices also need to be configured to point their syslog messages to the CSPM server. Note that those devices managed by both RME and CSPM will now be sending their syslog messages to two different hosts. Figure 11 illustrates how CSPM is applied in our reference topology.

Figure 11
CSPM Applied



Cisco Systems, Inc.
All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Putting It All Together

Clearly, it is important to distinguish which components to use, determine where to deploy the various components of VMS, and identify what elements of the network infrastructure each piece manages. Table 12 summarizes the information presented in this section along with the associated management protocols that must be enabled in order for the applications to function properly.

Table 12 Summary of CiscoWorks VMS Components Applied

Application	Traffic Flow	Service(s)	TCP/UDP Port Number
CiscoView		SNMP	UDP 161
Inventory Manager		SNMP	UDP 161
Configuration Manager		Telnet TFTP SNMP	TCP 23 UDP 69 UDP 161
Software Image Manager		Telnet TFTP SNMP	TCP 23 UDP 69 UDP 161
Change Audit Services		Syslog	UDP 514
Availability Manager		Telnet SNMP ICMP	TCP 23 UDP 161 N/A
Syslog Analyzer		Syslog	UDP 514

Caveats

When deploying VMS, it is important to realize the specific services required by each individual application, as outlined in the previous section. In certain instances, two different applications may require the same type of access to a particular device (for example, CiscoView and VPN Monitor both use SNMP to retrieve the management information). However, because some of the applications within VMS have a security focus, sharing access to a device can be a potentially contentious situation. This section discusses some of the things that need to be considered should you deviate from the deployment guidelines provided in this document.

Considerations with Network Address Translation

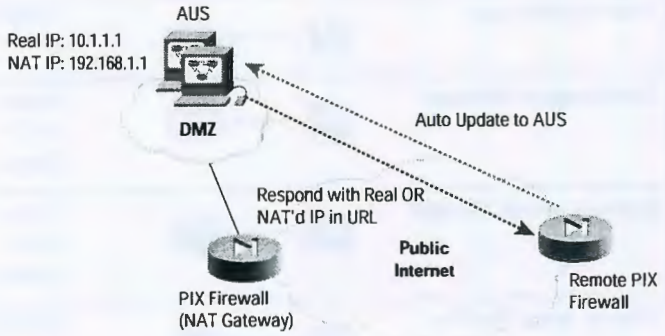
In many topologies, Network Address Translation (NAT) is used. This is an excellent feature for security and address space conservation, but it can create some problems with management tools. This section points out some of the caveats and issues that may occur if CiscoWorks VMS is deployed into a network environment with NAT.

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

NAT and AUS

If the AUS application is used and the server is sitting behind a NAT gateway, pay special attention to the PIX Firewalls you are managing. Consider a remote PIX that contacts the AUS server. It will actually contact the NAT address (not the real address). When the AUS responds with the proper URL to download the updated configuration or software image, it will use the NAT address. Conversely, if the AUS is NOT behind a NAT gateway, you could also configure it to provide it's real address (Figure 12). The bottom line is that you have to decide to use the NAT address or the real address for ALL the PIX Firewalls you are managing—NAT and non-NAT addresses cannot be mixed within a single installation of AUS.

Figure 12
NAT and AUS



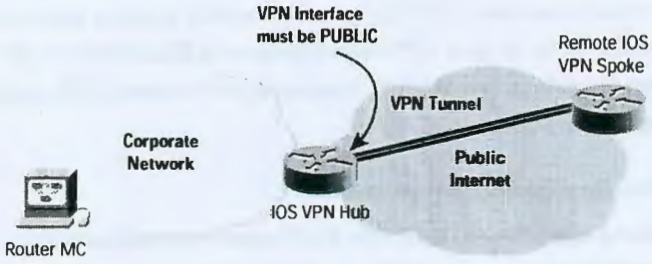
When it is necessary to manage PIX Firewalls (both internal and external), we recommend installing two copies of AUS—one for the external firewalls that will use the NAT address and one for the internal firewalls that will use the real IP address.

NAT and Router MC (Hub Side)

When using Router MC to set up a hub-and-spoke VPN environment, be careful about the hub router VPN interface. Because of the way the product is designed, this interface cannot be behind a NAT gateway. The VPN termination interface must be a publicly addressable IP subnet. If it was behind a NAT gateway, then from the perspective of the peer it would be necessary to assign it the NAT'd address. The Router MC application, however, only allows you to assign by interface and not IP address—so the peer statements will be incorrect. Refer to Figure 13 to see how the VPN topology must be built for compatibility with Router MC.

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Figure 13
NAT and Router MC



NAT and Router MC (Spoke Side)

There is also a deployment caveat with NAT and VPN spoke devices. Router MC needs to manage the spoke devices (VPN peers) with their real IP address. The current version of Router MC does not support the situation where the spoke is behind a NAT gateway.

Managing a Device with CSPM and a MC

With the number of different applications within the VMS bundle, it is possible to have some functional overlap between tools. For example, if you want to change a PIX Firewall access rule, you can use either CSPM or PIX MC. This section describes some caveats and issues that exist when using overlapping applications.

CSPM and PIX MC

The first area of functional overlap is between CSPM and PIX MC. Both applications can be used to manage firewall device settings and access rules. So what happens when somebody tries to use both tools? Will this configuration even work?

The short answer is that this will NOT work. What will happen is when a configuration change is made using one of the applications, it will overwrite that change with the other application. This can be avoided by doing a re-import of the existing configuration before every deployment, but this is not practical. Also, you would need to make sure that you had an access rule set up to allow SSL traffic to the PIX. The recommendation here is to either use CSPM or PIX MC to manage a device, but not both.

CSPM and Router MC

The second area of functional overlap involves CSPM and Router MC. Both applications can be used to configure site-to-site VPNs on IOS VPN routers. CSPM can also be used to configure the firewall features set on those routers. Here, the consideration when each application would be used and how the two can work together.

As with PIX MC, avoid managing a single router's VPN settings with multiple applications. Even though Router MC does not push out a whole configuration file to the device (it sends out individual commands), it is possible that something will get overwritten in the original configuration. Looking at the reverse, it is definitely a problem if CSPM tries to configure a router that has already been configured with Router MC. The device will need to be re-imported into the CSPM database every time, just to make sure your configuration is current. This is also not a very practical solution. Either use CSPM or Router MC to manage a device, but not both.

ECT 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 275
Nº Doc 3702

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

When To Use What

Based on some of the overlap in product functionality, it can be confusing to decide which product should be used in what situations. CSPM is currently the only product that can help manage a mixed environment, so you need to use CSPM to set up a VPN tunnel between a PIX device and an IOS device. Otherwise, since they are designed for better scalability, it is ALWAYS recommended to use the MC applications instead, based on the network environment and management needs.

Multiple Syslog Daemons

Several applications within the VMS bundle can receive syslog messages from multiple sources. Now, with Cisco modified OS support, all of these applications can also be installed on a single server. In this case, it is necessary to determine how to make all of these syslog daemons compatible.

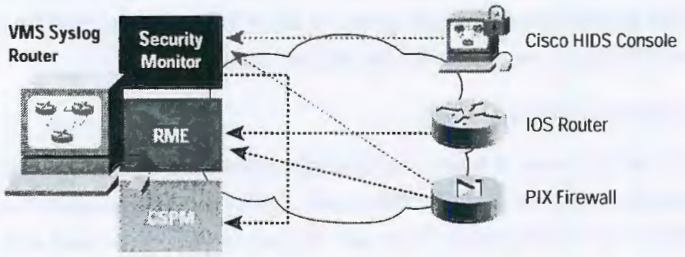
First, look at which applications can receive syslog messages, and from which devices (Table 13):

Table 13 Summary of Syslog Server Applications in VMS

CiscoWorks VMS Module	Syslog Source
RME	IOS, PIX, VPN3K
CSPM	IOS, PIX
Security Monitor	IOS, PIX, Host IDS Console

By default, all of these application listen on UDP port 514. This is not a problem if these applications are split across different servers—simply send syslog messages to multiple sources. However, what happens when all of these applications are installed on a single system AND the customer wants to try and take advantage of all three syslog daemons? (Figure 14.)

Figure 14
Syslog Consolidation in VMS



There are two ways that Security Monitor can alleviate this problem. The first is to configure what port number it should listen for syslog messages. By default it is UDP 514, but it can be changed. Also, Security Monitor can be set up to forward the syslog messages to another port on that same system. This is important because CSPM can change the port numbers they listen to for syslog messages. The other important factor is that PIX Firewalls can send syslog messages to the same host, but different port numbers. In this situation, here is the solution to maximize the syslog functionality:

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

16.359
2.

- From IOS, send syslog to RME at UDP 514
- From PIX, send syslog to RME at UDP 514
- From PIX, send syslog to Security Monitor at port x
- From Cisco HIDS Console, send syslog to Security Monitor at port x
- From Security Monitor, forward syslog to CSPM at port y

The only caveat here is that CSPM will not be able to receive IOS syslog messages.

Ideally, at least two servers would be used in this scenario to take advantage of all three tools. The first box would run Security Monitor and CSPM, and the second system would run RME. This way, no syslog functionality within VMS is lost.

Running the Cisco HIDS Software with other Applications

A major component of the CiscoWorks VMS bundle is the ability to manage IDS on a host level—or rather, to provide intrusion protection to critical servers. The management servers for VMS should definitely be considered critical and as such, we also recommend installing the Cisco HIDS agent software on these systems.

When installing another CiscoWorks VMS module on a server with Cisco HIDS, make sure the agent is in "Full Warning" mode during the install process. Running in "Full Protect" mode, it is possible that the normal operations of the software may trigger a HIDS event and, as such, may actually be prevented. In this case, a false positive would have an adverse effect on your management system by not allowing it to perform a legitimate task. In most cases, you should first install the Cisco HIDS agent and run it in "Full Warning" mode. Do this for the first several weeks of regular use to develop a baseline. This allows the user to first see events—but they will NOT be prevented. Based on this activity you can then identify any false positives and create appropriate exceptions. When the exceptions are configured, then you can change the status of your management server agents to "Full Protect" to ensure that the server is properly shielded.

Even using this deployment method, note that even in "Full Protect" mode out of the box, the HIDS agent software does not prevent any normal operations by any of the applications in the VMS bundle.

Compatibility Issues with IDS Event Viewer

Cisco IDS Event Viewer (IEV) is a Java-based application that lets users view and manage alarms from up to three IDS sensors. At the time of this writing, when IEV is installed on a PC, that PC can NOT be used as a client for the CiscoWorks VMS Web-based modules. While this compatibility limitation will be addressed in future releases, the current workarounds for this limitation are:

- Uninstall IEV from that client system
- Use a different PC as your client system

This will not be an issue for most users. Those using IDS MC and Security Monitor will most likely not need IEV as well.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 276
3702
Doc

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Out-of-Band Management

In many networks, it is desirable to design a separate management subnet. This is commonly referred to as out-of-band management and describes a situation where the management stations reside on an isolated subnet separate from the network elements they are trying to manage. This is attractive to many network administrators due to the inherent higher level of security and clear functional division within their network.

As is the case with all network management tools, however, CiscoWorks VMS requires network access to the devices it is trying to manage. So when making this decision, consider that, while it might be nice to have a completely isolated management subnet, it will do no good unless there is IP connectivity to the rest of the network. This must be carefully planned out when deploying VMS in such an environment.

Conclusions

Evolution of VPNs and Security

In the recent past, we have seen huge growth in the need for network security, specifically in two areas: perimeter network security and secured transactions over public infrastructure. This growth has made it necessary to evolve how a management scheme handles this environment, which has resulted in the introduction of the CiscoWorks VPN/Security Management Solution (VMS).

The CiscoWorks VMS provides customers with applications to assist in the management of their security-specific hardware such as the Cisco VPN 3000 Concentrator series, Cisco IOS VPN routers, Cisco PIX Firewalls, and Cisco IDS products. VMS addresses the challenges of VPN deployment, monitoring, development of perimeter security policies, and management of intrusion detection. This paper provides some basic deployment guidelines for VMS by outlining the different components of the solution, what they do, and how they can be configured to work together. After reading this document, the user should clearly understand how VMS fits into the network management scheme and the values it adds.

As with any dynamic environment, the needs and technologies around network security are constantly evolving. From a network management perspective, CiscoWorks VMS will continue to evolve to provide a comprehensive set of tools to manage the unique aspects of this environment.

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 317 7777
Fax: +65 317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the
Cisco Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland
Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland
Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

All contents are Copyright © 1992–2002, Cisco Systems, Inc. All rights reserved. Cisco, Cisco IOS, Cisco Systems, the Cisco Systems logo, and Cisco Unity are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0208R)

202881/ETMG 10/02

46-597
L

Segurança Tipo 2 doc1

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 277
Doc. 3702

Cisco Systems

Data Sheet

Cisco PIX **525** Security Appliance

The Cisco PIX® 525 Security Appliance delivers enterprise-class security for medium-to-large enterprise networks in a reliable, purpose-built appliance. Its modular two-rack unit (2RU) design supports up to eight 10/100 Fast Ethernet interfaces or three Gigabit Ethernet interfaces, making it an ideal choice for businesses requiring a resilient, high performance, Gigabit Ethernet-ready solution that provides solid investment protection. Part of the world-leading Cisco PIX Security Appliance Series, the Cisco PIX 525 Security Appliance provides a wide range of rich integrated security services, hardware VPN acceleration capabilities, and powerful remote management capabilities in a cost-effective, highly-resilient solution.

Enterprise-Class Security for Medium-to-Large Enterprise Networks

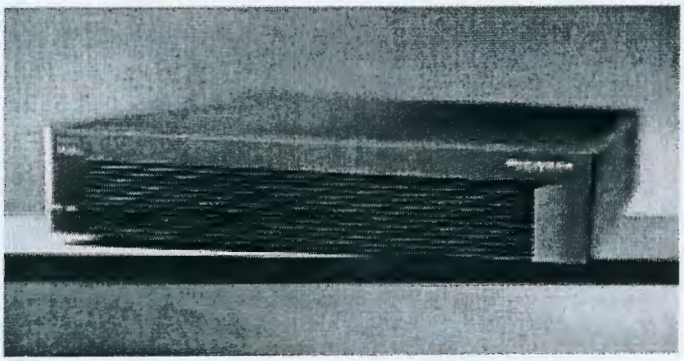
The Cisco PIX 525 Security Appliance delivers a multilayered defense for large enterprise networks through rich, integrated security services including stateful inspection firewalling, protocol and application inspection, virtual private networking (VPN) in-line intrusion protection and rich multimedia and voice security in a single device. The state-of-the-art Cisco Adaptive Security Algorithm (ASA) provides rich stateful inspection firewall services, tracking the state of all authorized network communications and preventing unauthorized network access.

Enterprise networks benefit from an additional layer of security via intelligent, "application-aware" security services that examine packet streams at Layers 4–7, using inspection engines specialized for many of today's popular applications. Administrators can also easily create custom security policies for firewall traffic by using the flexible access control methods and the more than 100 predefined applications, services, and protocols that Cisco PIX Security Appliances provide.

Market-Leading Voice-over-IP Security Services Protect Next-Generation Converged Networks

Cisco PIX Security Appliances provide market-leading protection for a wide range of voice-over-IP (VoIP) and multimedia standards, allowing businesses to securely take advantage of the many benefits that converged data, voice, and video networks deliver. By combining VPN with the rich stateful inspection firewall services that Cisco PIX Security Appliances provide for these converged networking standards, businesses

Figure 1
Cisco PIX 525 Security Appliance



Cisco Systems, Inc.
All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RDS n° 03/2005 - CN
File N° 278
N° - Doc 3702

can securely extend voice and multimedia services to home office and remote office environments for additional cost savings, improved productivity, and competitive advantage.

Flexible VPN Services Extend Networks Economically to Remote Networks and Mobile Users

Businesses can securely extend their networks across low-cost Internet connections to mobile users, business partners, and remote offices worldwide using the full-featured VPN capabilities provided by the Cisco PIX 525 Security Appliance. Solutions range from standards-based site-to-site VPN leveraging the Internet Key Exchange (IKE) and IP security (IPsec) VPN standards, to the innovative Cisco Easy VPN capabilities found in Cisco PIX Security Appliances and other Cisco security solutions—such as Cisco IOS® routers and Cisco VPN 3000 Series Concentrators. Easy VPN delivers a uniquely scalable, cost-effective, and easy-to-manage remote-access VPN architecture that eliminates the operational costs associated with maintaining remote-device configurations typically required by traditional VPN solutions. Cisco PIX Security Appliances encrypt data using 56-bit Data Encryption Standard (DES), 168-bit Triple DES (3DES), or up to 256-bit Advanced Encryption Standard (AES) encryption. Certain Cisco PIX 525 Security Appliance models have integrated hardware VPN acceleration capabilities, delivering highly scalable, high performance VPN services.

Integrated Intrusion Protection Guards Against Popular Internet Threats

The integrated in-line intrusion-protection capabilities of the Cisco PIX 525 Security Appliance can protect enterprise networks from many popular forms of attacks, including Denial-of-Service (DoS) attacks and malformed packet attacks. Using a wealth of advanced intrusion-protection features, including DNSGuard, FloodGuard, FragGuard, MailGuard, IPVerify and TCP intercept, in addition to looking for more than 55 different attack "signatures," Cisco PIX Security Appliances keep a vigilant watch for attacks, can optionally block them, and can notify administrators about them in real time.

Award-Winning Resiliency Provides Maximum Business Uptime

Select models of Cisco PIX 525 Security Appliances provide stateful failover capabilities that ensure resilient network protection for enterprise network environments. Employing a cost-effective, active-standby, high-availability architecture, Cisco PIX Security Appliances that are configured as a failover pair continuously synchronize their connection state and device configuration data. Synchronization can take place over a high-speed LAN connection, providing another layer of protection through the ability to geographically separate the failover pair. In the event of a system or network failure, network sessions are automatically transitioned between appliances, with complete transparency to users.

Robust Remote-Management Solutions Lower Total Cost of Ownership

The Cisco PIX 525 Security Appliance is a reliable, easy-to-maintain platform that provides a wide variety of methods for configuring, monitoring, and troubleshooting. Management solutions range from centralized, policy-based management tools to integrated, Web-based management to support for remote monitoring protocols such as Simple Network Management Protocol (SNMP) and syslog.

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 279
Doc 3702

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Administrators can easily manage large numbers of remote Cisco PIX Security Appliances using CiscoWorks VPN/Security Management Solution (VMS). This suite consists of numerous modules including Management Center for Firewalls, Auto Update Server Software and Security Monitor. This powerful combination provides a highly scalable, next-generation, three-tier management solution that includes the following features:

- Comprehensive configuration and software image management
- Device hierarchy with "Smart Rules"-based configuration inheritance
- Customizable administrative roles and access privileges
- Comprehensive enterprise change management and auditing
- "Touchless" software image management for remote Cisco PIX Security Appliances
- Support for dynamically addressed appliances

Additional integrated event management and inventory solutions are also available as part of the CiscoWorks VMS network management suite.

The integrated Cisco PIX Device Manager provides an intuitive, Web-based management interface for remotely configuring, monitoring, and troubleshooting a Cisco PIX 525 Security Appliance—without requiring any software (other than a standard Web browser) to be installed on an administrator's computer. A setup wizard is provided for easy installation into any network environment.

Alternatively, through methods including Telnet and Secure Shell (SSH), or out of band through a console port, administrators can remotely configure, monitor, and troubleshoot Cisco PIX Security Appliances using a command-line interface (CLI).

Table 1 Key Product Features and Benefits

Key Features	Benefit
Enterprise-Class Security	
True security appliance	• Uses a proprietary, hardened operating system that eliminates security risks associated with general purpose operating systems • Cisco quality and no moving parts provide a highly reliable security platform
Stateful inspection firewall	• Provides perimeter network security to prevent unauthorized network access • Uses state-of-the-art Cisco ASA for robust stateful inspection firewall services • Provides flexible access-control capabilities for over 100 predefined applications, services and protocols, with the ability to define custom applications and services • Includes numerous application-aware inspection engines that secure advanced networking protocols such as H.323 Version 4, Session Initiation Protocol (SIP), Cisco Skinny Client Control Protocol (SCCP), Real-Time Streaming Protocol (RTSP), Internet Locator Service (ILS), and more • Includes content filtering for Java and ActiveX applets
Easy VPN Server	• Provides remote access VPN concentrator services for a wide variety of Cisco software or hardware-based VPN clients • Pushes VPN policy dynamically to Cisco Easy VPN Remote-enabled solutions upon connection, ensuring the latest corporate security policies are enforced • Extends VPN reach into environments using Network Address Translation (NAT) or Port Address Translation (PAT), via support of Internet Engineering Task Force (IETF) UDP-based draft standard for NAT traversal

CPMI - CORREIOS
280
Doc 3702

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

16.393

Table 1 Key Product Features and Benefits

Key Features	Benefit
Site-to-site VPN	• Supports IKE and IPsec VPN standards • Ensures data privacy/integrity and strong authentication to remote networks and remote users over the Internet • Supports 56-bit DES, 168-bit 3DES and up to 256-bit AES data encryption to ensure data privacy
Intrusion protection	• Provides protection from over 55 different types of popular network-based attacks ranging from malformed packet attacks to DoS attacks • Integrates with Cisco Network Intrusion Detection System (IDS) sensors for the ability to dynamically block/shun hostile network nodes via the firewall
AAA support	• Integrates with popular authentication, authorization, and accounting services via TACACS+ and RADIUS support • Provides tight integration with Cisco Secure Access Control Server (ACS)
X.509 certificate and CRL support	• Supports SCEP-based enrollment with leading X.509 solutions from Baltimore, Entrust, Microsoft, and VeriSign
Integration with leading third-party solutions	• Supports the broad range of Cisco AVVID (Architecture for Voice, Video and Integrated Data) partner solutions that provide URL filtering, content filtering, virus protection, scalable remote management, and more
Robust Network Services/Integration	
Virtual LAN (VLAN)-based virtual interfaces	• Provides increased flexibility when defining security policies and eases overall integration into switched network environments by supporting the creation of logical interfaces based on IEEE 802.1q VLAN tags, and the creation of security policies based on these virtual interfaces • Supports multiple virtual interfaces on a single physical interface through VLAN trunking • Supports multiple VLAN trunks per Cisco PIX Security Appliance • Supports up to 10 VLANs on Cisco PIX 525 Security Appliances
Open Shortest Path First (OSPF) dynamic routing	• Provides comprehensive OSPF dynamic routing services using technology based on world-renowned Cisco IOS Software • Offers improved network reliability through fast route convergence and secure, efficient route distribution • Delivers a secure routing solution in environments using NAT through tight integration with Cisco PIX Security Appliance NAT services • Supports MD5-based OSPF authentication, in addition to plaintext OSPF authentication, to prevent route spoofing and various routing-based DoS attacks • Provides route redistribution between OSPF processes, including OSPF, static, and connected routes • Supports load balancing across equal-cost multipath routes
DHCP server	• Provides DHCP Server services one or more interfaces for devices to obtain IP addresses dynamically • Includes extensions for support of Cisco IP Phones and Cisco SoftPhone IP telephony solutions
DHCP relay	• Forwards DHCP requests from internal devices to an administrator-specified DHCP server, enabling centralized distribution, tracking, and maintenance of IP addresses
NAT/PAT support	• Provides rich dynamic/static NAT and PAT capabilities

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

CPMI CORREIOS
281
3702

16 392

Table 1 Key Product Features and Benefits

Key Features	Benefit
Rich Remote Management Options	
CiscoWorks VPN/ Security Management Solution (CiscoWorks VMS)	• Comprehensive management suite for large scale deployments • Integrates policy management, software maintenance, and security monitoring
PIX Device Manager (PDM)	• Intuitive, Web-based GUI enables simple, secure remote management of Cisco PIX Security Appliances • Provides wide range of informative, real-time, and historical reports which give critical insight into usage trends, performance baselines, and security events
Auto Update	• Provides "touchless" secure remote management of Cisco PIX Security Appliance configuration and software images via a unique push/pull management model • Next-generation secure XML/HTTPS management interface can be leveraged by Cisco and third-party management applications for remote Cisco PIX Security Appliance configuration management, inventory, software image management/deployment and monitoring • Integrates seamlessly with CiscoWorks Management Center for Firewalls and Auto Update Server for robust, scalable remote management of up to 1000 Cisco PIX Security Appliances (per management server)
Cisco PIX CLI	• Allows customers to use existing PIX CLI knowledge for easy installation and management without additional training • Accessible through variety of methods including console port, Telnet, and SSH
Command-level authorization	• Enables businesses to create up to 16 customizable administrative roles/profiles for accessing Cisco PIX Security Appliances (for example, monitoring only, read-only access to configuration, VPN administrator, firewall/NAT administrator, and so on) • Leverages either the internal administrator database or outside sources via TACACS+, such as Cisco Secure ACS
SNMP and syslog support	• Provide remote monitoring and logging capabilities, with integration into Cisco and third-party management applications
Flexible Expansion Capabilities	
Fast Ethernet and Gigabit Ethernet expansion options	• Supports easy installation of additional network interfaces via 3 PCI expansion slots • Supports expansion cards including single-port Fast Ethernet card, 4-port Fast Ethernet card, and single-port Gigabit Ethernet card
Hardware VPN acceleration options	• Delivers high speed VPN services via support of VPN Accelerator Card (VAC) and VPN Accelerator Card+ (VAC+)

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 282
Doc 3702

License Options

The Cisco PIX 525 Security Appliance is available in three primary models that provide different levels of interface density, failover capabilities, and VPN throughput.

Restricted Software License

The Cisco PIX 525 "Restricted" (PIX 525-R) model provides an excellent value for organizations looking for robust Cisco PIX Security Appliance services with Gigabit Ethernet support, medium interface density, and moderate VPN throughput requirements. It includes 128 MB of RAM and support for up to six 10/100 Fast Ethernet or three Gigabit Ethernet interfaces.

Unrestricted Software License

The PIX 525 "Unrestricted" (PIX 525-UR) model extends the capabilities of the family with support for stateful failover, additional LAN interfaces, and increased VPN throughput via integrated hardware-based VPN acceleration. It includes an integrated VAC or VAC+ hardware VPN accelerator, 256 MB of RAM, and support for up to eight 10/100 Fast Ethernet or three Gigabit Ethernet interfaces. The Cisco PIX 525-UR also adds the ability to share state information with a hot-standby Cisco PIX Security Appliance for resilient network protection.

Failover Software License

The Cisco PIX 525 "Failover" (PIX 525-FO) model is designed for use in conjunction with a PIX 525-UR, providing a cost-effective, high-availability solution. It operates in hot-standby mode acting as a complete redundant system that maintains current session state information. With the same hardware configuration as the Cisco PIX 525-UR, it delivers the ultimate in high availability for a fraction of the price.

Performance Summary

Cleartext throughput: 330 Mbps

Concurrent connections: 280,000

168-bit 3DES IPsec VPN throughput: Up to 155 Mbps with VAC+ or 72 Mbps with VAC

128-bit AES IPsec VPN throughput: Up to 165 Mbps with VAC+

256-bit AES IPsec VPN throughput: Up to 170 Mbps with VAC+

Simultaneous VPN tunnels: 2000

Technical Specifications

Processor: 600-MHz Intel Pentium III Processor

Random access memory: 128 MB or 256 MB of SDRAM

Flash memory: 16 MB

Cache: 256 KB level 2 at 600 MHz

System bus: Single 32-bit, 33-MHz PCI

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 283
Doc 3702

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Environmental Operating Ranges

Operating

Temperature: –25° to 104°F (–5° to 40°C)

Relative Humidity: 5% to 95%, noncondensing

Altitude: 0 to 6500 ft (2000 m)

Shock: 1.14 m/sec (45 in./sec) 1/2 sine input

Vibration: 0.41 Grms2 (3–500 Hz) random input

Acoustic Noise: 45 dBa maximum

Nonoperating

Temperature: –13° to 158°F (–25° to 70°C)

Relative Humidity: 5% to 95%, noncondensing

Altitude: 0 to 15,000 ft (4570 m)

Shock: 30G

Vibration: 0.41 Grms2 (3–500 Hz) random input

Power

Input (per power supply)

Range Line Voltage: 100V to 240V AC or 48V DC to 60V DC

Nominal Line Voltage: 100V to 240V AC or 48V DC to 60V DC

Current: 5–2.5 Amps AC or 12 Amps DC

Frequency: 50 to 60 Hz, single phase

Output

Steady State: 50W

Maximum Peak: 65W

Maximum Heat Dissipation: 410 BTU/hr, full power usage (65W)

Physical Specifications

Dimensions and Weight Specifications

Form factor: 2 RU, standard 19-in. rack mountable

Dimensions (H x W x D): 3.5 x 17.5 x 18.25 in. (8.89 x 44.45 x 46.36 cm)

Weight (one power supply): 32 lb (14.5 kg)

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 284
Doc 3702

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

16.359

Expansion

Three 32-bit/33-MHz PCI slots

Two 168-pin DIMM RAM slots, supporting up to 256 MB memory maximum

Interfaces

Console Port: RS-232 (RJ-45) 9600 baud

Failover Port: RS-232 (DB-15) 115 Kbps (Cisco specified cable required)

Two integrated 10/100 Fast Ethernet ports, auto-negotiate (half/full duplex), RJ-45

Regulatory and Standards Compliance

Safety

UL 1950, CSA C22.2 No. 950, EN 60950 IEC 60950, AS/NZS3260, TS001

Electro Magnetic Compatibility (EMC)

CE marking, FCC Part 15 Class A, AS/NZS 3548 Class A, VCCI Class A, EN55022 Class A, CISPR22 Class A, EN61000-3-2, EN61000-3-3

Product Ordering Information

PIX-525	PIX 525 chassis only
PIX-525-DC	PIX 525 DC chassis only
PIX-525-R-BUN	PIX 525 restricted bundle (chassis, restricted software, 2 10/100 ports, 128 MB RAM)
PIX-525-UR-BUN	PIX 525 unrestricted bundle (chassis, unrestricted software, 2 10/100 ports, 256 MB RAM, VAC or VAC+)
PIX-525-UR-GE-BUN	PIX 525 unrestricted 2 GE + 2 FE bundle (chassis, unrestricted software, 2 Gigabit Ethernet + 2 10/100 ports, 256 MB RAM, VAC or VAC+)
PIX-525-FO-BUN	PIX 525 failover bundle (chassis, failover software, 2 10/100 ports, 256 MB RAM, VAC or VAC+)
PIX-525-FO-GE-BUN	PIX 525 failover 2 GE + 2 FE bundle (chassis, failover software, 2 Gigabit Ethernet + 2 10/100 ports, VAC or VAC+)
PIX-525-HW=	PIX 525 rack-mount kit, console cable and failover serial cable
PIX-FO=	PIX failover serial cable
PIX-4FE	4-port 10/100 Fast Ethernet PCI expansion card
PIX-1FE	Single-port 10/100 Fast Ethernet PCI expansion card
PIX-1GE-66	Single-port Gigabit Ethernet 64-bit/66-MHz PCI expansion card, Multimode (SX) SC connector
PIX-VPN-ACCEL	3DES IPsec hardware VAC
PIX-VAC-PLUS	3DES/AES IPsec hardware VAC+

ROS nº 03/2005 - CN
DPME - CORREIOS
Fls. Nº 285
Doc 3702

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

PIX-VPN-3DES	168-bit 3DES and up to 256-bit AES encryption software license
PIX-VPN-3DES=	168-bit 3DES and up to 256-bit AES encryption software license
PIX-VPN-DES	56-bit DES encryption software license
PIX-VPN-DES=	56-bit DES encryption software license

Support Services

Support services are available from Cisco and Cisco partners. Cisco SMARTnet service augments customer support resources, and provides anywhere, anytime access to technical resources (both online and by telephone), the ability to download updated system software, and hardware advance replacement.

Support Ordering Information

CON-SNT-PIX525	SMARTnet 8x5xNBD service for PIX 525 chassis only
CON-SNT-PIX525R	SMARTnet 8x5xNBD service for PIX 525-R bundle
CON-SNT-PIX525UR	SMARTnet 8x5xNBD service for PIX 525-UR bundle
CON-SNT-PIX525FO	SMARTnet 8x5xNBD service for PIX 525-FO bundle
CON-SNTE-PIX525	SMARTnet 8x5x4 service for PIX 525 chassis only
CON-SNTE-PIX525R	SMARTnet 8x5x4 service for PIX 525-R bundle
CON-SNTE-PIX525UR	SMARTnet 8x5x4 service for PIX 525-UR bundle
CON-SNTE-PIX525FO	SMARTnet 8x5x4 service for PIX 525-FO bundle
CON-SNTP-PIX525	SMARTnet 24x7x4 service for PIX 525 chassis only
CON-SNTP-PIX525R	SMARTnet 24x7x4 service for PIX 525-R bundle
CON-SNTP-PIX525UR	SMARTnet 24x7x4 service for PIX 525-UR bundle
CON-SNTP-PIX525FO	SMARTnet 24x7x4 service for PIX 525-FO bundle
CON-S2P-PIX525R	SMARTnet 24x7x2 service for PIX 525-R bundle
CON-S2P-PIX525UR	SMARTnet 24x7x2 service for PIX 525-UR bundle
CON-S2P-PIX525FO	SMARTnet 24x7x2 service for PIX 525-FO bundle
CON-OS-PIX525	SMARTnet On-Site 8x5xNBD service for PIX 525 chassis only
CON-OS-PIX525R	SMARTnet On-Site 8x5xNBD service for PIX 525-R bundle
CON-OS-PIX525UR	SMARTnet On-Site 8x5xNBD service for PIX 525-UR bundle
CON-OS-PIX525FO	SMARTnet On-Site 8x5xNBD service for PIX 525-FO bundle
CON-OSE-PIX525	SMARTnet On-Site 8x5x4 service for PIX 525 chassis only
CON-OSE-PIX525R	SMARTnet On-Site 8x5x4 service for PIX 525-R bundle
CON-OSE-PIX525UR	SMARTnet On-Site 8x5x4 service for PIX 525-UR bundle

ECT 03/2005
CPMI - CORREIOS
Fls Nº 286
Doc 3702

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

CON-OSE-PIX525FO	SMARTnet On-Site 8x5x4 service for PIX 525-FO bundle
CON-OSP-PIX525	SMARTnet On-Site 24x7x4 service for PIX 525 chassis only
CON-OSP-PIX525R	SMARTnet On-Site 24x7x4 service for PIX 525-R bundle
CON-OSP-PIX525UR	SMARTnet On-Site 24x7x4 service for PIX 525-UR bundle
CON-OSP-PIX525FO	SMARTnet On-Site 24x7x4 service for PIX 525-FO bundle

16-337

Additional Information

For more information, please visit the following links:

Cisco PIX Security Appliance Series:

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

Cisco PIX Device Manager:

http://www.cisco.com/warp/public/cc/pd/fw/sqfw500/prodlit/pixd3_ds.pdf

Cisco Secure ACS:

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

CiscoWorks VMS, Management Center for Firewalls, Auto Update Server Software and Security Monitor:

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

SAFE Blueprint from Cisco:

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

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the **Cisco Web site at www.cisco.com/go/offices**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. CCIP, CCSP, the Cisco Arrow logo, the Cisco *Powered* Network mark, Cisco Unity, Follow Me Browsing, FormShare, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, Fast Step, GigaStack, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, MGX, MICA, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, ScriptShare, SlideCast, SMARTnet, StrataView Plus, Stratm, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0304R)

RD/LW3946 04/03

CPMI – CORREIOS
Fls. Nº 287
Doc 3702

16.386
C

Segurança Tipo 2 doc 2

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 288
Nº Doc 3702

Cisco Systems

Data Sheet

Cisco **PIX** Firewall Version 6.2

The world-leading Cisco PIX® Firewall Series of purpose-built security appliances provides robust, enterprise-class security services, including stateful inspection firewalling, virtual private networking (VPN), intrusion protection, and much more—in cost-effective, easy-to-deploy solutions. Ranging from compact, plug-and-play desktop firewalls for small/home offices to carrier-class gigabit firewalls for the most demanding enterprise and service-provider environments, Cisco PIX Firewalls provide robust security, performance, and reliability for network environments of all sizes.

Advanced Firewall Technologies Provide Enterprise-Class Network Security

Cisco PIX Firewalls deliver a broad range of advanced firewall services that protect enterprise networks from the threats lurking on the Internet and in today's network environments. The state-of-the-art Cisco Adaptive Security Algorithm (ASA) provides rich stateful inspection firewall services, tracking the state of all authorized network communications and preventing unauthorized network access. Cisco PIX Firewalls deliver an additional layer of security through intelligent, "application-aware" security services that examine packet streams at Layers 4 through 7, using inspection engines specialized for many of today's popular applications. Administrators can easily create custom security policies that will be enforced on network traffic traversing the firewall by leveraging more than 100 pre-defined applications, services, and protocols within Cisco PIX Firewalls, and the flexible access control capabilities that Cisco PIX Firewalls provide. Access to network resources can also be strongly authenticated via the Cisco PIX Firewall's seamless integration with enterprise databases, either directly using TACACS+/RADIUS or indirectly via Cisco Secure Access Control Server (ACS). In addition to these services, Cisco PIX Firewalls provide extensive logging, URL filtering, content filtering, and more in concert with Cisco AVVID (Architecture for Voice, Video and Integrated Data) partner solutions.

Market-Leading Voice-over-IP Security Services Protect Next-Generation Converged Networks

Cisco PIX Firewalls continue to provide market-leading protection for numerous voice-over-IP (VoIP) standards and other multimedia standards, including H.323, Session Initiation Protocol (SIP), Skinny, Real-Time Transport Protocol (RTP), Real-Time Streaming Protocol (RTSP), and Real-Time Transport Control Protocol (RTCP). This allows businesses to securely take advantage of the many benefits that converged data and voice networks provide, such as significant total cost of ownership (TCO) savings and the competitive advantages and improved productivity gained through the power of fully integrated voice, video, and data networks. By combining VPN with the rich

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 289
3702
Doc

stateful inspection firewall services that Cisco PIX Firewalls provide for these converged networking standards, businesses can easily extend voice and multimedia services to remote/satellite offices for additional bandwidth and cost savings.

Site-to-Site VPNs Extend Networks Economically to Remote Sites and Business Partners

Using the standards-based site-to-site VPN capabilities within Cisco PIX Firewalls, businesses can securely extend their network across low-cost Internet connections to business partners and remote/satellite offices worldwide. Built upon the Internet Key Exchange (IKE) and IP Security (IPSec) VPN standards, Cisco PIX Firewalls encrypt data using 56-bit Data Encryption Standard (DES) or advanced 168-bit Triple DES (3DES) encryption, ensuring that malicious individuals cannot see sensitive business data as it safely travels across the Internet. Cisco PIX Firewalls can also participate in X.509-based Public Key Infrastructures (PKI) and provide easy, automated certificate enrollment by taking advantage of the Simplified Certificate Enrollment Protocol (SCEP)—another Internet standard Cisco helped to pioneer. Certain Cisco PIX Firewall models also provide integrated hardware VPN acceleration, providing up to 100 Mbps of 3DES throughput and support for up to 2000 IKE security associations.

Easy VPN Enables Highly Scalable, Easy-to-Manage VPN Deployments

The innovative Easy VPN capabilities found in Cisco PIX Firewalls and other Cisco solutions—such as Cisco IOS® Software-based routers and Cisco VPN 3000 Series Concentrators—deliver a uniquely scalable, cost-effective, and easy-to-manage remote-access VPN architecture. Built upon the foundation of dynamic policy distribution and effortless provisioning, Easy VPN eliminates the operational costs associated with maintaining remote-device configurations typically required by traditional VPN solutions. Easy VPN enables Cisco customers to enjoy the numerous benefits that VPNs provide—increased employee productivity by taking advantage of high-speed broadband connectivity, and significantly reduced operational costs by eliminating expenses associated with legacy dialup architectures—without the problems commonly found with other remote-access VPN solutions.

Cisco PIX Firewalls provide robust, remote-access VPN concentrator services that enable enterprises to securely extend their network to traveling employees, teleworkers, and remote offices for "anytime, anywhere access" to vital corporate network resources. Acting as an Easy VPN Server, Cisco PIX Firewalls support the wide range of Cisco software- and hardware-based Easy VPN Remote products. By dynamically pushing VPN security policies to Easy VPN-enabled users as they connect, Cisco PIX Firewalls ensure that the latest VPN security policy is consistently enforced for all remote-access users.

Certain models of Cisco PIX Firewalls can also act as "hardware VPN clients" using the new Easy VPN Remote features in Cisco PIX Firewall OS, transparently providing secure access to a corporate network for all devices protected by a Cisco PIX Firewall in a remote network. This dramatically simplifies the initial deployment and ongoing management of VPNs deployed to remote offices and teleworker environments by eliminating the need to install and maintain VPN client software on the individual devices protected by a remote Cisco PIX Firewall. Advanced client-side resiliency features ensure maximum VPN uptime by providing automatic failover to backup Easy VPN Servers in the event of a network or service failure.

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 290
Nº Doc 3702

Integrated Intrusion Protection Guards from Popular Internet Threats

The integrated intrusion-protection capabilities in Cisco PIX Firewalls protect today's networks from many popu forms of attacks, including Denial-of-Service (DoS) attacks and malformed packet attacks. Using a wealth of advanced intrusion-protection features, including DNSGuard, FloodGuard, FragGuard, MailGuard, and TCP intercept, in addition to looking for more than 55 different attack "signatures," Cisco PIX Firewalls keep a vigila watch for attacks, can optionally block them, and can notify administrators about them in real time. Additionall Cisco PIX Firewalls support virtual packet reassembly, searching for attacks that are hidden over a series of fragmented packets. Strong integration with Cisco Intrusion Detection Systems (IDS) sensors enables Cisco PIX Firewalls to automatically shun (block) network nodes identified as being hostile by Cisco IDS sensors.

Enterprise-Class Resiliency Provides Maximum Business Uptime

Cisco PIX Firewalls provide award-winning stateful failover capabilities (on select models) that ensure resilient network protection for enterprise network environments. Employing a cost-effective, active-standby high-availabilit architecture, Cisco PIX Firewalls configured as a failover pair continuously synchronize connection state informatio and device configuration data between one another. Performing this synchronization over a high-speed LAN connection provides the added benefit of being able to geographically separate failover pair members, thus providing a further layer of protection. In the rare event of a system or network failure, network sessions are automatically transitioned between firewalls seamlessly, and with complete transparency to network users.

Robust Remote-Management Solutions Lower Total Cost of Ownership

Cisco PIX Firewalls deliver a wealth of remote-management methods for configuration, monitoring, and troubleshooting. Management solutions range from an integrated, Web-based management application to highly scalable multi-firewall management tools to support for remote-monitoring protocols such as Simple Network Management Protocol (SNMP) and syslog. Cisco PIX Firewalls additionally provide up to 16 levels of customizable administrative roles, so that enterprises can grant administrators and operations personnel the appropriate level of permissions they need for each firewall they manage (for example, monitoring only, read-only access to the configuration, VPN configuration only, firewall configuration only, etc.). Cisco PIX Firewalls now also support Auto Update, a revolutionary secure remote-management capability that ensures firewalls configurations and software images are kept up-to-date.

Cisco PIX Device Manager (PDM), integrated with Cisco PIX Firewalls, provides administrators an intuitive, Web-based management interface for remotely configuring and monitoring a single Cisco PIX Firewall, without requiring any software (other than a standard Web browser) to be installed on an administrator's computer. Administrators can also remotely configure, monitor, and troubleshoot Cisco PIX Firewalls using a command-line interface (CLI) through various methods, including Telnet and Secure Shell (SSH) Protocol, or out-of-band via a console port.

Administrators can easily manage a large number of remote Cisco PIX Firewalls using either the new combination of the CiscoWorks Management Center for Cisco PIX Firewalls and Auto Update Server, or Cisco Secure Policy Manager (CSPM)—all available within the Cisco VPN Security Management Solution (VMS) network management suite. The CiscoWorks Management Center for Cisco PIX Firewalls is a highly scalable, next-generation, three-tier management solution for Cisco PIX Firewalls that includes features such as hierarchical grouping of managed firewalls, "Smart Rules" configuration inheritance, customizable administrative roles and access privileges,

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN
CPMI CORREIOS
Fls. Nº 291
3702
Doc

workflow-based enterprise change management, comprehensive support for Cisco PIX Firewall's new Auto Update capabilities, and support for dynamically addressed firewalls. Cisco Secure Policy Manager Release 3.0 is a policy-based centralized management solution for Cisco PIX Firewalls that includes a task-based interface, an interactive network topology map, policy wizards, and policy import capabilities. Additional integrated event management and inventory solutions are also available as part of the Cisco VMS network management suite.

New Features Found in Cisco PIX Firewall Release 6.2

Cisco PIX Firewall Release 6.2 provides a wealth of new innovative features, which are detailed below:

Table 1 New Features and Benefits

New Features	Benefits
Enterprise-Class Security	
LAN-based failover	• Extends failover functionality and enables geographic separation of Cisco PIX Firewalls in a failover pair by allowing failover information to be shared over a dedicated LAN connection (instead of a serial cable) between failover pairs
Bidirectional Network Address Translation (NAT)	• Enhances rich NAT functionality in Cisco PIX Firewalls to support environments with overlapping private address ranges
Turbo access control lists (ACLs)	• Provides significantly enhanced performance and deterministic search times for ACL processing; especially useful in environments where extensive ACLs are deployed
N2H2 URL filtering	• Integrates with N2H2 Sentian™ products—leading Internet filtering solutions—to provide robust employee Web access control and monitoring
Enhanced small-packet performance	• Delivers up to 48 percent more firewall performance for 64- to 512-byte packets than previous Cisco PIX Firewall OS releases, due to further optimization of small-packet processing
Management	
Auto Update	• Provides highly scalable, secure remote management of PIX Firewalls with a unique push/pull management model • Next-generation secure XML/HTTPS interface can be leveraged by Cisco and third-party management applications for remote firewall configuration management, inventory, software image management/deployment and monitoring • Supports dynamically addressed firewalls in addition to firewalls with static IP addresses • Integrates seamlessly with CiscoWorks Management Center for Cisco PIX Firewalls and Auto Update Server for robust, scalable remote management of up to 1000 PIX Firewalls
Object grouping	• Enables administrators to group network objects (such as devices, networks, and services) into logical groups to greatly simplify access control rule definition and maintenance

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

16 382

Table 1 New Features and Benefits

New Features	Benefits
Command-level authorization	• Enables businesses to create up to 16 customizable administrative roles and profiles for accessing Cisco PIX Firewalls (for example, monitoring only, read-only access to configuration, VPN administrator, firewall administrator, etc.) • Uses either the internal Cisco PIX Firewall administrator database or outside sources via TACACS+, such as Cisco Secure ACS
Dynamic ACLs via Cisco Secure ACS	• Supports dynamic downloading and enforcement of ACLs on a per-user basis, upon user authentication with the firewall
Network Time Protocol (NTP) v3 client	• Provides convenient method for synchronizing the clock on Cisco PIX Firewalls with other devices on a network
CPU monitoring via SNMP v2	• Extends SNMP-based remote firewall health monitoring to include the ability to monitor CPU utilization
Software and configuration updates via HTTP and HTTPS	• Adds support for downloading Cisco PIX Firewall OS and Cisco PIX Device Manager software, as well as configuration updates via HTTP or HTTPS • Provides ability to deliver configuration and software updates over authenticated, encrypted network connection
HTTPS-based CLI access	• Delivers flexible, secure interface for interactive and easily scriptable access to Cisco PIX Firewall CLI via standard HTTPS requests
Packet capture	• Gives administrators new, powerful troubleshooting capabilities by providing robust packet-capturing facilities on each interface of the firewall • Supports several methods of accessing captured packets, including via the console, secure Web access or a file exported to a Trivial File Transfer Protocol (TFTP) server
Small Office/Home Office	
Easy VPN Remote (hardware VPN client)	• Enables dramatically simplified VPN rollouts to small office, teleworker, and remote/branch-office environments, allowing Cisco PIX 501, 506, and 506E Firewalls to act as hardware VPN clients, and eliminating the provisioning complexities of traditional site-to-site VPN deployments • Downloads VPN policy dynamically from an Easy VPN Server upon connection, ensuring the latest corporate security policies are enforced • Provides robust client-side VPN resiliency with support for up to ten Easy VPN servers with automatic failover, in addition to Dead Peer Detection (DPD) support • Enables the network behind a Cisco PIX Firewall to appear as a single user to the VPN headend when using Easy VPN Remote Client Mode • Provides site-to-site VPN-like functionality without requiring any additional provisioning when using Easy VPN Remote Network Extension Mode • Supports both split and non-split tunneling environments • Provides intelligent, transparent Domain Name System (DNS) proxy capabilities for access to both corporate and public DNS servers
PPP over Ethernet (PPPoE) support	• Ensures compatibility with networks that require PPPoE support, such as xDSL and cable modem broadband environments

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RÓS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 293
Doc. 3702

Table 1 New Features and Benefits

New Features	Benefits
Voice-over-IP (VoIP)/Multimedia	
Multicast support	• Supports wide range of multicast applications by introducing support for Internet Group Management Protocol (IGMP) v2 and stub multicast routing, including NAT and Port Address Translation (PAT) and the ability to build access control lists for multicast traffic
PAT for H.323 and SIP	• Extends market-leading VoIP support and enables SIP and H.323 to work in PAT environments, typically found in home offices and remote offices
DHCP server support for Cisco IP phones	• Simplifies remote Cisco IP Phone deployments by providing Cisco CallManager contact information via DHCP options 66 and 150 to Cisco IP phones for automated bootstrapping
Internet Locator Service (ILS) Fixup	• Adds support for ILS, a popular directory service used by applications such as Microsoft NetMeeting, SiteServer and Active Directory, for registration and location of network entities/endpoints

Technical Specifications

VPN Client Compatibility

Cisco PIX Firewalls support a wide variety of software- and hardware-based VPN clients, including:

Software IPSec VPN clients	Cisco Secure VPN Client Release 1.1 Cisco VPN 3000 Concentrator Client, Release 2.5 and higher Cisco VPN Client for Microsoft Windows, Release 3.0 and higher Cisco VPN Client for Linux, Release 3.5 and higher Cisco VPN Client for Solaris, Release 3.5 and higher Cisco VPN Client for Mac OS X, Release 3.5 and higher
Hardware IPSec VPN clients	Cisco VPN 3002 Hardware Client, Release 3.0 and higher Cisco IOS Software Easy VPN Remote, Release 12.2(8)YJ Cisco PIX Firewall Easy VPN Remote, Release 6.2 and higher
Layer 2 Tunneling Protocol (L2TP)/IPSec VPN clients	Microsoft Windows 2000
Point-to-Point Tunneling Protocol (PPTP) VPN clients	Microsoft Windows 95 Microsoft Windows 98 Microsoft Windows NT 4.0 Microsoft Windows 2000

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

ROS nº 03/2005 - CPMI - CORREIOS
Fls. Nº 294
Nº Doc. 3702

Easy VPN Server Compatibility

Cisco PIX Firewalls can now act as hardware-based VPN clients, taking advantage of the new Easy VPN Remote capabilities in Cisco PIX Firewall OS. The following Easy VPN Server platforms are supported for this deployment scenario:

Cisco IOS Routers	Release 12.2(8)T and higher
Cisco PIX Firewalls	Release 6.0(1) and higher
Cisco VPN 3000 Concentrators	Release 3.1 and higher

Cisco Site-to-Site VPN Compatibility

In addition to supporting interoperability with many third-party VPN products, Cisco PIX Firewalls interoperate with the following Cisco VPN products for site-to-site VPN connectivity:

Cisco IOS Routers	Release 12.1(6)T and higher
Cisco PIX Firewalls	Release 5.1(1) and higher
Cisco VPN 3000 Concentrators	Release 2.5.2 and higher

Cryptographic Standards Supported

Cisco PIX Firewalls support numerous cryptographic standards and related third-party products and services, including the following:

Asymmetric (public key) encryption algorithms	RSA (Rivest, Shamir, Adelman) public/private key pairs, 512 bits to 2048 bits
Symmetric encryption algorithms	DES: 56 bits 3DES: 168 bits RC4: 40, 56, 64, and 128 bits
Perfect Forward Secrecy (Diffie-Hellman key negotiation)	Group 1: 768-bits Group 2: 1024-bits
Hash algorithms	MD5: 128-bits SHA-1: 160-bits
X.509 certificate authorities	Baltimore UniCERT Entrust Authority Microsoft Windows 2000 Certificate Services VeriSign OnSite
X.509 certificate enrollment protocols	SCEP

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

ROS nº 033005
CPMI - CORREIOS
Fls. Nº 295
Nº Doc. 3702

System Requirements

Platforms supported	Cisco PIX 501 Firewall Cisco PIX 506 Firewall Cisco PIX 506E Firewall Cisco PIX 515 Firewall Cisco PIX 515E Firewall Cisco PIX 520 Firewall Cisco PIX 525 Firewall Cisco PIX 535 Firewall
RAM, minimum	32 MB, except Cisco PIX 501 which requires 16 MB
Flash memory, minimum	16 MB, except Cisco PIX 501/506/506E which require 8 MB
Expansion cards supported	Single-port 10/100 Fast Ethernet card Four-port 10/100 Fast Ethernet card Single-port Gigabit Ethernet, multimode (SX) SC, card VPN Acceleration Card (VAC)

Product Ordering Information

PIX-SW-UPGRADE=	Cisco PIX software one-time upgrade for customers without a current SMARTnet™ support contract

Support Services

Support services are available from Cisco partners as well as from Cisco. The Cisco SMARTnet service augments customer support resources. It provides 24x7x 365 access to technical resources (both online and via telephone), the ability to download updated system software, and hardware advance replacement.

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 296
Doc 3702

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Additional Information

For more information, please visit the following links:

Cisco PIX Firewall:

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

Cisco PIX Device Manager:

http://www.cisco.com/warp/public/cc/pd/fw/sqfw500/prodlit/pixdm_ds.pdf

Cisco Secure ACS:

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

Cisco Secure Policy Manager:

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

Cisco VPN Security Management Solution (VMS), CiscoWorks Management Center for Cisco PIX Firewalls and Auto Update Server:

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

Cisco SAFE Blueprint:

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

To download the latest Cisco PIX Firewall OS and Cisco PIX Device Manager software (with a valid Cisco.com login), visit:

http://www.cisco.com/cgi-bin/tablebuild.pl/pix

Cisco Systems, Inc.
All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 297
Nº 3702

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 317 7777
Fax: +65 317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the

Cisco Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland
Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland
Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Cisco, Cisco IOS, Cisco Systems, the Cisco Systems logo, PIX, and SMARTnet are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0208R)

RD/LW3946 12/02

CPMI - CORREIOS
Fls. Nº 298
Doc 3702

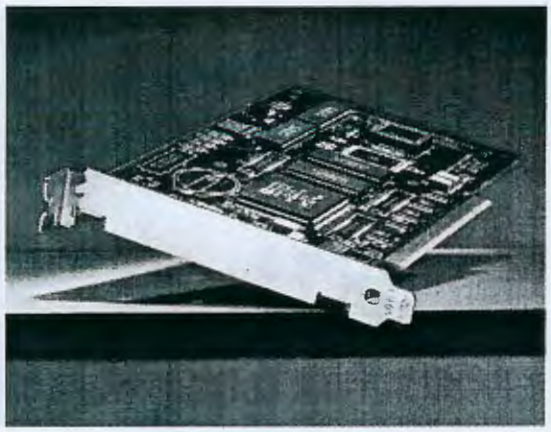
Segurança Tipo 2 doc 3

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 299
Doc. 3702

Cisco Secure PIX Firewall VPN Accelerator Card

Overview

The VPN Accelerator Card (VAC) for the Cisco Secure PIX Firewall series provides high-performance, tunneling and encryption services suitable for site-to-site and remote access applications. This hardware-based VPN accelerator is optimized to handle the repetitive but voluminous mathematical functions required for IPsec. Offloading encryption functions to the card not only improves IPsec encryption processing, but also maintains high-end firewall performance. As an integral component of the Cisco virtual private network (VPN) solution, the VPN Accelerator Card provides platform scalability and security while working seamlessly with services necessary for successful VPN deployments—encryption, tunneling, and firewall.



High Performance

The VPN Accelerator Card, which fits in a PCI slot inside the PIX chassis, encrypts data using the 56-bit Data Encryption Standard (DES) or 168-bit 3DES algorithms at speeds up to 100 Mbps. A PIX equipped with a VAC supports as many as 2,000 encrypted tunnels for concurrent sessions with mobile users or other sites. In addition to encryption, the card handles a variety of other IPsec-related tasks—hashing, key exchange, and storage of security associations—which free the PIX main processor and memory to perform other perimeter security functions.

- *Encryption*—DES and 3DES encryption are very CPU intensive, potentially impacting firewall performance in high-throughput configurations. The VAC makes it possible to send DES or 3DES encrypted data at high speed while still providing the full range of perimeter security services available from the Cisco Secure PIX Firewall.
- *Authentication*—RSA and Diffie-Hellman are CPU-intensive protocols that are used when a new IPsec tunnel is established. RSA authenticates the remote device while Diffie-Hellman exchanges keys that will be used for DES or 3DES encryption. The VPN Accelerator Card implements these protocols in specialized hardware ensuring fast tunnel setup and high overall encryption throughput.

Cisco Systems
Copyright © 2000 Cisco Systems, Inc. All Rights Reserved.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 300
Doc 3702

- *Tunneling*—The PIX and VAC support IPsec tunneling protocol enabling high-performance, flexible network designs for both remote access and site-to-site VPNs. Site-to-site solutions can be designed with PIX or combinations of PIX with Cisco VPN appliances or VPN-enabled multi-service routers. Remote access solutions can utilize Cisco's VPN client or other 3rd party clients supporting the IPsec tunneling protocol.

Increased Security

The PIX VAC provides an extra level of security by segregating sensitive VPN information from standard system processing. Encryption, authentication, and key generation mechanisms are handled by onboard memory and processors. In addition, a hardware random number generator provides high quality input to crypto functions resulting in strong security while ensuring high throughput during process-intensive re-keying operations.

Easy Implementation

PIX Firewall automatically detects the presence of the VPN Accelerator Card and transfers encryption activities to the VAC without configuration changes. Throughput is enhanced through the use of specialized hardware to perform the complex mathematical transformations necessary to generate keys, authenticate devices, authenticate packets, and encrypt and decrypt data. The VPN Accelerator Card is fully compatible with network-layer IPsec and the Layer 3 encryption software services of the Cisco Secure PIX Firewall Software.

Performance Summary

168-bit 3DES IPsec VPN throughput: 100 Mbps
Simultaneous VPN tunnels: 2,000

System Requirements

Operating System: PIX OS v5.3(1) or later (with DES or 3DES license)
Platforms: PIX 515/515E, 520, 525, 535 (limit one per chassis)

Standards Support

Protocols: IPsec, IKE, PKCS #11
Symmetric Algorithms: 56-bit DES, 168-bit 3DES
Hashing algorithms: MD-5, SHA-1
Asymmetric Algorithms: RSA, Diffie-Helman, DSA

Technical Specifications

Processor: IRE 2141
Random Access Memory: 2 MB of SDRAM
PCI Interface: 32-bit, 33-MHz PCI v2.1 (short form)

Environmental

Operating
Temperature: 32° to 122° F (0° to 50° C)
Relative Humidity: 10% to 90% noncondensing

Nonoperating
Temperature: 32° to 158° F (0° to 70° C)

Power

Input
Range Line Voltage: 5V +/-10%, 3.3V +/-10%
Nominal Line Voltage: 5V +/-10%, 3.3V +/-10%
Power: 1.5W

Dimensions and Weight

Height: 4.2 inches (10.7 cm)
Depth: 6.875 inches (17.5 cm)
Weight: ~ .5 pounds (.2 kg)

Certifications

Safety: UL 1950, CSA C22.2 No. 950, EN 60950, IEC 60950, AS/NZS3260, TS001, IEC60825, EN 60825, 21CFR104

EMI: CFR 47 Part 15 Class A (FCC), ICES 003 Class A with UTP, EN55022 Class A with UTP, CISPR 22 Class A with UTP, AS/NZ 3548 Class A with UTP, VCCI Class A with UTP, EN55024, EN50082-1 (1997), CE marking, EN55022 Class B with FTP, Cispr 22 Class B with FTP, AS/NZ 3548 Class B with FTP, VCCI Class B with FTP

Cisco Systems
Copyright © 2000 Cisco Systems, Inc. All Rights Reserved.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 301
Doc 3702

Ordering Information

PIX-VPN-ACCEL	IPsec Hardware VPN Accelerator Card (VAC)
PIX-VPN-3DES	168-bit 3DES IPsec VPN software license
PIX-VPN-DES	56-bit DES IPsec VPN software license

Additional Information

For more information about PIX Firewall, go to http://www.cisco.com/go/pix

Export Considerations

The PIX VPN Accelerator Card and associated software may be export controlled. Refer to the export compliance Web site at: http://www.cisco.com/wwl/export/crypto/ for guidance. For specific export questions, contact export@cisco.com

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems Europe
11, Rue Camille Desmoulins
92782 Issy Les Moulineaux
Cedex 9
France
www.cisco.com
Tel: 33 1 58 04 60 00
Fax: 33 1 58 04 61 00

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems Australia, Pty., Ltd
Level 17, 99 Walker Street
North Sydney
NSW 2059 Australia
www.cisco.com
Tel: +61 2 8448 7100
Fax: +61 2 9957 4350

Cisco Systems has more than 190 offices in the following countries. Addresses, phone numbers, and fax numbers are listed on the **Cisco.com Web site at www.cisco.com/go/offices.**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China • Colombia • Costa Rica • Croatia • Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong • Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Copyright © 2000 Cisco Systems, Inc. All rights reserved. PIX is a trademark, and Cisco, Cisco IOS, Cisco Systems, and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. or its affiliates in the U.S. and certain other countries. All other brands, names, or trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (00010R)

11/00 DA

№ Doc. 3702

16 343

Segurança Tipo 2 doc 4

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 303
Doc 3702

Cisco Systems

Data Sheet

CiscoWorks **Management Center** for Firewalls, Version 1.2

Introduction

The CiscoWorks Management Center for Firewalls and Auto Update Server Software are the functional components, within the CiscoWorks VPN/Security Solution (VMS), that provide unprecedented manageability for the Cisco Firewall product line. The Management Center for Firewalls features the "look and feel" of the Cisco PIX Device Manager (PDM) but offers centralized management scalability of up to 1,000 Cisco Firewalls.

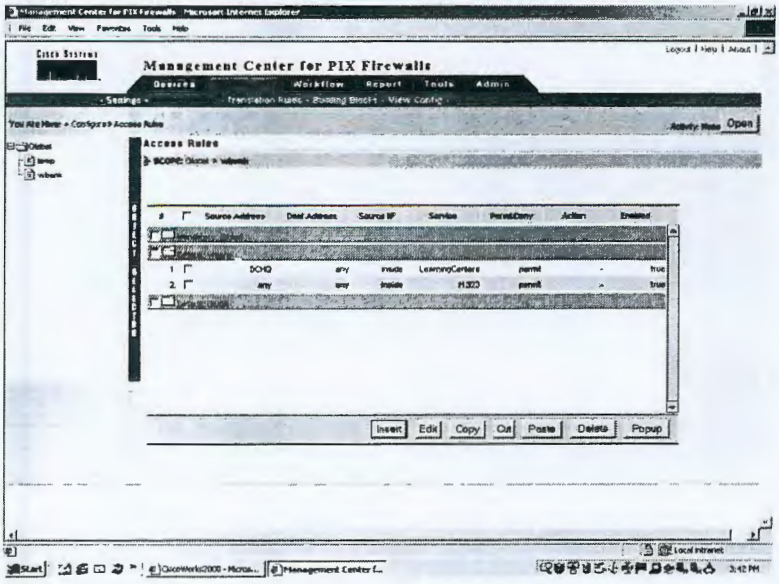
This management center component of CiscoWorks VMS, is an integral part of the SAFE blueprint, and combines Web-based tools for configuring, monitoring, and troubleshooting the following:

- VPNs
- Firewalls
- Network intrusion detection systems (IDS)
- Host-based IDS

CiscoWorks VMS addresses the needs of both small- and large-scale VPN and security deployments, and enables organizations to protect productivity gai and reduce operating costs.

Cisco protects the productivity of your enterprise with an integrated security management solution. Unlike pointer security products from multiple vendors that leave vulnerable gaps with different GUIs, CiscoWorks VMS provides a comprehensive solution that ties separate security and VPN technologies into a singl whole secure network.

Figure 1
CiscoWorks Management Center for PIX Firewalls



New Features

Management Center for Firewalls version 1.2 is the follow-on version of the Management Center for PIX Firewalls version 1.1. This module has been rename to reflect the additional support for the Firwall Services Module (FWSM). Managment Center for Firewalls version 1.2 adds support for the following new features:

- Cisco PIX 6.3
- Single ckick to deploy configurations (No activity and job management)
- Object groups
- Dual NAT

Cisco Systems, Inc.
All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

ECT nº 03/2006 - CN
CPMI - CORREIOS
Fls Nº 304
Nº Doc 3702

- Solaris
- VLANs
- Syslog per access-list
- Single Auto Update Server (AUS) set up for an entire group of Cisco PIX
- NAT 0 ACL
- Cut and paste of building blocks

Intended Use

The Management Center for Firewalls provides SAFE coverage and centralized management of access rules, Netwo Address Translation (NAT), intrusion detection, and VPN on Cisco Firewalls. It supports centralized manageme of virtually any Cisco Firewall security network including remote access; demilitarized zone (DMZ); small office home office (SOHO); voice, storage, and wireless networks; Internet security; and management security provide scenarios.

Features and Benefits

The Management Center for Firewalls provides unique and robust scalability with these industry-first features:

- Smart Rules hierarchy and inheritance
- User-defined device and customer groups including nesting
- Global role-based access (RBAC) with administrative privileges per device and customer groups with CiscoWo products and Cisco Secure Access Control Server (ACS)
- Mandatory and default device settings inheritance
- Workflow deployment to device, directory or Auto Update Server
- Look and feel of Cisco PIX Device Manager (PDM) but with scalability to 1,000 Cisco Firewalls
- Web GUI
- Integration of market-leading management features from other CiscoWorks products
- Complete SAFE coverage for centralized management of Cisco PIX and Firewall Services Module including access control, virtual private networks (VPN), intrusion detection systems (IDS), and authentication, authorization, and accounting (AAA)
- Reduction in total configuration time
- Reduction in manual configuration errors
- Automatic update of remote firewall configurations and operating systems
- Automatic and periodic verification of remote firewall configurations

Smart Rules

Smart Rules is an innovate feature that allows common information, including access rules and settings, to be inherited for all firewalls in a device or customer group. Smart Rules allows a user to define common rules once, reducing configuration time and resulting in fewer administrative errors. Furthermore, Smart Rules offers higher device scalability. A user can configure a common rule (such as allowing all HTTP traffic) once, and then apply th global rule to all firewalls. Smart Rules can also be defined on a device or customer group.

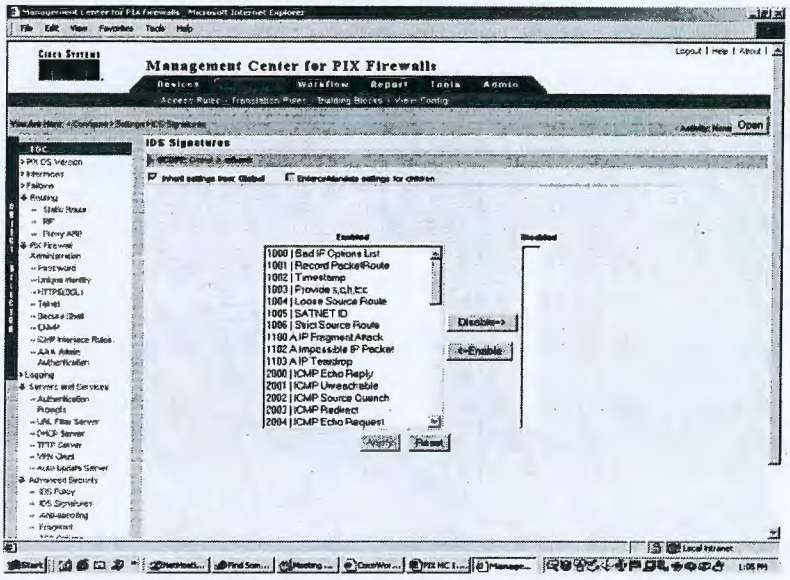
ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 305
Doc 3702

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Granular Administrative Privileges for Customer/Device Groups

The CiscoWorks Management Center for Firewalls allows devices to be separated by geography, customer, device type, or any other mechanism the user wants. The Management Center for Firewalls supports multiple administrators. Administrative privileges can be defined on a device or customer group. Basic administrative privileges include the five roles defined in the CiscoWorks desktop. Administrative privileges can also be defined within Cisco Secure Access Control Server (ACS) to allow very granular administrative privileges so that a custom can view their own firewall configurations but not those of another customer.

Global/Group Device Settings



The CiscoWorks Management Center for Firewalls supports an extensive list of device settings including Failover, Routing, SNMP, ICMP, AAA, DHCP, TFTP, VPN Client, IDS, and IP Anti-spoofing. All of these settings can be defined globally and inherited by all applicable firewalls. Any of these settings can also be defined on a device or customer group for unprecedented scalability. Powerful feature settings, including IDS signatures, can now be defined for all applicable firewalls with just a few mouse clicks.

Benefits of Cisco PDM, Cisco.com, and CiscoWorks

Other competitive products simply distribute all configuration changes to all devices. Like other CiscoWorks products, the Management Center for Firewalls supports flexible configuration deployment to either a device, file directory, or Auto Update Server. The Management Center for Firewalls features the "look and feel" of the single-firewall Cisco PDM. It also offers the usability of Cisco PDM combined with the scalability of centralized management for up to 1,000 Cisco Firewalls.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
306
3702

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

The Management Center for Firewalls incorporates an easy-to-use Web GUI and secure configuration and distribution with Secure Socket Layer (SSL) and secure digital certificates. The Management Center for Firewalls also supports key scalability features from CiscoWorks LAN Management Solution (LMS) and Routed WAN Management Solution (RWAN) that facilitate LAN and WAN deployments of more than 20,000 devices. Key CiscoWorks features supported by the Management Center for Firewalls include an approval flow, device list from CiscoWorks Resource Manager Essentials (RME), rollback, and activity and job management.

Device Support

- The Management Center for Firewalls supports the following Cisco Firewall platforms: Cisco PIX 501, 506, 506E, 515, 515E, 525, 535; and the Cisco Firewall Services Module (FWSM)
- The Management Center for Firewalls supports versions 6.0, 6.1, and 6.2 of the Cisco PIX Operating System, and FWSM versions 1.1(x).

The Management Center for Firewalls will import the configuration of existing Cisco Firewall version 6.0 deployments. The Management Center for Firewalls also features an outbound/conduit to an access list conversion tool that enables conversion of existing access configurations to access lists.

System Requirements

The Management Center server software is currently supported on Windows 2000 only. For comprehensive hardware and operating requirements, see the CiscoWorks VMS Overview at http://www.cisco.com/go/vms.

Ordering Information

The Management Center for Firewalls is available exclusively as part of CiscoWorks VPN/Security Management Solution (VMS). For details on ordering, refer to the CiscoWorks VMS Product Bulletin at http://www.cisco.com/go/vms.

For More Information

Please reference http://www.cisco.com/go/vms for more information about CiscoWorks VMS, or email ciscoworks@cisco.com.

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 317 7777
Fax: +65 317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the **Cisco Web site at www.cisco.com/go/offices**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

All contents are Copyright © 1992–2002, Cisco Systems, Inc. All rights reserved. Cisco, Cisco IOS, Cisco Systems, the Cisco Systems logo, and PIX are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries. All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0208R)

202970/ETMG 9/02

RGIS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 307
3702
Doc

16 566
L

Segurança Tipo 2 doc 5

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 308
Doc 3702

Cisco Systems

16.365

Data Sheet

Monitoring Center for **Security**, Version 1.2

Introduction

The Monitoring Center for Security is a tool to capture, store, view, correlate and report on events from:

- Cisco Network IDS
- Cisco Switch IDS
- Cisco IDS Network Module for routers
- Management Center for Cisco Security Agents
- Cisco PIX Firewalls
- Cisco Firewall Services Modules
- Cisco IOS Routers

The Monitoring Center for Security will increase the accuracy of threat detection and lower the operational costs for event monitoring, and will increase your administrator's productivity. The software delivers event correlation to identify attacks that are not easily recognizable from a single event, a flexible notification scheme and automated responses to critical events. By taking advantage of user-defined event correlation rules, the operator can:

- Monitor attacks against specific, high visibility hosts (for example, a web server).
- Monitor the traffic for patterns of attacks
- Correlate IDS information from multiple security devices (e.g., firewalls, network IDS, host IDS)
- Receive early notification of emerging threats
- Trigger an automated response, as a corrective action against an attack
- Reduce the number of false positives

The Monitoring Center for Security is a component of the CiscoWorks VPN/ Security Management Solution (VMS). VMS is an integral part of the SAFE blueprint and combines web-based tools for configuring, monitoring and troubleshooting:

- Virtual Private Networks (VPN)
- Firewalls
- Network Intrusion Detection Systems (IDS)
- Host-based IDS

CiscoWorks VMS addresses the needs of both small- and large-scale VPN and security deployments by protecting productivity gains and reducing operating costs fororganizations.

Intended Use

The Monitoring Center for Security will benefit those organizations experiencing information overload, resulting from:

- Too many security consoles
- Too many security events to monitor
- Difficulty in viewing the big security picture

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 309
Doc 3702

New Features

The Monitoring Center for Security includes support for additional event types. The operator can now monitor events from the Management Center for Cisco Security Agents, version 4.0 and also monitor events from the Cisco Intrusion Detection System (IDS) software version 4.1. The Management Center for Cisco Security Agents 4.0 will receive events from agents and then forward these events to the Monitoring Center for Security version 1.2. As a result, the Monitoring Center for Security provides a broad, unified view of security messages.

Support for IDS 4.1 allows the operator to monitor network IDS sensors that communicate using the Remote Data Exchange Protocol (RDEP). With the RDEP protocol the operator can subscribe to specific IDS event types and better control which events are received.

Enhancements in the event viewer include performance improvements for event deletions and an addition of a new interface graphing capability. The user can also preserve their preferred column ordering in the event viewer.

Enhancements for reporting include the ability to save generated reports to the database and to a file for more flexible storage options. Furthermore, new summary information has been added to reports to help with analysis. Cisco has added more reports for firewalls and Cisco Security Agents.

Enhancements in the notification system include an increase in the number of active events rules from 5 to 10. Event rules help identify critical events and automate a response so that the operator does not need to monitor a screen over long periods. The operator can also import Cisco IDS Sensor configurations from a remote Management Center for IDS Sensors server to save time.

The Monitoring Center for Security, version 1.1 is now supported on Solaris 8. This software does not have some of the features that are available in the Monitoring Center for Security version 1.2, which is available only on Windows 2000 currently. Examples of features not supported on the Solaris platform include:

- No support for events from the Management Center for Cisco Security Agents, version 4.0
- No support for events from the Cisco IDS Network Module for routers
- No support for events form IDS version 4.1 (however, IDS 4.0 is supported)
- No additional reports for firewall and Cisco Security Agents
- No support for saving the preferences of column ordering in the event viewer

Features and Benefits

Comprehensive reporting options for finding information

- Web-based wizard for creating flexible security reports
- On-demand and scheduled reports
- Reports by top incidents, by IP address, by time, by signature, by event, etc.
- Send notifications of reports by email

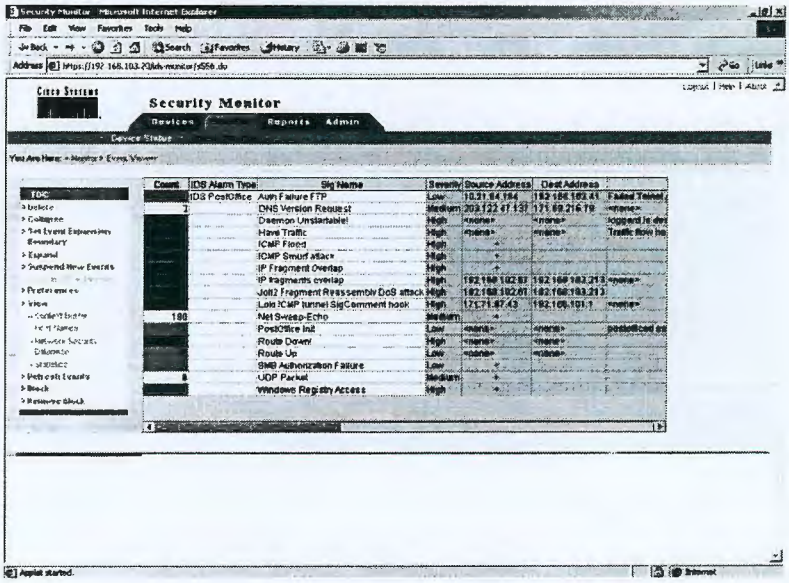
Web-based event viewer with features to easily locate attacks

- Easily "slice and dice" data by moving event field columns and sifting through thousands of events in seconds. The Event Viewer can read both real-time and historical events from the database.

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

ROS nº 03/2005 - CN
CPMI CORREIOS
Fls. Nº 310
Doc 3702

Figure 1
Design based on award winning event viewer.



Perform event correlation to detect an emerging threat

- Create user-defined rules for establishing relationships between events (correlate by type of event, by time, acros sensors, across source addresses, etc.). This helps to identify attacks, which may not be apparent from a single event.
- The user can define thresholds and time periods when a rule should be triggered
- If a rule is triggered, the user can be notified via email and fine-tune what information from the suspicious packe is forwarded with the email. Alternatively, the user can automatically execute a script as a corrective response

Database Management

- The Monitoring Center for Security provides a relational database that is used for storage of event data. Various database management functions such as archiving and purging can easily be performed without database administration skills within the Monitoring Center for Security using the web interface.

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

ROS n° 03/2005 - CPMI CORREIOS
Fls. Nº 311
Doc 3702

Devices Supported for Monitoring

Platform	Software Version Supported
Cisco Network IDS sensors	IDS 3.0, 3.1, 4.0 and 4.1
Cisco Switch IDS (IDSM) sensors	IDSM 3.0(5), 4.0 and 4.1
Cisco IDS Network Module for Cisco Routers	IDS 4.1
Cisco PIX Firewall	Cisco PIX Firewall OS 6.0(x), 6.1(x), 6.2(x), 6.3.1
Cisco Firewall Services Modules	1.1
Cisco IOS Router for IDS messages (with IOS Firewall toolkit)	12.2x mainline and later
Cisco Security Agents (forwarded by Management Center for Cisco Security Agents, version 4.0)	4.0
Cisco IDS Host Console (forwarded by the Cisco IDS Host Console, version 2.5)	2.5

System Requirements

For comprehensive hardware and operating requirements see the VMS Overview.

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

Ordering Information

The Monitoring Center for Security is a featured component of CiscoWorks VMS. For ordering details click on the VMS Product Bulletin found at:

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

For More Information

Please reference http://www.cisco.com/go/vms or email ciscoworks@cisco.com

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 317 7777
Fax: +65 317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the

Cisco Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland
Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland
Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

All contents are Copyright © 1992–2002, Cisco Systems, Inc. All rights reserved. Cisco, Cisco IOS, Cisco Systems, the Cisco Systems logo, and PIX are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries. All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0208R)

202970/ETMG 9/02

CFMI CORREIOS
Fls Nº 372
Doc 3702

Segurança Tipo 2 doc 6

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 313
Doc. 3702

Configuring IPSec

This chapter provides information about IP Security Protocol (IPSec), Internet Key Exchange (IKE), IKE Mode Configuration, and Certification Authority (CA) features so that you can successfully implement these features into the PIX Firewall and have Virtual Private Network (VPN) capability. This chapter describes the features' functions, as well as how these features interoperate with one another. You will find the applicable configuration procedures after each component's "about" section.

This chapter includes the following sections:

- Supported Standards
- List of Terms
- Order in Which You Configure Your IPSec
- About IPSec
- Configuring IPSec
- About IKE
- Configuring IKE
- About IKE Mode Configuration (Dynamic IP Address Assignment for Cisco Secure VPN Client)
- Configuring Dynamic IP Addressing Assignment
- About CA
- Configuring CA

The IPSec-related commands are listed and described within Chapter 6, "Command Reference."

See Chapter 5, "Configuration Examples," for additional examples of IPSec configurations.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 314
Doc 3702

Supported Standards

Cisco implements the following standards for the IPSec and IKE features within the PIX Firewall:

- IPSec—IP Security Protocol. IPSec is a framework of open standards that provides data confidentiality, data integrity, and data authentication between participating peers. IPSec provides these security services at the IP layer; it uses IKE to handle negotiation of protocols and algorithms based on local policy and to generate the encryption and authentication keys to be used by IPSec. IPSec can be used to protect one or more data flows between a pair of hosts, between a pair of security gateways, or between a security gateway and a host.

  IPSec is documented in a series of Internet RFCs, all available at http://www.ietf.org/html.charters/ipsec-charter.html. The overall IPSec implementation is guided by "Security Architecture for the Internet Protocol," RFC2401.

- Internet Key Exchange (IKE)—A hybrid protocol that implements Oakley and SKEME key exchanges inside the Internet Security Association and Key Management Protocol (ISAKMP) framework. While IKE can be used with other protocols, its initial implementation is with the IPSec protocol. IKE provides authentication of the IPSec peers, negotiates IPSec security associations, and establishes IPSec keys.

IPSec as implemented in PIX Firewall supports the following additional standards:

- AH—Authentication Header. A security protocol that provides data authentication and optional anti-replay services. AH is embedded in the data to be protected (a full IP datagram).

  The AH protocol (RFC2402) allows for the use of various authentication algorithms; PIX Firewall has implemented the mandatory MD5-HMAC (RFC2403) and SHA-HMAC (RFC2404) authentication algorithms. Used in conjunction with ISAKMP, the AH protocol algorithms. In conjunction with ISAKMP, the ESP protocol provides anti-replay services.

- ESP—Encapsulating Security Payload. A security protocol that provides data privacy services and optional data authentication, and anti-replay services. ESP encapsulates the data to be protected.

  The ESP protocol (RFC2406) allows for the use of various cipher algorithms and (optionally) various authentication algorithms. The PIX Firewall implements the mandatory 56-bit DES-CBC with Explicit IV (RFC2405); as the encryption algorithm, and MD5-HMAC (RFC2403) or SHA-HMAC (RFC2404) as the authentication.

IKE is implemented per the latest version of the "The Internet Key Exchange" Internet Draft (draft-ietf-ipsec-isakmp-oakley-xx.txt).

ISAKMP—The Internet Security Association and Key Management Protocol. A protocol framework that defines payload formats, the mechanics of implementing a key exchange protocol, and the negotiation of a security association.

ISAKMP is implemented per the latest version of the "Internet Security Association and Key Management Protocol (ISAKMP)" Internet Draft (draft-ietf-ipsec-isakmp-xx.txt).

Oakley—A key exchange protocol that defines how to derive authenticated keying material.

Skeme—A key exchange protocol that defines how to derive authenticated keying material, with rapid key refreshment.

The component technologies implemented for use by IKE include:

- DES—Data Encryption Standard (DES) is used to encrypt packet data. IKE implements the 56-bit DES-CBC with Explicit IV standard. See "CBC."
- Triple DES (3DES)—A variant of DES, which iterates three times with three separate keys, effectively doubling the strength of DES.

CPMI - CORREIOS
Fls. Nº 315
Doc 3702

- CBC—Cipher Block Chaining (CBC) requires an initialization vector (IV) to start encryption. The IV is explicitly given in the IPSec packet.
- Diffie-Hellman—A public-key cryptography protocol which allows two parties to establish a shared secret over an unsecure communications channel. Diffie-Hellman is used within IKE to establish session keys. 768-bit and 1024-bit Diffie-Hellman groups are supported.
- MD5 (HMAC variant)—MD5 (Message Digest 5) is a hash algorithm used to authenticate packet data. HMAC is a variant which provides an additional level of hashing.
- SHA (HMAC variant)—SHA (Secure Hash Algorithm) is a hash algorithm used to authenticate packet data. HMAC is a variant which provides an additional level of hashing.
- RSA signatures—RSA is the public key cryptographic system developed by Ron Rivest, Adi Shamir, and Leonard Adleman. RSA signatures provides non-repudiation.

IKE interoperates with the following standard:

X.509v3 certificates—Used with the IKE protocol when authentication requires public keys. Certificate support that allows the IPSec-protected network to scale by providing the equivalent of a digital ID card to each device. When two peers wish to communicate, they exchange digital certificates to prove their identities (thus removing the need to manually exchange public keys with each peer or to manually specify a shared key at each peer). These certificates are obtained from a CA. X.509 is part of the X.500 standard by the ITU.

CA supports the following standards:

- X.509v3 certificates
- Public-Key Cryptography Standard #7 (PKCS #7)—A standard from RSA Data Security, Inc. used to encrypt and sign certificate enrollment messages.
- Public-Key Cryptography Standard #10 (PKCS #10)—A standard syntax from RSA Data Security, Inc. for certificate requests.
- RSA Keys—RSA is the public key cryptographic system developed by Ron Rivest, Adi Shamir, and Leonard Adleman. RSA keys come in pairs: one public key and one private key.

List of Terms

anti-replay—A security service where the receiver can reject old or duplicate packets to protect itself against replay attacks. IPSec provides this optional service by use of a sequence number combined with the use of data authentication. PIX Firewall IPSec provides this service whenever it provides the data authentication service, except in the following cases:

- The service is not available for manually established security associations (that is, security associations established by manual configuration and not by IKE).

client—Node or software program (front-end device) that requests services from a server.

data authentication—Includes two concepts:

- Data integrity (verify that data has not been altered).
- Data origin authentication (verify that the data was actually sent by the claimed sender).

Data authentication can refer either to integrity alone or to both of these concepts (although data origin authentication is dependent upon data integrity).

data confidentiality—A security service where the protected data cannot be observed.

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 3156
Doc 3702

data flow—A grouping of traffic, identified by a combination of source address/netmask, destination address/netmask, IP next protocol field, and source and destination ports, where the protocol and port fields can have the values of any. In effect, all traffic matching a specific combination of these values is logically grouped together into a data flow. A data flow can represent a single TCP connection between two hosts, or it can represent all traffic between two subnets. IPSec protection is applied to data flows.

gateway—A device that performs an application layer conversion from one protocol stack to another.

peer—In the context of this chapter, a peer refers to a PIX Firewall or other device, such as a Cisco router, that participates in IPSec, IKE, and CA.

perfect forward secrecy (PFS)—A cryptographic characteristic associated with a derived shared secret value. With PFS, if one key is compromised, previous and subsequent keys are not compromised, because subsequent keys are not derived from previous keys.

repudiation—A quality that prevents a third party from being able to prove that a communication between two other parties ever took place. This is a desirable quality if you do not want your communications to be traceable. Non-repudiation is the opposite quality—a third party can prove that a communication between two other parties took place. Non-repudiation is desirable if you want to be able to trace your communications and prove that they occurred.

security association—An IPSec security association (SA) is a description of how two or more entities will use security services in the context of a particular security protocol (AH or ESP) to communicate securely on behalf of a particular data flow. It includes such things as the transform and the shared secret keys to be used for protecting the traffic.

The IPSec security association is established either by IKE or by manual user configuration. Security associations are uni-directional and are unique per security protocol. So when security associations are established for IPSec, the security associations (for each protocol) for both directions are established at the same time.

When using IKE to establish the security associations for the data flow, the security associations are established when needed and expire after a period of time (or volume of traffic). If the security associations are manually established, they are established as soon as the necessary configuration is completed and do not expire.

Security parameter index (SPI)—This is a number which, together with a destination IP address and security protocol, uniquely identifies a particular security association. When using IKE to establish the security associations, the SPI for each security association is a pseudo-randomly derived number. Without IKE, the SPI is manually specified for each security association.

transform—A transform lists a security protocol (AH or ESP) with its corresponding algorithms. For example, one transform is the AH protocol with the MD5-HMAC authentication algorithm; another transform is the ESP protocol with the 56-bit DES encryption algorithm and the SHA-HMAC authentication algorithm.

tunnel—In the context of this chapter, a tunnel refers to secure communication path between two peers, such as two PIX Firewall units. It does not refer to using IPSec in tunnel mode.

Virtual Private Network (VPN)—Enables IP traffic to travel securely over a public TCP/IP network by encrypting all traffic from one network to another.

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 317
Doc
Nº 3702

Order in Which You Configure Your IPSec

If you will implement interoperability with a CA, it is recommended that you perform your IPSec configuration in the following order:

1 CA (see "Configuring CA")

2 IKE (see "Configuring IKE")

3 (Optional) IKE Mode Configuration—applies only if you are configuring dynamic IP addressing for remote clients (see "Configuring Dynamic IP Addressing Assignment"

4 IPSec (see "Configuring IPSec")

If you will *not* implement interoperability with a CA, and you will implement IKE, it is recommended that you perform your IPSec configuration in the following order:

1 IKE (see "Configuring IKE")

2 (Optional) IKE Mode Configuration—applies only if you are configuring dynamic IP addressing for remote clients (see "Configuring Dynamic IP Addressing Assignment"

3 IPSec (see "Configuring IPSec")

If you will *not* implement IKE, see "Configuring IPSec."

Note Be sure to disable IKE, if you will not implement it.

About IPSec

IPSec provides security for transmission of sensitive information over unprotected networks such as the Internet. IPSec acts at the network layer, protecting and authenticating IP packets between participating IPSec devices (peers), such as PIX Firewall units.

With IPSec, data can be transmitted across a public network without fear of observation, modification, or spoofing. This enables applications such as VPNs, which are categorized by intranets, extranets, and remote dial access. Each VPN type has different security service needs.With VPN, customers, business partners, and remote users, such as telecommuters, can access enterprise computing resources securely. VPNs essentially extend a network's capability by accommodating the demands of a networked economy for diverse secured connectivity.

IPSec provides the following network security services. These services are optional. In general, local security policy will dictate the use of one or more of these services:

- Data Confidentiality—The IPSec sender can encrypt packets before transmitting them across a network.
- Data Integrity—The IPSec receiver can authenticate packets sent by the IPSec sender to ensure that the data has not been altered during transmission.
- Data Origin Authentication—The IPSec receiver can authenticate the source of the IPSec packets sent. This service is dependent upon the data integrity service.
- Anti-Replay—The IPSec receiver can detect and reject replayed packets.

Note The term data authentication is generally used to mean data integrity and data origin authentication. Within this chapter, it also includes anti-replay services, unless otherwise specified.

POS Nº 03/2005 CPMI CORREIOS
Fls Nº 578
Doc 3702

In simple terms, IPSec provides secure tunnels between two peers, such as two PIX Firewall units. You define which packets are considered sensitive and should be sent through these secure tunnels, and you define the parameters that should be used to protect these sensitive packets, by specifying the characteristics of these tunnels. Then, when the IPSec peer sees such a sensitive packet, it sets up the appropriate secure tunnel and sends the packet through the tunnel to the remote peer.

More accurately, these tunnels are sets of security associations that are established between two remote IPSec peers. The security associations define which protocols and algorithms should be applied to sensitive packets, and also specify the keying material to be used by the two peers. security associations are uni-directional and are established per security protocol (AH or ESP).

With IPSec, you define what traffic should be protected between two remote IPSec peers by configuring access lists and applying these access lists to interfaces by way of crypto map sets. Therefore, traffic may be selected on the basis of source and destination address. (Access lists used for IPSec are used only to determine which traffic should be protected by IPSec, not which traffic should be blocked or permitted through the interface. Separate access lists define blocking and permitting at the interface or inbound and outbound from the PIX Firewall.)

Note Access lists used by IPSec on the PIX Firewall can only contain host selector or greater.

A crypto map set can contain multiple entries, each with a different access list. The crypto map entries are searched in order—the PIX Firewall attempts to match the packet to the access list specified in that entry.

When a packet matches a permit entry in a particular access list, and the corresponding crypto map entry is tagged as ipsec-isakmp, IPSec is triggered. If no security association exists that IPSec can use to protect this traffic to the peer, IPSec uses IKE to negotiate with the peer to set up the necessary IPSec security associations on behalf of the data flow. The negotiation uses information specified in the crypto map entry as well as the data flow information from the specific access list entry. (The behavior is different for dynamic crypto map entries. Refer to "Dynamic Crypto Maps."

If the crypto map entry is tagged as ipsec-manual, IPSec is triggered. If no security association exists that IPSec can use to protect this traffic to the peer, the traffic is dropped. In this case, the security associations are installed via the configuration, without the intervention of IKE. If the security associations did not exist, IPSec did not have all the necessary pieces configured.

Once established, the set of security associations (outbound, to the remote peer) is then applied to the triggering packet as well as to subsequent applicable packets as those packets exit the PIX Firewall. "Applicable" packets are packets that match the same access list criteria that the original packet matched. For example, all applicable packets could be encrypted before being forwarded to the remote peer. The corresponding inbound security associations are used when processing the incoming traffic from that peer.

If IKE is used to establish the security associations, the security associations will have lifetimes so that they will periodically expire and require renegotiation. (This provides an additional level of security.)

Multiple IPSec tunnels can exist between two peers to secure different data streams, with each tunnel using a separate set of security associations. For example, some data streams might be just authenticated while other data streams must be both encrypted and authenticated.

Access lists associated with IPSec crypto map entries also represent which traffic the PIX Firewall requires to be protected by IPSec. Inbound traffic is processed against the crypto map entries—if an unprotected packet matches a permit entry in a particular access list associated with an IPSec crypto map entry, that packet is dropped because it was not sent as an IPSec-protected packet.

CPMI - CORREIOS
Fls. Nº 319
Doc. 3702

Crypto map entries also include transform sets. A transform set is an acceptable combination of security protocols, algorithms, and other settings to apply to IPSec-protected traffic. During the IPSec security association negotiation, the peers agree to use a particular transform set when protecting a particular data flow.

This section includes the following topics, which describe more IPSec conceptual information you will need to know prior to performing your IPSec configuration tasks. The procedures for configuring IPSec are covered in the section "Configuring IPSec."

- Access Lists' Compatibility with IPSec
- Global Lifetimes for IPSec Security Associations
- Crypto Access Lists
- Transform Sets
- Crypto Map Entries
- Apply Crypto Map Sets to Interface
- Monitor and Maintain IPSec

Access Lists' Compatibility with IPSec

By default, IPSec and all packets that traverse the PIX Firewall are subjected to blocking as specified by inbound conduit, outbound list or interface access-list. To enable IPSec packets to traverse the PIX Firewall, ensure that you have statements in conduits, outbound lists or interface access-lists that permit the packets. Optionally, **sysopt connection permit-ipsec** can be configured to enable IPSec packets to bypass the conduit, outbound list and interface access-list blocking.

Note The **syopt connection permit-ipsec** command enables all packets that are destined to and arriving from an IPSec tunnel to bypass the conduit, outbound list, and interface access-list checks.

Note IPSec packets that are destined to an IPSec tunnel are selected by the crypto map access-list bound to the outgoing interface. IPSec packets that arrive from an IPSec tunnel are authenticated/deciphered by IPSec and subjected to the proxy identity match of the tunnel.

Global Lifetimes for IPSec Security Associations

You can change the global lifetime values that are used when negotiating new IPSec security associations. (These global lifetime values can be overridden for a particular crypto map entry.)

These lifetimes only apply to security associations established via IKE. Manually established security associations do not expire.

There are two lifetimes: a "timed" lifetime and a "traffic-volume" lifetime. A security association expires after the respective lifetime is reached and negotiations will be initiated for new one. The default lifetimes are 28,800 seconds (eight hours) and 4,608,000 kilobytes (10 megabytes per second for one hour).

If you change a global lifetime, the new lifetime value will not be applied to currently existing security associations, but will be used in the negotiation of subsequently established security associations. If you wish to use the new values immediately, you can clear all or part of the security association database. Refer to the **clear crypto sa** command for more details.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 320
Doc. 3702

IPSec security associations use one or more shared secret keys. These keys and their security associations time out together.

How These Lifetimes Work

Assuming that the particular crypto map entry does not have lifetime values configured, when the firewall requests new security associations it will specify its global lifetime values in the request to the peer; it will use this value as the lifetime of the new security associations. When the firewall receives a negotiation request from the peer, it will use the smaller of either the lifetime value proposed by the peer or the locally configured lifetime value as the lifetime of the new security associations.

The security association (and corresponding keys) will expire according to whichever occurs sooner, either after the seconds timeout or after the kilobytes amount of traffic is passed.

A new security association is negotiated before the lifetime threshold of the existing security association is reached to ensure that a new security association is ready for use when the old one expires. The new security association is negotiated either 30 seconds before the seconds lifetime expires or when the volume of traffic through the tunnel reaches 256 kilobytes less than the kilobytes lifetime (whichever occurs first).

If no traffic has passed through the tunnel during the entire life of the security association, a new security association is not negotiated when the lifetime expires.

Instead, a new security association will be negotiated only when IPSec sees another packet that should be protected.

Crypto Access Lists

Crypto access lists are used to define which IP traffic will be protected by crypto and which traffic will not be protected by crypto. (These access lists are not the same as regular access lists, which determine what traffic to forward or block at an interface.) For example, access lists can be created to protect all IP traffic between Subnet A and Subnet Y or between Host A and Host B.

The access lists themselves are not specific to IPSec. It is the crypto map entry referencing the specific access list that defines whether IPSec processing is applied to the traffic matching a permit in the access list.

Crypto access lists associated with IPSec crypto map entries have four primary functions:

- Select outbound traffic to be protected by IPSec (permit = protect).
- Indicate the data flow to be protected by the new security associations (specified by a single permit entry) when initiating negotiations for IPSec security associations.
- Process inbound traffic to filter out and discard traffic that should have been protected by IPSec.
- Determine whether or not to accept requests for IPSec security associations on behalf of the requested data flows when processing IKE negotiation from the peer. (Negotiation is only done for ipsec-isakmp crypto map entries.) In order for the peer's request to be accepted during negotiation, the peer must specify a data flow that is "permitted" by a crypto access list associated with an ipsec-isakmp crypto map entry.

If you want certain traffic to receive one combination of IPSec protection (for example, authentication only) and other traffic to receive a different combination of IPSec protection (for example, both authentication and encryption), you need to create two different crypto access lists to define the two different types of traffic. These different access lists are then used in different crypto map entries which specify different IPSec policies.

Fls. Nº 321
Doc. 3702

You will then later associate the crypto access lists to the PIX Firewall's outside interface when you configure and apply crypto map sets to this interface.

Crypto Access List Tips

Using the **permit** keyword causes all IP traffic that matches the specified conditions to be protected by crypto, using the policy described by the corresponding crypto map entry. Using the **deny** keyword prevents traffic from being protected by crypto IPSec in the context of that particular crypto map entry. (In other words, it does not allow the policy as specified in this crypto map entry to be applied to this traffic.) If this traffic is denied in all the crypto map entries for that interface, the traffic is not protected by crypto IPSec.

The crypto access list you define will be applied to an interface after you define the corresponding crypto map entry and apply the crypto map set to the interface. Different access lists must be used in different entries of the same crypto map set. However, both inbound and outbound traffic will be evaluated against the same "outbound" IPSec access list. Therefore, the access list's criteria are applied in the forward direction to traffic exiting your PIX Firewall, and the reverse direction to traffic entering your PIX Firewall. In Figure 4-1, IPSec protection is applied to traffic between Host 10.0.0.1 and Host 20.0.0.2 as the data exits PIX Firewall A's outside interface en route to Host 20.0.0.2. For traffic from Host 10.0.0.1 to Host 20.0.0.2, the access list entry on PIX Firewall A is evaluated as follows:

source = host 10.0.0.1

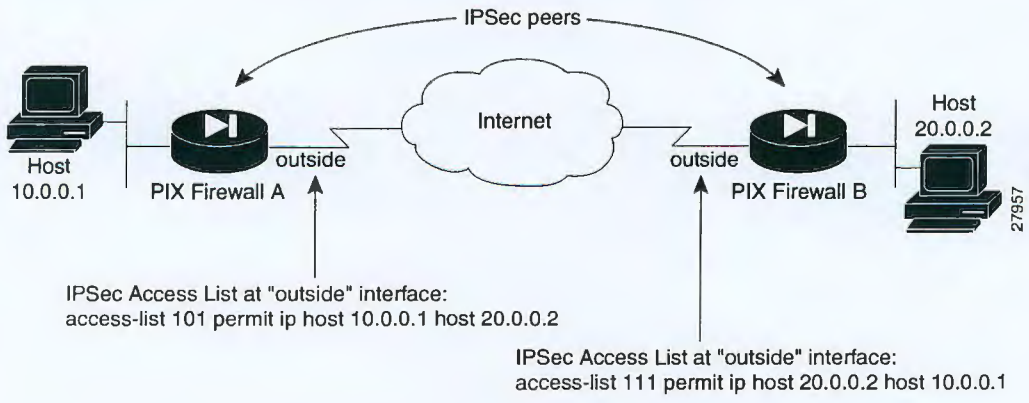
dest = host 20.0.0.2

For traffic from Host 20.0.0.2 to Host 10.0.0.1, that same access list entry on PIX Firewall A is evaluated as follows:

source = host 20.0.0.2

dest = host 10.0.0.1

Figure 4-1 How Crypto Access Lists Are Applied for Processing IPSec



Traffic exchanged between hosts 10.0.0.1 and 20.0.0.2
is protected between PIX Firewall A "outside" and PIX Firewall B "outside"

If you configure multiple statements for a given crypto access list that is used for IPSec, in general the first permit statement that is matched will be the statement used to determine the scope of the IPSec security association. That is, the IPSec security association will be set up to protect traffic that

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 322
Doc 3702

meets the criteria of the matched statement only. Later, if traffic matches a different permit statement of the crypto access list, a new, separate IPSec security association will be negotiated to protect traffic matching the newly matched access list statement.

Note Access lists for crypto map entries tagged as ipsec-manual are restricted to a single permit entry and subsequent entries are ignored. In other words, the security associations established by that particular crypto map entry are only for a single data flow. To support multiple manually established security associations for different kinds of traffic, define multiple crypto access lists, and apply each one to a separate ipsec-manual crypto map entry. Each access list should include one permit statement defining what traffic to protect.

Any unprotected inbound traffic that matches a permit entry in the crypto access list for a crypto map entry flagged as IPSec will be dropped because this traffic was expected to be protected by IPSec.

Note If you clear or delete the last element from an access list, the crypto map references to the destroyed access list are also removed.

Note If you modify an access list that is currently referenced by one or more crypto map entries, the run-time security association database will need to be re initialized using the **crypto map interface** command. See the **crypto ipsec** command page for information on the **crypto map interface** command.

Mirror Image Crypto Access Lists at each IPSec Peer

Cisco recommends that for every crypto access list specified for a static crypto map entry that you define at the local peer, you define a "mirror image" crypto access list at the remote peer. This ensures that traffic that has IPSec protection applied locally can be processed correctly at the remote peer. (The crypto map entries themselves must also support common transforms and must refer to the other system as a peer.)

any Keyword in Crypto Access Lists

When you create crypto access lists, using the **any** keyword could cause problems. Cisco discourages the use of the **any** keyword to specify source or destination addresses.

The **permit any any** statement is strongly discouraged, as this will cause all outbound traffic to be protected (and all protected traffic sent to the peer specified in the corresponding crypto map entry) and will require protection for all inbound traffic. Then, all inbound packets that lack IPSec protection will be silently dropped.

You need to be sure you define which packets to protect. If you must use the **any** keyword in a **permit** statement, you must preface that statement with a series of **deny** statements to filter out any traffic (that would otherwise fall within that **permit** statement) that you do not want to be protected.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 323
Doc. 3702

Transform Sets

A transform set represents a certain combination of security protocols and algorithms. During the IPSec security association negotiation, the peers agree to use a particular transform set for protecting a particular data flow.

You can specify multiple transform sets, and then specify one or more of these transform sets in a crypto map entry. The transform set defined in the crypto map entry will be used in the IPSec security association negotiation to protect the data flows specified by that crypto map entry's access list.

During IPSec security association negotiations with IKE, the peers search for a transform set that is the same at both peers. When such a transform set is found, it is selected and will be applied to the protected traffic as part of both peers' IPSec security associations.

With manually established security associations, there is no negotiation with the peer, so both sides must specify the same transform set.

If you change a transform set definition, the change is only applied to crypto map entries that reference the transform set. The change will not be applied to existing security associations, but will be used in subsequent negotiations to establish new security associations. If you want the new settings to take effect sooner, you can clear all or part of the security association database by using the **clear crypto sa** command.

Selecting Appropriate Transforms

Choosing IPSec transforms combination can be complex. The following tips may help you select transforms that are appropriate for your situation. If you want to:

- provide data confidentiality, include an ESP encryption transform.
  Also consider including an ESP authentication transform or an AH transform to provide authentication services for the transform set.
- ensure data authentication for the outer IP header as well as the data, include an AH transform.
- ensure data authentication (using either ESP or AH) you can choose from the MD5 or SHA (HMAC keyed hash variants) authentication algorithms. The SHA algorithm is generally considered stronger than MD5, but it is slower.

Note Some transforms may not be supported by the peer.

Suggested transform combinations:

- esp-3des and esp-sha-hmac
- esp-des and esp-sha-hmac

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 324
Doc 3702

Crypto Map Entries

To create crypto map entries, follow the guidelines described in this section:

- About Crypto Maps
- Load Sharing
- How Many Crypto Maps Should You Create?
- Manual Security Associations (Using Pre-shared Keys)
- IKE Security Associations
- Dynamic Crypto Maps

About Crypto Maps

Crypto maps specify IPSec policy. Crypto map entries created for IPSec pull together the various parts used to set up IPSec security associations, including:

- Which traffic should be protected by IPSec (per a crypto access list)
- Where IPSec-protected traffic should be sent (who the peer is)
- The local address to be used for the IPSec traffic (See the "Apply Crypto Map Sets to Interface" section for more details.)
- What IPSec security should be applied to this traffic (selecting from a list of one or more transform sets)
- Whether security associations are manually established or are established via IKE
- Other parameters that might be necessary to define an IPSec SA

Crypto map entries with the same crypto map name (but different map sequence numbers) are grouped into a crypto map set. Later, you will apply these crypto map sets to interfaces; then, all IP traffic passing through the interface is evaluated against the applied crypto map set. If a crypto map entry sees outbound IP traffic that should be protected and the crypto map specifies the use of IKE, a security association is negotiated with the peer according to the parameters included in the crypto map entry; otherwise, if the crypto map entry specifies the use of manual security associations, a security association should have already been established via configuration. (If a dynamic crypto map entry sees outbound traffic that should be protected and no security association exists, the packet is dropped.)

The policy described in the crypto map entries is used during the negotiation of security associations. If the local PIX Firewall initiates the negotiation, it will use the policy specified in the static crypto map entries to create the offer to be sent to the specified peer. If the peer initiates the negotiation, the PIX Firewall will check the policy from the static crypto map entries, as well as any referenced dynamic crypto map entries to decide whether to accept or reject the peer's request (offer).

For IPSec to succeed between two peers, both peers' crypto map entries must contain compatible configuration statements.

When two peers try to establish a security association, they must each have at least one crypto map entry that is compatible with one of the other peer's crypto map entries. For two crypto map entries to be compatible, they must at a minimum meet the following criteria:

- The crypto map entries must contain compatible crypto access lists (for example, mirror image access lists). In the case where the responding peer is using dynamic crypto maps, the entries in the PIX Firewall crypto access list must be "permitted" by the peer's crypto access list.

16345
2
ROS nº 03/2005 - Fl
CPMI - CORR
Fls. Nº 325
Doc 3702

- The crypto map entries must each identify the other peer (unless the responding peer is using dynamic crypto maps).
- The crypto map entries must have at least one transform set in common.

Load Sharing

You can define multiple peers by using crypto maps to allow for load sharing. If one peer fails, there will still be a protected path. The peer that packets are actually sent to is determined by the last peer that the PIX Firewall heard from (received either traffic or a negotiation request from) for a given data flow. If the attempt fails with the first peer, IKE tries the next peer on the crypto map list.

If you are not sure how to configure each crypto map parameter to guarantee compatibility with other peers, you might consider configuring dynamic crypto maps as described in the section "Dynamic Crypto Maps." Dynamic crypto maps are useful when the establishment of the IPSec tunnels is initiated by the peer. They are not useful if the establishment of the IPSec tunnels is locally initiated, because the dynamic crypto maps are policy templates, not complete statements of policy. (Although the access lists in any referenced dynamic crypto map entry are used for crypto packet filtering.)

How Many Crypto Maps Should You Create?

You can apply only one crypto map set to a single interface. The crypto map set can include a combination of IPSec/IKE and IPSec/manual entries.

Note The PIX Firewall currently only supports IPSec on the outside interface. Although the PIX Firewall currently can simulate the Private Link inside termination with the use of the **sysopt ipsec pl-compatible** command, the termination on the inside interface is not a true termination. The use of the **sysopt ipsec pl-compatible** command allows IPSec packets to bypass the NAT and ASA features, and enables incoming IPSec packets to terminate on the inside interface only after initially terminating on the outside interface. For more information on the **sysopt ipsec pl-compatible** command, see the **sysopt** command page within Chapter 6, "Command Reference."

If you create more than one crypto map entry on the outside interface, use the seq-num of each map entry to rank the map entries: the lower the seq-num, the higher the priority. At the interface that has the crypto map set, traffic is evaluated against higher priority map entries first.

You must create multiple crypto map entries for the PIX Firewall's outside interface, if any of the following conditions exist:

- If different data flows are to be handled by separate peers.
- If you want to apply different IPSec security to different types of traffic (to the same or separate peers); for example, if you want traffic between one set of subnets to be authenticated, and traffic between another set of subnets to be both authenticated and encrypted. In this case the different types of traffic should have been defined in two separate access lists, and you must create a separate crypto map entry for each crypto access list.
- If you are not using IKE to establish a particular set of security associations, and want to specify multiple access list entries, you must create separate access lists (one per permit entry) and specify a separate crypto map entry for each access list.

ROS nº 03/2005 - CPMI - CORREIOS
Fls. Nº 326
3702

Manual Security Associations (Using Pre-shared Keys)

The use of manual security associations is a result of a prior arrangement between the users of the PIX Firewall and its peer. There is no negotiation of security associations, so the configuration information in both systems must be the same for traffic to be processed successfully by IPSec.

The PIX Firewall can simultaneously support manual and IKE-established security associations, even within a single crypto map set.

IKE Security Associations

When IKE is used to establish security associations, the peers can negotiate the settings they will use for the new security associations. This means that you can specify lists (such as lists of acceptable transforms) within the crypto map entry.

Dynamic Crypto Maps

Dynamic crypto maps (this requires IKE) can ease IPSec configuration and are recommended for use with networks where the peers are not always predetermined. An example of this is mobile users, who obtain dynamically assigned IP addresses. First, the mobile clients need to authenticate themselves to the local PIX Firewall IKE by something other than an IP address, such as a fully qualified domain name. Once authenticated, the security association request can be processed against a dynamic crypto map that is set up to accept requests (matching the specified local policy) from previously unknown peers.

Dynamic crypto maps are only available for use by IKE.

A dynamic crypto map entry is essentially a crypto map entry without all the parameters configured. It acts as a policy template where the missing parameters are later dynamically configured (as the result of an IPSec negotiation) to match a peer's requirements. This allows peers to exchange IPSec traffic with the PIX Firewall even if the PIX Firewall does not have a crypto map entry specifically configured to meet all the peer's requirements.

Note Only the transform-set field is required to be configured within each dynamic crypto map entry.

Dynamic crypto maps are not used by the PIX Firewall to initiate new IPSec security associations with peers. Dynamic crypto maps are used when a peer tries to initiate an IPSec security association with the PIX Firewall. Dynamic crypto maps are also used in evaluating traffic.

A dynamic crypto map set is included by reference as part of a crypto map set. Any crypto map entries that reference dynamic crypto map sets should be the lowest priority crypto map entries in the crypto map set (that is, have the highest sequence numbers) so that the other crypto map entries are evaluated first; that way, the dynamic crypto map set is examined only when the other (static) map entries are not successfully matched.

If the PIX Firewall accepts the peer's request, at the point that it installs the new IPSec security associations it also installs a temporary crypto map entry. This entry is filled in with the results of the negotiation. At this point, the PIX Firewall performs normal processing, using this temporary crypto map entry as a normal entry, even requesting new security associations if the current ones are expiring (based upon the policy specified in the temporary crypto map entry). Once the flow expires (that is, all the corresponding security associations expire), the temporary crypto map entry is then removed.

ECT nº 03/2005 - DN
CPMI - CORREIOS
Fls. Nº 327
Doc 3702

For both static and dynamic crypto maps, if unprotected inbound traffic matches a permit statement in an access list, and the corresponding crypto map entry is tagged as "IPSec," the traffic is dropped because it is not IPSec protected. (This is because the security policy as specified by the crypto map entry states that this traffic must be IPSec protected.)

For static crypto map entries, if outbound traffic matches a permit statement in an access list and the corresponding security association is not yet established, the PIX Firewall will initiate new security associations with the peer. In the case of dynamic crypto map entries, if no security association existed, the traffic would simply be dropped (because dynamic crypto maps are not used for initiating new security associations).

Note Use care when using the **any** keyword in **permit** entries in dynamic crypto maps. If it is possible for the traffic covered by such a **permit** entry to include multicast or broadcast traffic, the access list should include deny entries for the appropriate address range. Access lists should also include **deny** entries for network and subnet broadcast traffic, and for any other traffic that should not be IPSec protected.

Dynamic Crypto Map Set

Dynamic crypto map entries, like regular static crypto map entries, are grouped into sets. A set is a group of dynamic crypto map entries all with the same dynamic-map-name but each with a different dynamic-seq-num.

If this is configured, the data flow identity proposed by the IPSec peer must fall within a **permit** statement for this crypto access list.

If this is not configured, the PIX Firewall will accept any data flow identity proposed by the peer.

Care must be taken if the **any** keyword is used in the access list, because the access list is used for packet filtering, as well as for negotiation.

Dynamic crypto map entries specify crypto access lists that limit traffic for which IPSec security associations can be established. A dynamic crypto map entry that does not specify an access list will be ignored during traffic filtering. If there is only one dynamic crypto map entry in the crypto map set, it must specify acceptable transform sets.

Add the Dynamic Crypto Map Set into a Regular (Static) Crypto Map Set

You can add one or more dynamic crypto map sets into a crypto map set via crypto map entries that reference the dynamic crypto map sets. You should set the crypto map entries referencing dynamic maps to be the lowest priority entries in a crypto map set (that is, use the highest sequence numbers).

ROS nº 03/2005 - CVM
Fls Nº 328
Nº Doc. 3702

Apply Crypto Map Sets to Interface

You need to apply a crypto map set to each interface through which IPSec traffic will flow. Currently the PIX Firewall only supports IPSec on the outside interface. Applying the crypto map set to an interface instructs the PIX Firewall to evaluate all the interface's traffic against the crypto map set and to use the specified policy during connection or security association negotiation on behalf of traffic to be protected by crypto IPSec.

Note Although the PIX Firewall currently can simulate the Private Link inside termination with the use of the **sysopt ipsec pl-compatible** command, the termination on the inside interface is not a true termination. For more information on the **sysopt ipsec pl-compatible** command, see the **sysopt** command page within Chapter 6, "Command Reference."

Note Binding a crypto map to the outside interface will also initialize the run-time data structures, such as the security association database and the security policy database. If the crypto map is modified in any significant manner, reapplying the crypto map to the outside interface will resynchronize the various run-time data structures with the crypto map configuration.

Monitor and Maintain IPSec

Certain configuration changes will only take effect when negotiating subsequent security associations. If you want the new settings to take immediate effect, you must clear the existing security associations so that they will be re-established with the changed configuration. For manually established security associations, you must clear and reinitialize the security associations or the changes will never take effect. If the PIX Firewall is actively processing IPSec traffic, it is desirable to clear only the portion of the security association database that would be affected by the configuration changes (that is, clear only the security associations established by a given crypto map set). Clearing the full security association database should be reserved for large-scale changes, or when the PIX Firewall is processing very little other IPSec traffic.

To clear (and reinitialize) IPSec security associations, use one of the following commands in the configuration mode:

Command	Purpose
crypto map *map-name* **interface** *interface-name*	Reinitalize the IPSec run-time security association database and security policy database.
clear crypto sa or **clear crypto sa peer** *ip-address* | *peer-name* or **clear crypto sa map** *map-name* or **clear crypto sa entry** *destination-address protocol spi*	Clear IPSec security associations. **Note** Using the **clear crypto sa** command without parameters will clear out the full security association database, which will clear out active security sessions. You may also specify the **peer**, **map**, or **entry** keywords to clear out only a subset of the security association database. For more information, see the **clear crypto sa** command within Chapter 6, "Command Reference."

RGS nº 03/2005 - CPMI - CORREIOS
Fls. Nº 329
Doc 3702

To view information about your IPSec configuration, use one or more of the following commands in EXEC mode:

Command	Purpose
show crypto ipsec transform-set	View your transform set configuration.
show crypto map [interface *interface-name* **| tag** *map-name*]	View your crypto map configuration.
show crypto ipsec sa [map *map-name* **| address | identity] [detail]**	View information about IPSec security associations.
show crypto dynamic-map [tag *map-name*]	View information about dynamic crypto maps.
show crypto ipsec security-association lifetime	View global security association lifetime values.

Configuring IPSec

This section provides procedures to configure IPSec where IPSec security associations will be established via IKE or pre-shared keys (without IKE). See "Configuring IPSec with IKE" to configure IPSec with IKE. Otherwise, see "Configuring Manual IPSec."

Configuring IPSec with IKE

The following steps cover minimal IPSec configuration where the IPSec security associations will be established via IKE.

Step 1 Create an access list to define the traffic to protect:

```
access-list access-list-name {deny | permit} ip source source-netmask destination destination-netmask
```

For example:

```
access-list 101 permit ip 10.0.0.0 255.255.255.0 10.1.1.0 255.255.255.0
```

In the above example, the **permit** keyword causes all traffic that matches the specified conditions to be protected by crypto.

Step 2 Configure a transform set that defines how the traffic will be protected. You can configure multiple transform sets, and then specify one or more of these transform sets in a crypto map entry (Step 3d).

```
crypto ipsec transform-set transform-set-name transform1 [transform2, transform3]
```

For example:

```
crypto ipsec transform-set myset1 esp-des esp-sha-hmac
crypto ipsec transform-set myset2 ah-sha-hmac esp-3des esp-sha-hmac
```

In this example, "myset1" and "myset2" are the names of the transform sets. "myset1" has two transforms defined, while "myset2" has three transforms defined.

Step 3 Create a crypto map entry by performing the following steps:

(a) Create a crypto map entry in IPSec ISAKMP mode:

```
crypto map map-name seq-num ipsec-isakmp
```

For example:

```
crypto map mymap 10 ipsec-isakmp
```


ROS nº 03/2005 CPMI
Fls. Nº 330
3702
Doc

"mymap" is the name of the crypto map set. The map set's sequence number is 10, which is used to rank multiple entries within one crypto map set. The lower the sequence number, the higher the priority.

(b) Assign an access list to a crypto map entry:

```
crypto map map-name seq-num match address access-list name
```

For example:

```
crypto map mymap 10 match address 101
```

In the example, access-list 101 is assigned to crypto map "mymap."

(c) Specify the peer to which the IPSec protected traffic can be forwarded:

```
crypto map map-name seq-num set peer ip-address
```

For example:

```
crypto map mymap 10 set peer 192.168.1.100
```

The security association will be set up with the peer having an IP address of 192.168.1.100. Specify multiple peers by repeating this command.

(d) Specify which transform sets are allowed for this crypto map entry. List multiple transform sets in order of priority (highest priority first). You can specify up to six transform sets.

```
crypto map map-name seq-num set transform-set transform-set-name1
[transform-set-name2, …transform-set-name6]
```

For example:

```
crypto map mymap 10 set transform-set myset1 myset2
```

In this example, when traffic matches access list 101, the security association can use either "myset1" (first priority) or "myset2" (second priority) depending on which transform set matches the peer's transform set.

(e) (Optional) Specify security association lifetime for the crypto map entry, if you want the security associations for this entry to be negotiated using different IPsec security association lifetimes other than the global lifetimes.

```
crypto map map-name seq-num set security-association lifetime {seconds
seconds | kilobytes kilobytes}
```

For example:

```
crypto map mymap 10 set security-association lifetime seconds 2700
```

This example shortens the timed lifetime for the crypto map "mymap 10" to 2,700 seconds (45 minutes). The traffic volume lifetime is not change.

(f) (Optional) Specify that IPSec should ask for perfect forward secrecy (PFS) when requesting new security associations for this crypto map entry, or should require PFS in requests received from the peer:

```
crypto map map-name seq-num set pfs [group1|group2]
```

For example:

```
crypto map mymap 10 set pfs group2
```

This example specifies that PFS should be used whenever a new security association is negotiated for the crypto map "mymap 10." The 1024-bit Diffie-Hellman prime modulus group will be used when a new security association is negotiated using the Diffie-Hellman exchange.

POS Nº 03/2005 - DIN CPMI - CORREIOS
Fls Nº 331
Doc 3702

Step 4 (Optional) Create a crypto dynamic map entry by performing the following steps:

(a) Create a dynamic crypto map entry:

```
crypto dynamic-map dynamic-map-name dynamic-seq-num
```

For example:

```
crypto dynamic-map dyn1 10
```

"dyn1" is the name of the dynamic crypto map set. The map set's sequence number is 10.

(b) (Optional) Assign an access list to a dynamic crypto map entry, which determines which traffic should be protected and not protected:

```
crypto dynamic-map dynamic-map-name dynamic-seq-num match address
access-list- name
```

For example:

```
crypto dynamic-map dyn1 10 match address 101
```

In the example, access list 101 is assigned to dynamic crypto map "dyn1."

(c) (Optional) Specify the peer to which the IPSec-protected traffic can be forwarded. This is *rarely* configured in dynamic crypto map entries because dynamic crypto map entries are often used for unknown peers.

```
crypto dynamic-map dynamic-map-name dynamic-seq-num set peer ip-address
```

For example:

```
crypto dynamic-map dyn1 10 set peer 192.168.1.102
```

The security association will be set up with the peer having an IP address of 192.168.1.102. Specify multiple peers by repeating this command.

(d) Specify which transform sets are allowed for this dynamic crypto map entry. List multiple transform sets in order of priority (highest priority first).

```
crypto dynamic-map dynamic-map-name dynamic-seq-num set transform-set
transform-set name1, [transform-set name2, …transform-set name9]
```

For example:

```
crypto dynamic-map dyn 10 set transform-set myset1 myset2
```

In this example, when traffic matches access list 101, the security association can use either "myset1" (first priority) or "myset2" (second priority) depending on which transform set matches the peer's transform sets.

(e) (Optional) Specify security association lifetime for the crypto dynamic map entry, if you want the security associations for this entry to be negotiated using different IPsec security association lifetimes other than the global lifetimes:

```
crypto dynamic-map dynamic-map-name dynamic-seq-num set security-association
lifetime {seconds seconds | kilobytes kilobytes}
```

For example:

```
crypto dynamic-map dyn1 10 set security-association lifetime 2700
```

This example shortens the timed lifetime for dynamic crypto map "dyn1 10" to 2,700 seconds (45 minutes). The time volume lifetime is not changed.

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 332
Doc 3702

(f) (Optional) Specify that IPSec should ask for PFS when requesting new security associations for this dynamic crypto map entry, or should demand PFS in requests received from the peer:

```
crypto dynamic-map dynamic-map-name dynamic-seq-num set pfs [group1 | group2]
```

For example:

```
crypto dynamic-map dyn1 10 set pfs group1
```

(g) Add the dynamic crypto map set into a static crypto map set.

Be sure to set the crypto map entries referencing dynamic maps to be the lowest priority entries (highest sequence numbers) in a crypto map set.

```
crypto map map-name seq-num ipsec-isakmp dynamic dynamic-map-name
```

For example:

```
crypto map mymap 200 ipsec-isakmp dynamic dyn1
```

Step 5 Apply a crypto map set to the outside interface:

```
crypto map map-name interface interface-name
```

For example:

```
crypto map mymap interface outside
```

In this example, the PIX Firewall will evaluate the traffic going through the outside interface against the crypto map "mymap" to determine whether it needs to be protected.

Configuring Manual IPSec

The following procedure covers minimal IPSec configuration where the security associations will be established via pre-shared keys.

Step 1 Create an access list to define the traffic to protect:

```
access-list access-list-name {deny | permit} ip source source-netmask destination destination-netmask
```

For example:

```
access-list 101 permit ip 10.0.0.0 255.255.255.0 10.1.1.0 255.255.255.0
```

In this example, the keyword **permit** causes all traffic that matches the specified conditions to be protected by crypto.

Step 2 Configure a transform set that defines how the traffic will be protected.

You can configure only one transform set for manually established security associations. The peer must also have the same transform set specified.

```
crypto ipsec transform-set transform-set-name transform
```

For example:

```
crypto ipsec transform-set myset3 esp-des esp-sha-hmac
```

In the example, "myset3" is the name of the transform set and two transforms have been defined.

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 333
Doc 3702

Step 3 Create a crypto map entry in IPSec manual mode:

```
crypto map map-name seq-num ipsec-manual
```

For example:

```
crypto map mymaptwo 30 ipsec-manual
```

Step 4 Name an IPSec access list. The access list can specify only one permit entry when you are establishing manual security associations.

```
crypto map map-name seq-num match address access-list name
```

For example:

```
crypto map mymaptwo 30 match address 101
```

Step 5 Specify the peer to which the IPSec protected traffic can be forwarded. Only one peer can be specified when you are establishing manual security associations.

```
crypto map map-name seq-num set peer ip-address
```

For example:

```
crypto map mymaptwo 30 set peer 192.186.1.103
```

Step 6 Specify which transform set should be used. This must be the same transform set that is specified in the peer's corresponding crypto map entry.

```
crypto map map-name seq-num set transform-set transform-set-name
```

For example:

```
crypto map mymaptwo 30 set transform-set myset3
```

Step 7 If the specified transform set includes the AH protocol (authentication via MD5-HMAC or SHA-HMAC), set the AH Security Parameter Index (SPI) and key to apply to inbound protected traffic. If the specified transform set includes only the ESP protocol, skip to Step 9.

```
crypto map map-name seq-num set session-key inbound ah spi hex-key-data
```

For example:

```
crypto map mymaptwo 30 set session-key inbound ah 300
123456789A123456789A123456789A123456789A
```

This specifies the IPSec session key for AH protocol within crypto map "mymaptwo" to be used with the inbound protected traffic.

Step 8 Set the AH SPIs and keys to apply to outbound protected traffic:

```
crypto map map-name seq-num set session-key outbound ah spi hex-key-data
```

For example:

```
crypto map mymaptwo 30 set session-key outbound ah 400
123456789A123456789A123456789A123456789A
```

Step 9 If the specified transform set includes the ESP protocol, set the ESP SPIs and keys to apply to inbound protected traffic. If the transform set includes an ESP cipher algorithm, specify the cipher keys. If the transform set includes an ESP authenticator algorithm, specify the authenticator keys.

```
crypto map map-name seq-num set session-key inbound esp spi cipher hex-key-data
[authenticator hex-key-data]
```

For example:

```
crypto map mymaptwo 30 set session-key inbound esp 300 cipher
123456789012345 authenticator 0000111122223333444455556666777788889999
```


334
Doc. 3702

Step 10 Set the ESP SPIs and keys to apply to inbound protected traffic. If the transform set includes an ESP cipher algorithm, specify the cipher keys. If the transform set includes an ESP authenticator algorithm, specify the authenticator keys.

```
crypto map map-name seq-num set session-key outbound esp spi cipher hex-key-data
[authenticator hex-key-data]
```

For example:

```
crypto map mymaptwo 30 set session-key outbound esp 300 cipher
abcdefghijklmno authenticator 9999888877776666555544443333222211110000
```

Step 11 Apply a crypto map set to the outside interface:

```
crypto map map-name interface interface-name
```

For example:

```
crypto map mymaptwo interface outside
```

In this example, the PIX Firewall will evaluate the traffic going through the outside interface against the "mymaptwo" crypto map to determine whether it needs to be protected.

About IKE

IKE is a key management protocol standard that is used in conjunction with the IPSec standard.

IPSec can be configured without IKE, but IKE enhances IPSec by providing additional features, flexibility, and ease of configuration for the IPSec standard.

IKE is a hybrid protocol, which implements the Oakley key exchange and Skeme key exchange inside the ISAKMP framework. (ISAKMP, Oakley, and Skeme are security protocols implemented by IKE.) IKE automatically negotiates IPSec security associations and enables IPSec secure communications without manual preconfiguration.

Specifically, IKE provides these benefits:

- Eliminates the need to manually specify all the IPSec security parameters in the crypto maps at both peers.
- Allows you to specify a lifetime for the IPSec security association.
- Allows encryption keys to change during IPSec sessions.
- Allows IPSec to provide anti-replay services.
- Permits CA support for a manageable, scalable IPSec implementation.
- Allows dynamic authentication of peers.

This section includes the following topics, which provide background information applicable to the tasks of configuring IKE. The IKE configuration steps are provided in the section "Configuring IKE."

- IKE Policies
- IKE Pre-shared Keys

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 335
Nº 3702 Doc

IKE Policies

You must create IKE policies at each peer. An IKE policy defines a combination of security parameters to be used during IKE negotiation.

To create an IKE policy, follow the guidelines in these topics:

- Why Do You Need to Create These Policies?
- What Parameters Do You Define in a Policy?
- How Do IKE Peers Agree upon a Matching Policy?
- Which Value Should You Select for Each Parameter?
- Creating Policies
- Additional Configuration Required for IKE Policies

Why Do You Need to Create These Policies?

IKE negotiations must be protected, so each IKE negotiation begins by each peer agreeing on a common (shared) IKE policy. This policy states which security parameters will be used to protect subsequent IKE negotiations.

After the two peers agree upon a policy, the security parameters of the policy are identified by a security association established at each peer, and these security associations apply to all subsequent IKE traffic during the negotiation.

You can create multiple, prioritized policies at each peer to ensure that at least one policy will match a remote peer's policy.

What Parameters Do You Define in a Policy?

There are five parameters to define in each IKE policy. These parameters apply to the IKE negotiations when the IKE security association is established. Table 4-1 provides the five IKE policy parameters and their accepted values.

Table 4-1 IKE Policy Parameters

Parameter	Accepted Values	Keyword	Default Value
encryption algorithm	56-bit DES-CBC	des	56-bit DES-CBC
	168-bit Triple DES	3des	
hash algorithm	SHA-1 (HMAC variant)	sha	SHA-1
	MD5 (HMAC variant)	md5	
authentication method	RSA signatures	rsa-sig	RSA signatures
	pre-shared keys	pre-share	
Diffie-Hellman group identifier	768-bit Diffie-Hellman or	1	768-bit Diffie-Hellman
	1024-bit Diffie-Hellman	2	
security association's lifetime	can specify any number of seconds	–	86,400 seconds (one day)

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 336
Doc 3702

How Do IKE Peers Agree upon a Matching Policy?

When the IKE negotiation begins, IKE looks for an IKE policy that is the same on both peers. The peer that initiates the negotiation will send all its policies to the remote peer, and the remote peer will try to find a match. The remote peer looks for a match by comparing its own highest priority policy against the other peer's received policies. The remote peer checks each of its policies in order of its priority (highest priority first) until a match is found.

A match is made when both policies from the two peers contain the same encryption, hash, authentication, and Diffie-Hellman parameter values, and when the remote peer's policy specifies a lifetime less than or equal to the lifetime in the policy being compared. (If the lifetimes are not identical, the shorter lifetime—from the remote peer's policy—will be used.)

If no acceptable match is found, IKE refuses negotiation and IPSec will not be established.

If a match is found, IKE will complete negotiation, and IPSec security associations will be created.

Note Depending on which authentication method is specified in a policy, additional configuration might be required (as described in the section "Additional Configuration Required for IKE Policies"). If a peer's policy does not have the required companion configuration, the peer will not submit the policy when attempting to find a matching policy with the remote peer.

Which Value Should You Select for Each Parameter?

You can select certain values for each parameter, per the IKE standard. But why chose one value over another?

If you are interoperating with a peer that supports only one of the values for a parameter, your choice is limited to the other peer's supported value. Aside from this, there is often a trade-off between security and performance, and many of these parameter values represent such a trade-off. You should evaluate the level of your network's security risks and your tolerance for these risks. Then the following tips might help you select which value to specify for each parameter.

- The encryption algorithm has two options: 56-bit DES and 168-bit triple DES.
- The hash algorithm has two options: SHA-1 and MD5.

  MD5 has a smaller digest and is considered to be slightly faster than SHA-1. There has been a demonstrated successful (but extremely difficult) attack against MD5; however, the HMAC variant used by IKE prevents this attack.
- The authentication method has two options: RSA signatures and pre-shared keys.

  RSA signatures provide non-repudiation for the IKE negotiation (you can prove to a third party after the fact that you had an IKE negotiation with a specific peer).

  RSA signatures requires use of a CA. Using a CA can dramatically improve the manageability and scalability of your IPSec network.

  Pre-shared keys are clumsy to use if your secured network is large, and do not scale well with a growing network. However, they do not require use of a CA, as do RSA signatures, and might be easier to set up in a small network with fewer than 10 nodes.
- The Diffie-Hellman group identifier has two options: 768-bit or 1024-bit Diffie-Hellman.

  1024-bit Diffie-Hellman is more secure than the 768-bit Diffie-Hellman, but requires more CPU time to execute.
- The SA's lifetime can be set to any value.

ECT nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 337
Doc 3702

As a general rule, the shorter the lifetime (up to a point), the more secure your IKE negotiations will be. However, with longer lifetimes, future IPSec security associations can be set up more quickly.

Creating Policies

You can create multiple IKE policies, each with a different combination of parameter values. For each policy that you create, you assign a unique priority (1 through 65,534, with 1 being the highest priority).

You can configure multiple policies on each peer—but at least one of these policies must contain exactly the same encryption, hash, authentication, and Diffie-Hellman parameter values as one of the policies on the remote peer. (The lifetime parameter does not necessarily have to be the same; see details in the section "How Do IKE Peers Agree upon a Matching Policy?")

If you do not configure any policies, your PIX Firewall will use the default policy, which is always set to the lowest priority, and which contains each parameter's default value.

If you do not specify a value for a parameter, the default value is assigned.

Additional Configuration Required for IKE Policies

Depending on which authentication method you specify in your IKE policies, you need to do certain additional configuration before IKE and IPSec can successfully use the IKE policies.

Each authentication method requires additional companion configuration as follows:

- RSA signatures method:

  If you specify RSA signatures as the authentication method in a policy, you must configure the peers to obtain certificates from a CA. (And, of course, the CA must be properly configured to issue the certificates.) Configure this certificate support as described in the section "Configuring CA."

  The certificates are used by each peer to securely exchange public keys. (RSA signatures require that each peer has the remote peer's public signature key.) When both peers have valid certificates, they will automatically exchange public keys with each other as part of any IKE negotiation in which RSA signatures are used.

- Pre-shared keys authentication method:

  If you specify pre-shared keys as the authentication method in a policy, you must configure these pre-shared keys as described in "Configuring Pre-shared (Authentication) Keys Manually."

IKE Pre-shared Keys

To configure pre-shared keys, perform one or both of the following tasks at each peer that uses pre-shared keys in an IKE policy. See "Configuring Pre-shared (Authentication) Keys Manually" for the procedure that tells you how to configure pre-shared keys.

- You will need to set each peer's ISAKMP identity, if its identity is to be set to hostname. Each peer's identity is set either to its host name or its IP address. When two peers use IKE to establish IPSec security associations, each peer sends its identity to its peer.

  By default, a peer's identity is its IP address. If appropriate, you could change the identity to be the peer's host name instead. As a general rule, set all peers' identities the same way—either all peers should use their IP addresses or all peers should use their host names. If some peers use

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 338
Nº 3702 Doc

their host names and some peers use their IP addresses to identify themselves to one another, IKE negotiations could fail if a peer's identity is not recognized and a DNS lookup is unable to resolve the identity.

- Specify the shared keys at each peer. A given pre-shared key is shared between two peers. At a given peer you could specify the same key to share with multiple peers; however, a more secure approach is to specify different keys to share between different pairs of peers.

Configuring IKE

This section provides the procedures to enable and configure IKE. It also provides a procedure to disable IKE, if you choose not use it with your IPSec implementation.

The following topics are included in this section:

- Enabling and Configuring IKE
- Configuring Pre-shared (Authentication) Keys Manually
- Disabling IKE

Enabling and Configuring IKE

To enable and configure IKE, perform the following steps:

Step 1 Enable IKE on the outside interface:

```
isakmp enable interface-name
```

For example:

```
isakmp enable outside
```

Step 2 Configure the IKE policies by performing the following steps:

Note If you enter a default value for a given policy parameter, it will not be written in the configuration. If you do not specify a value for a given policy parameter, the default value is assigned.

(a) Identify the policy to create. Each policy is uniquely identified by the priority number you assign.

```
isakmp policy priority
```

For example:

```
isakmp policy 20 …
```

(b) Specify the encryption algorithm:

```
isakmp policy priority encryption des|3des
```

For example:

```
isakmp policy 20 encryption des
```

(c) Specify the hash algorithm:

```
isakmp policy priority hash md5|sha
```


ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 339
Doc 3702

For example:

```
isakmp policy 20 hash md5
```

(d) Specify the authentication method:

```
isakmp policy priority authentication pre-share|rsa-sig
```

For example:

```
isakmp policy 20 authentication rsa-sig
```

Note If you specify the authentication method of pre-shared keys, you are required to manually configure these keys. See "Configuring Pre-shared (Authentication) Keys Manually."

(e) Specify the Diffie-Hellman group identifier:

```
isakmp policy priority group 1|2
```

For example:

```
isakmp policy 20 group 2
```

(f) Specify the security association's lifetime:

```
isakmp policy priority lifetime seconds
```

For example:

```
isakmp policy 20 lifetime 5000
```

The following example shows two policies with policy 20 as the highest priority, policy 30 as the next priority, and the existing default policy as the lowest priority:

```
isakmp policy 20 encryption des
isakmp policy 20 hash md5
isakmp policy 20 authentication rsa-sig
isakmp policy 20 group 2
isakmp policy 20 lifetime 5000

isakmp policy 30 authentication pre-share
isakmp policy 30 lifetime 10000
```

In this example, the encryption des of policy 20 would not appear in the written configuration because this is the default for the encryption algorithm parameter.

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 340
Doc 3702

Step 3 (Optional) View all existing IKE policies:

```
show isakmp policy
```

The following is an example of the output after the policies 20 and 30 in the previous example were configured:

```
Protection suite priority 20
        encryption algorithm:   DES - Data Encryption Standard (56 bit keys)
        hash algorithm: Message Digest 5
        authentication method:  Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:   #2 (1024 bit)
        lifetime:       5000 seconds, no volume limit
Protection suite priority 30
        encryption algorithm:   DES - Data Encryption Standard (56 bit keys)
        hash algorithm: Secure Hash Standard
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #1 (768 bit)
        lifetime:       10000 seconds, no volume limit
Default protection suite
        encryption algorithm:   DES - Data Encryption Standard (56 bit keys)
        hash algorithm: Secure Hash Standard
        authentication method:  Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:   #1 (768 bit)
        lifetime:       86400 seconds, no volume limit
```

Note Although the output shows "no volume limit" for the lifetimes, you can currently only configure a time lifetime (such as 86,400 seconds) with IKE; volume limit lifetimes are not currently configurable.

Configuring Pre-shared (Authentication) Keys Manually

If you selected the authentication method of pre-shared keys within Step 2d in the section "Enabling and Configuring IKE," manually configure these keys between the PIX Firewall and its peer(s). To configure these pre-shared keys on the PIX Firewall, perform the following step:

Specify the pre-shared key that the PIX Firewall and its peer will use for authentication and the peer's address:

isakmp key *keystring* **address** *peer-address* [**netmask** *mask*]

For example:

isakmp key *1234567890* **address** *192.168.1.100*

The pre-shared key is 1234567890, and the peer's address is 192.168.1.100

Note Netmask allows you to configure a single key to be shared among multiple peers. You would use the netmask of 0.0.0.0. However, Cisco strongly recommends using a unique key for each peer.

Note The pre-shared key must be configured at both the PIX Firewall and its peer, otherwise the policy cannot be used.

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 341
Doc 3702

Disabling IKE

IKE is enabled in the PIX Firewall by default. If you do not want IKE to be used with your IPSec implementation, disable it.

If you disable IKE, you will have to make these concessions at the peers:

- You must manually specify all the IPSec security associations in the crypto maps at all peers.
- IPSec security associations will never time out for a given IPSec session.
- The encryption keys never change during IPSec sessions between peers.
- Anti-replay services will not be available between the peers.
- CA support cannot be used.

To disable IKE, use the following command:

```
no crypto isakmp enable interface-name
```

For example:

```
no crypto isakmp enable outside
```

About IKE Mode Configuration (Dynamic IP Address Assignment for Cisco Secure VPN Client)

The IKE Mode Configuration allows a gateway (in this case the PIX Firewall) to download an IP address (and other network level configuration) to the client (peer) as part of an IKE negotiation. Using this exchange, the PIX Firewall gives IP addresses to the IKE client to be used as an "inner" IP address encapsulated under IPSec. This provides a known IP address for the client, which can be matched against the IPSec policy.

The following topics are covered in this section to provide background information applicable to the the tasks of configuring the IKE Mode Configuration. The procedure to configure the IKE Mode Configuration is provided in the section "Configuring Dynamic IP Addressing Assignment."

- Benefits
- Types
- Configuration Tasks

Benefits

To implement IPSec VPNs between remote access clients with dynamic IP addresses and a corporate gateway, you have to dynamically administer scalable IPSec policy on the gateway once each client is authenticated. With IKE Mode Configuration, the gateway can set up scalable policy for a very large set of clients irrespective of the IP addresses of those clients.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 342
Doc. 3702

Types

There are two types of IKE Mode Configuration for VPN:

- Gateway initiation—Gateway initiates the configuration mode with the client. Once the client responds, the IKE modifies the sender's identity, the message is processed, and the client receives a response.
- Client initiation—Client initiates the configuration mode with the gateway. The gateway responds with an IP address it has allocated for the client.

Configuration Tasks

The following are the three steps to perform when configuring IKE Mode Configuration on your PIX Firewall. The next section, "Configuring Dynamic IP Addressing Assignment," gives you the procedure.

- Define the pool of IP addresses. Existing local address pools are used to define a set of addresses. Use the **ip local pool** command to define a local address pool. See the **ip** command page within Chapter 6, "Command Reference," for more information about this command.
- Reference the pool of IP addresses in the IKE configuration. Use the **isakmp client configuration address-pool local** command to configure the IP address local pool you defined to reference IKE. See the **isakmp** command page within Chapter 6, "Command Reference," for more information about this command.
- Define which crypto maps should attempt to configure clients, and whether the PIX Firewall or the client initiates the IKE Mode Configuration. Use the **crypto map client-configuration address** command to configure IKE Mode Configuration. See the **crypto map** command page within Chapter 6, "Command Reference," for more information about this command.

Configuring Dynamic IP Addressing Assignment

To configure IKE Mode Configuration on your PIX Firewall, perform the following steps after configuring IKE.

Step 1 Define the pool of IP addresses:

```
ip local pool pool-name start-address-[end-address]
```

For example:

```
ip local pool ire 171.72.1.1-171.72.1.254
```

Step 2 Reference the defined pool of IP addresses in the IKE configuration:

```
isakmp client configuration address-pool local pool-name [interface-name]
```

For example:

```
isakmp client configuration address-pool local ire outside
```

Step 3 Define which crypto maps should attempt to configure clients:

```
crypto map map-name client configuration address initiate|respond
```

For example:

```
crypto map mymap client configuration address initiate
```


ROS nº 03/2005 - CPMI CORREIOS
Fls. Nº 343
Doc 3702

Examples

The following partial configuration shows a PIX Firewall that has been configured to both set IP addresses to clients and respond to IP address requests from clients whose packets arrive on the outside interface using dynamic crypto map without explicitly specifying the peer. The IKE Mode Configuration commands are in bold.

Note The section "VPN Client Access with AAA and Pre-shared Keys" in Chapter 5, "Configuration Examples," provides another example of configuring IKE Mode Configuration.

```
! define the ip address pool
ip local pool ire 171.72.1.1-171.72.1.254
! tie the pool with ike
crypto isakmp client configuration address-pool local ire outside
!
access-list 103 permit ip host 172.21.230.34 172.21.1.0 255.255.255.0
!
crypto ipsec transform-set pc esp-des esp-md5-hmac
!
crypto dynamic-map dyn 10 set transform-set pc
crypto dynamic-map dyn 10 match address 103
! enable address assignment in crypto map
crypto map dyn client configuration address initiate
crypto map dyn client configuration address respond
!
crypto map dyn 10 ipsec-isakmp dynamic dyn
crypto map dyn interface outside
```

About CA

CAs are responsible for managing certificate requests and issuing certificates to participating IPSec network peers. These services provide centralized key management for the participating peers.

CAs simplify the administration of IPSec network devices (peers). You can use a CA with a network containing multiple IPSec-compliant devices, such as with the Cisco Secure PIX Firewalls and Cisco routers.

Digital signatures, enabled by public key cryptography, provide a means to digitally authenticate devices and individual users. In public key cryptography, such as the RSA encryption system, each user has a key-pair containing both a public and a private key. The keys act as complements, and anything encrypted with one of the keys can be decrypted with the other. In simple terms, a signature is formed when data is encrypted with a user's private key. The receiver verifies the signature by decrypting the message with the sender's public key. The fact that the message could be decrypted using the sender's public key indicates that the holder of the private key, the sender, must have created the message. This process relies on the receiver having a copy of the sender's public key and knowing with a high degree of certainty that it really does belong to the sender, and not to someone pretending to be the sender.

Digital certificates provide this link. A digital certificate contains information to identify a user or device, such as the name, serial number, company, department or IP address. It also contains a copy of the entity's public key. The certificate is itself signed by a Certification Authority, a third party that is explicitly trusted by the receiver to validate identities and to create digital certificates.

RQS nº 03/2005 - CN
CPMI
Fls Nº 344
Doc. 3702

In order to validate the CA's signature, the receiver must first know the CA's public key. Normally this is handled out-of-band or through an operation done at installation. For instance, most web browsers are configured with the public keys of several CAs by default. The IKE, a key component of IPSec, can use digital signatures to scaleably authenticate peer devices before setting up security associations.

Without digital signatures, one must either manually exchange public keys or secrets between each pair of peers that use IPSec to protect communications between them. Without certificates, every new peer added to the network requires a configuration change on every other peer it securely communicates with. However, by using digital certificates, each peer is enrolled with a CA. When two peers wish to communicate, they exchange certificates and digitally sign data to authenticate each other. When a new peer is added to the network, one simply enrolls that peer with a CA, and none of the other peers need modification. When the new peer attempts an IPSec connection, certificates are automatically exchanged and the peer can be authenticated.

The following topics are covered in this section to provide background information applicable to the the tasks of configuring for interoperability with a CA. The CA configuration steps are provided in "CA Configuration."

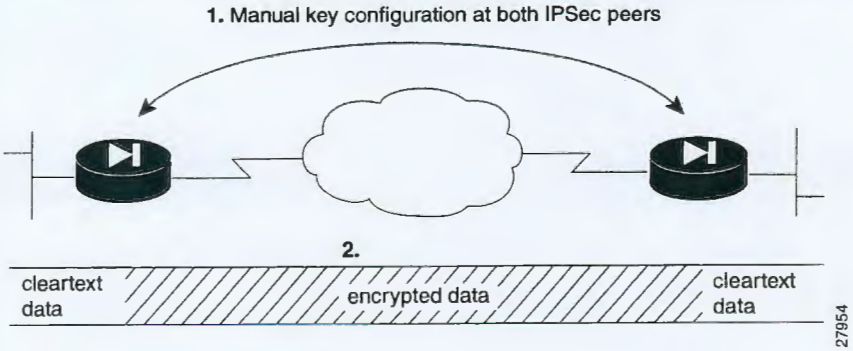
- IPSec without CAs
- IPSec with CAs
- How CA Certificates Are Used by IPSec Peers
- Registration Authorities

IPSec without CAs

Without a CA, if you want to enable IPSec services (such as encryption) between two peers, you must first ensure that each peer has the other's key (such as an RSA public key or a shared key). This requires that you manually perform one of the following at each peer:

- Enter the other peer's RSA public key, or
- Specify a shared key to be used between the two peers.

Figure 4-2 Without a CA: Key Configuration between two IPSec Peers

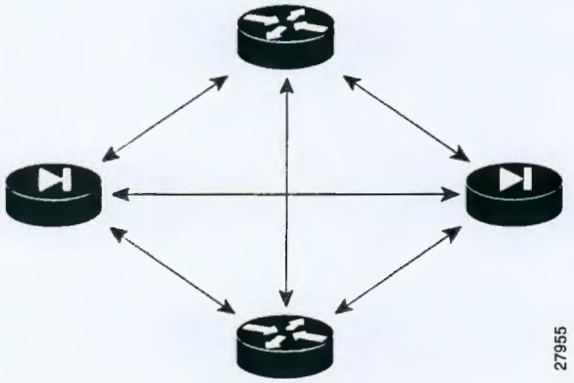


In Figure 4-2, number 1 illustrates how each PIX Firewall uses the other's key to authenticate the identity of the other PIX Firewall; this authentication always occurs whenever IPSec traffic is exchanged between two IPSec peers. Number 2 illustrates encrypted data within an IPSec tunnel between two IPSec peers.

RQS nº 03/2005 - CPMI - CORREIOS
Fls. Nº 345
Doc. 3702

If you have multiple Cisco peers in a mesh topology, and wish to exchange IPSec traffic passing between all of those peers, you must first configure shared keys or RSA public keys between all of those peers:

Figure 4-3 Without a CA: Six 2-Part Key Configurations Required for Four IPSec Peers



Every time a new peer is added to the IPSec network, you must configure keys between the new peer and each of the existing peers. (In Figure 4-3, four additional 2-part key configurations would be required to add a single IPSec peer to the network.)

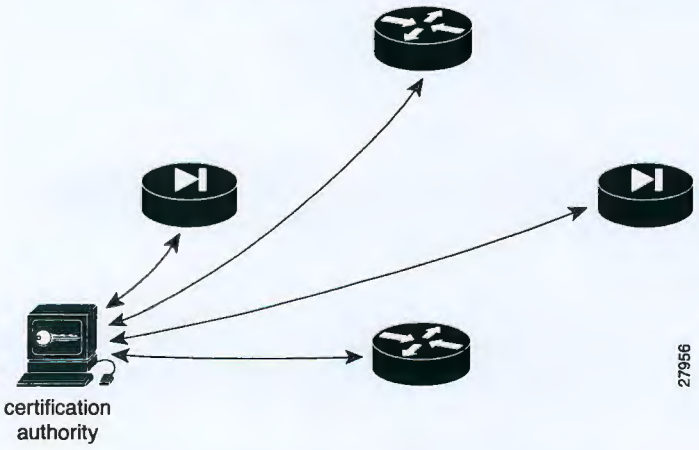
Consequently, the more peers there are that require IPSec services, the more involved the key administration becomes. This approach does not scale well for larger, more complex encrypting networks.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 346
Doc 3702

IPSec with CAs

With a CA, you do not need to configure keys between all of the encrypting devices (peers). Instead, you individually enroll each participating device with the CA, requesting a certificate for the device. When this has been accomplished, each participating device can dynamically authenticate all of the other participating peers. This is illustrated in Figure 4-4.

Figure 4-4 With a CA: Each IPSec Device Individually Makes Request of the CA



To add a new IPSec device to the network, you only need to configure that new device to request a certificate from the CA, instead of making multiple key configurations with all the other existing IPSec peers.

How CA Certificates Are Used by IPSec Peers

When two IPSec peers want to exchange IPSec-protected traffic passing between them, they must first authenticate each other—otherwise, IPSec protection cannot occur. The authentication is done with IKE.

Without a CA, a device authenticates itself to the remote peer using either RSA-encrypted nonces or pre-shared keys. PIX Firewall currently does *not* support RSA-encrypted nonces. Both methods require that keys must have been previously configured between the two peers.

With a CA, a peer authenticates itself to the remote peer by sending a certificate to the remote peer and performing some public key cryptography. Each peer must send its own unique certificate which was issued and validated by the CA. This process works because each peer's certificate encapsulates the peer's public key, each certificate is authenticated by the CA, and all participating peers recognize the CA as an authenticating authority. This is called IKE with an RSA signature.

The peer can continue sending its own certificate for multiple IPSec sessions, and to multiple IPSec peers, until the certificate expires. When its certificate expires, the peer administrator must obtain a new one from the CA.

CAs can also revoke certificates for peers that will no longer participate in IPSec. Revoked certificates are not recognized as valid by other peers. Revoked certificates are listed in a Certificate Revocation List (CRL), which each peer may check before accepting another peer's certificate.

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 347
Doc 3702

Registration Authorities

Some CAs have a Registration Authority (RA) as part of their implementation. An RA is essentially a server that acts as a proxy for the CA so that CA functions can continue when the CA is offline.

Some of the configuration tasks described in this section differ slightly depending on whether your CA supports an RA or not.

Configuring CA

To enable your PIX Firewall to interoperate with a CA and obtain your PIX Firewall certificate(s), complete the following steps:

Note Be sure that the PIX Firewall clock is set to the current time, month, day, and year before configuring CA. Otherwise, the CA may reject or allow certificates based on an incorrect timestamp. Cisco's PKI protocol uses the clock to make sure that a CRL is not expired.

Note You need to have a CA available to your network before you configure CA. The CA must support Cisco's PKI protocol, the certificate enrollment protocol.

Step 1 Configure the PIX Firewall host name:

```
hostname newname
```

For example:

```
hostname mypixfirewall
```

In this example, "mypixfirewall" is the name of a unique host in the domain.

Step 2 Configure the PIX Firewall domain name:

```
domain-name name
```

For example:

```
domain-name example.com
```

Step 3 Generate the PIX Firewall RSA key pair(s):

```
ca generate rsa key key_modulus_size
```

For example:

```
ca generate rsa key 512
```

In this example, one general purpose RSA key pair is to be generated. The other option is to generate two special-purpose keys. The selected size of the key modulus is 512.

Step 4 (Optional) View your RSA key pair(s):

```
show ca mypubkey rsa
```

348

The following is an example of the display after the **show ca mypubkey rsa** command is used:

```
% Key pair was generated at: 15:34:55 Aug 05 1999

Key name: mypixfirewall.example.com
 Usage: General Purpose Key
 Key Data:
  305c300d 06092a86 4886f70d 01010105 00034b00 30480241 00c31f4a ad32f60d
  6e7ed9a2 32883ca9 319a4b30 e7470888 87732e83 c909fb17 fb5cae70 3de738cf
  6e2fd12c 5b3ffa98 8c5adc59 1ec84d78 90bdb53f 2218cfe7 3f020301 0001
```

Step 5 Declare a CA:

ca identity *ca_nickname ca_ipaddress [:ca_script_location] [ldap_ip address]*

For example:

ca identity *myca.example.com 205.139.94.230*

In this example, 205.139.94.230 is the IP address of the CA, which is onsiteipsec.verisign.com. The CA name is myca.example.com.

Note The CA may require a particular name for you to use, such as its domain name.

Note When using VeriSign as your CA, VeriSign assigns the CA name you are to use in your CA configuration.

Step 6 Configure the parameters of communication between the PIX Firewall and the CA:

ca configure *ca_nickname* **ca**|**ra** *retry_period retry_count* [**crloptional**]

For example:

ca configure *myca.example.com* **ca** *1 20* **crloptional**

If the PIX Firewall does not receive a certificate from the CA within 1 minute (default) of sending a certificate request, it will resend the certificate request. The firewall will continue sending a certificate request every 1 minute until a certificate is received or until 20 requests have been sent. With the keyword **crloptional** included within the command statement, other peer's certificates can still be accepted by your firewall even if the CRL is not accessible to your firewall.

Step 7 Authenticate the CA by obtaining its public key and its certificate.

ca authenticate *ca_nickname [fingerprint]*

For example:

ca authenticate *myca.example.com 0123 4567 89AAB CDEF 0123*

The fingerprint (0123 4567 89AAB CDEF 0123 in the example) is optional and is used to authenticate the CA's public key within its certificate. The PIX Firewall will discard the CA certificate if the fingerprint that you included in the command statement is not equal to the fingerprint within the CA's certificate.

You also have the option to manually authenticate the public key by simply comparing the two fingerprints after you receive the CA's certificate rather than entering it within the command statement.

ECT Nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 349
Nº Doc. 3702

Note Depending on the CA you are using, you may need to ask your local CA administrator for this fingerprint.

Step 8 Request signed certificates from your CA for all of your PIX Firewall's RSA key pairs. Before entering this command, contact your CA administrator because he or she will have to authenticate your PIX Firewall manually before granting its certificate(s).

ca enroll *ca_nickname challenge_password [serial] [ipaddress]*

For example:

ca enroll *myca.example.com mypassword1234567*

The keyword mypassword1234567 in the example is a password, which is not saved with the configuration.

Note The password is required in the event your certificate needs to be revoked, so it is crucial that you remember this password. Note it and store it in a safe place.

The **ca enroll** command requests as many certificates as there are RSA key pairs. You will only need to perform this command once, even if you have special usage RSA key pairs.

Note If your PIX Firewall reboots after you issued the **ca enroll** command but before you received the certificate(s), you must reissue the command and notify the CA administrator.

Step 9 Verify that the enrollment process was successful:

show ca certificate

Here is an example of the output of the **show ca certificate** command including a PIX Firewall general purpose certificate and the RA and CA public-key certificates:

```
Subject Name
    Name: mypixfirewall.example.com
IP Address: 192.150.50.110
  Status: Available
  Certificate Serial Number: 36f97573
  Key Usage: General Purpose

RA Signature Certificate
  Status: Available
  Certificate Serial Number: 36f972f4
  Key Usage: Signature

CA Certificate
  Status: Available
  Certificate Serial Number: 36f972e5
  Key Usage: Not Set

RA KeyEncipher Certificate
  Status: Available
  Certificate Serial Number: 36f972f3
  Key Usage: Encryption
```

Step 10 Save your configuration.

```
ca save all
write memory
```


ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 350
Doc 3702

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 351
Doc. 3702

16.322

Segurança Tipo 2 doc 7

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 352
Doc 3702

Configuring Building Blocks

Building Blocks allow you to optimize your configuration. Objects such as hosts, protocols, or services can be grouped, allowing you to issue a single command to every item in the group by using the name of the group.

The Building Blocks feature is used to associate names that can be used in place of corresponding data values in settings and rules. This facilitates ease of maintenance.

For example, an access rule might have a source address of 1.2.3.4. As an alternative, you can use building blocks to create a network object named fred-pc with the address 1.2.3.4. You can then create an access rule with the source address as fred-pc.

Using Building Blocks, you identify objects that will be used on your network, that are configured separately. For example, you can identify the servers used for AAA authentication. The protocols used to connect to those servers, however, are configured in Settings. This design facilitates network updates, as building blocks are defined only once and in one location.

Important Notes About Building Blocks

- You can edit only those objects defined at the current scope.
- Building blocks do not have a one-to-one association.

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 353
Doc 3702

- When an object is selected in the directory tree, all elements defined at the same level and above are applied.
- If you select an object by name and that name is defined at multiple scopes, the version defined nearest the current scope is selected. (See the "Configuring Network Objects" section on page 6-2 for examples using network objects.)

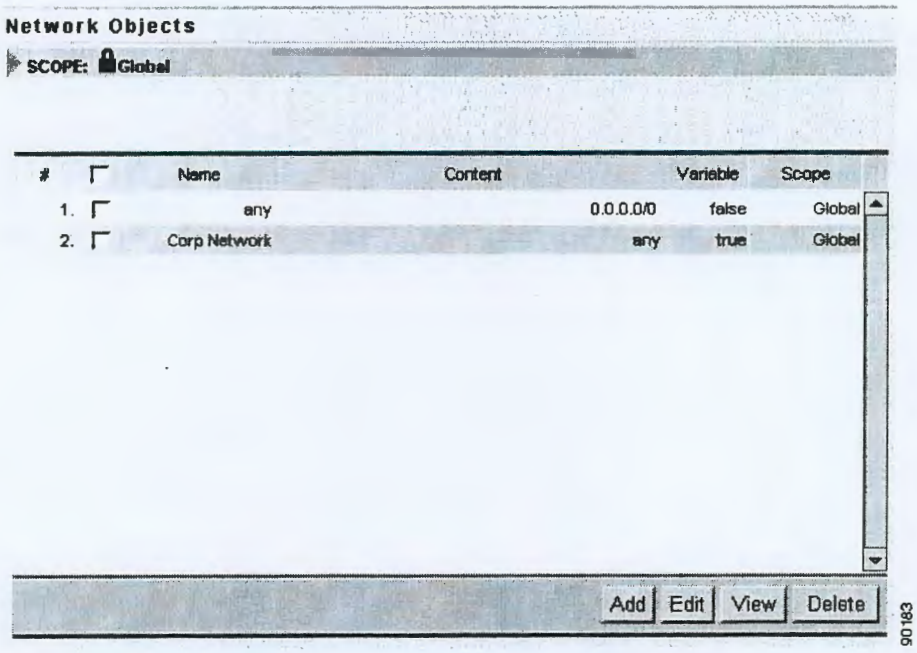
Configuring Network Objects

The Network Objects feature allows you to group a set of network addresses represented by an IP network (name, IP address, IP mask). This information provides the basic identification information for that network. Firewall MC uses the name and IP address–netmask pair to resolve references to the network in the source and destination conditions of access rules and in translation rules. Firewall MC uses the interface value to apply access and translation rules that refer the network to the correct interface. The interface delivers network packets to the network, thus enforcing the rules that refer to that network.

The following examples will help you to better understand how network objects can be used. Let's say you want to create the network object *Corp Network* at the Global scope, but different IP addresses will be used depending on the group being addressed. As a result, you can use a variable, which allows different values to be set for a building block for different devices or groups. The values are substituted into the same rule as applied to those different devices and groups (Figure 6-1).

ECT nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 354
Doc 3702

Figure 6-1 Example 1—Network Object "Corp Network" Defined at the Global Scope with Variable



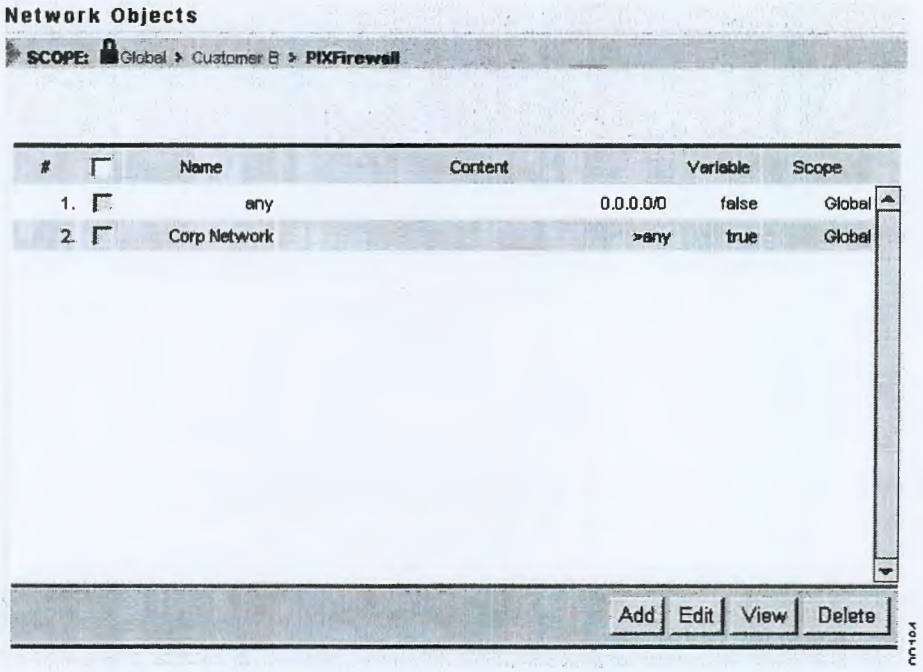
To access the Network Object feature, select **Configuration>Building Blocks>Network Objects**. The Network Objects table defaults to the Global scope. You complete the wizard to define the network object. When you are returned to the Network Objects table, *Corp Network* is shown in the table.

If you select the device *PIX Firewall* using the object selector, then view the Network Objects table for that scope, *Corp Network* is shown as created at the Global scope with the variable setting enabled. (The variable is set to true.) Notice that the check box is grayed-out, which means you cannot make changes at the device level (Figure 6-2).

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 355
Doc 3702

16.518

Figure 6-2 Example 1—Network Object "Corp Network" Shown at the Device Scope

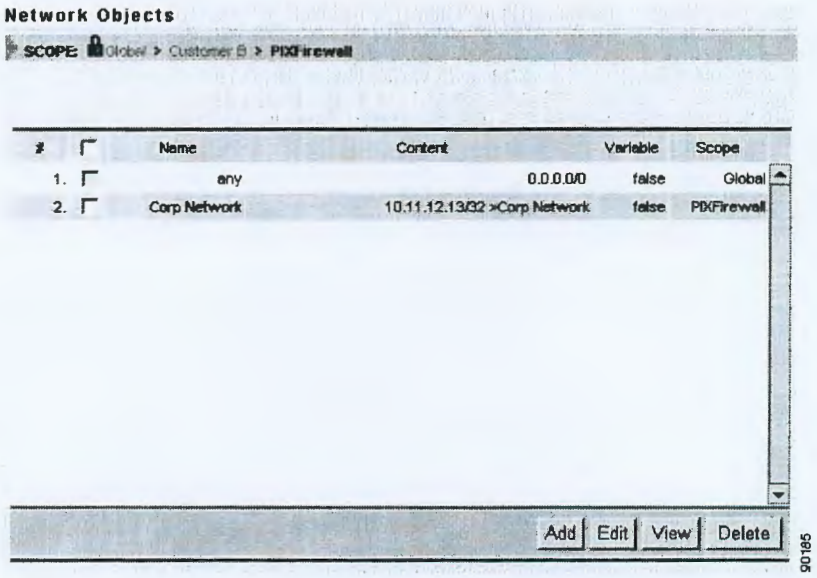


When you define *Corp Network* at the *PIX Firewall* scope, the new network object replaces the one defined at the Global scope and assigns an IP address to it (Figure 6-3). *Corp Network* can now be edited at the device scope; it is no longer shown as a variable. (The variable is set to false.)

RQS nº 03/2005 - CN
CPMI CORREIOS
Fls Nº 356
Doc 3702

16 317

Figure 6-3 Example 1—Network Object "Corp Network" Defined at the Device Scope



To create a mandatory access rule at the Global scope, you can use *Corp Network* as the source address.

If you view the access rules table for the Mandatory Global scope and the Default PIX Firewall scope, you will see the same access rule in each table. When the configuration file for the PIX Firewall is generated, the access rule uses the network object *Corp Network* and the IP address defined at the device level. This is displayed in the configuration file as

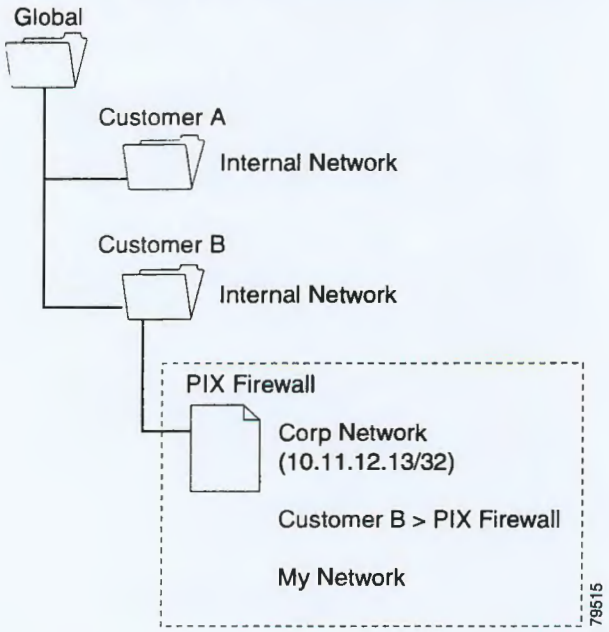
```
: acl_mdc_inside_access Access List

access-list acl_mdc_inside_access permit tcp 10.11.12.13
255.255.255.255 any
```

In conclusion, the network object defined at the Global scope using a variable must be redefined at the device scope with the same name, which then allows it to be used by access rules or translation rules.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 357
Doc 3702

Now consider another example. If you select an object by name and that name is defined at multiple scopes, the version defined nearest the current scope is selected. For this example, assume a service provider has two customers: *Customer A* and *Customer B* (Figure 6-4).

Figure 6-4 Example 2—Network Object Diagram

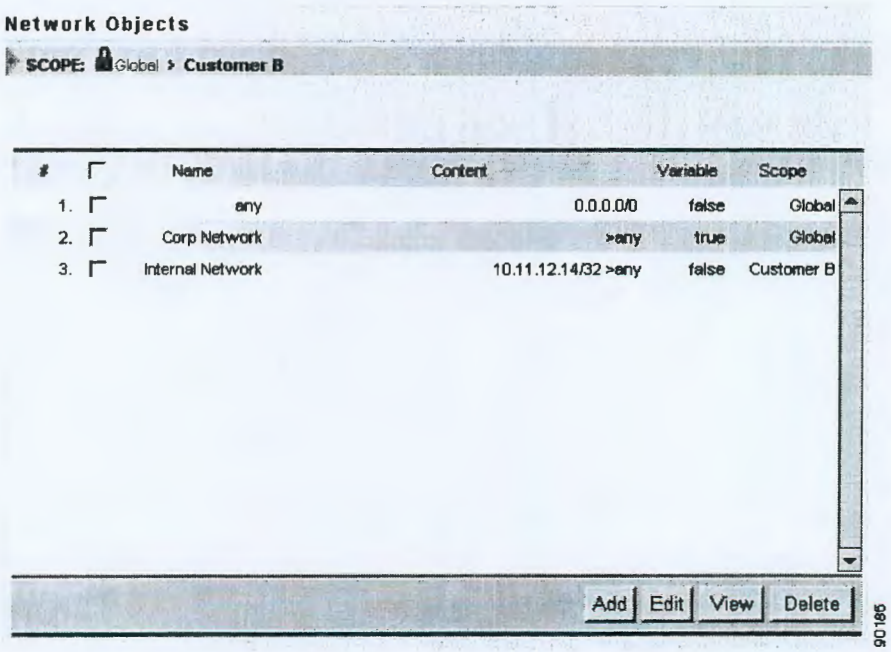


Customers A and B have the network object *Internal Network* defined. Customer B uses a device named *PIX Firewall*. Because *PIX Firewall* is closer to Customer B than Customer A in the navigation tree, the device will use the network object *Internal Network* defined at the *Customer B* scope. When you view the Network Objects table at the device scope, the object name is shown as Customer B>Internal Network.

The Network Object tables used to configure this example are shown in Figure 6-5 through Figure 6-7.

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 358
Nº Doc 3702

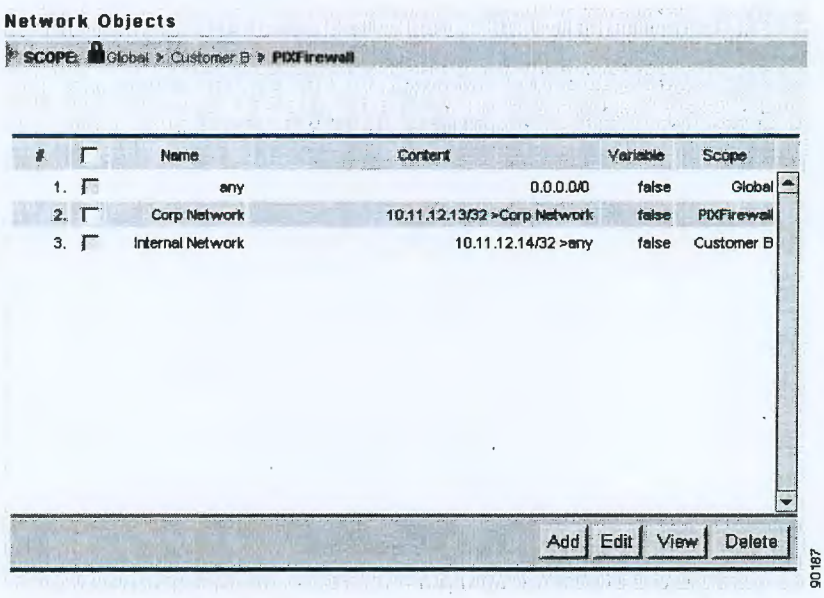
Figure 6-5 Example 2—Network Object "Internal Network" Defined at the Customer B Scope



To access the table in Figure 6-5, you select **Configuration>Building Blocks > Network Objects**. Using the object selector, you select *Customer B*.

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 359
Doc 3702

Figure 6-6 Example 2—Network Object "Internal Network" Shown at the Device Scope



To access the table in Figure 6-6, you select **Configuration>Building Blocks> Network Objects**. Using the object selector, you select *PIX Firewall*.

After you have defined the network object at the device scope, the table displays the updated network object *Internal Network* for the device.

A third example and a standard use of a network object is to define a network object (for example, *My Network)* at the PIX Firewall level. The network object is then used only at the device scope (Figure 6-7).

ROS nº 03/2005 - CPMI - CORREIOS
Fls. Nº 360
Nº 3702 Doc

Figure 6-7 Example 3—Network Object "My Network" Defined at the Device Scope

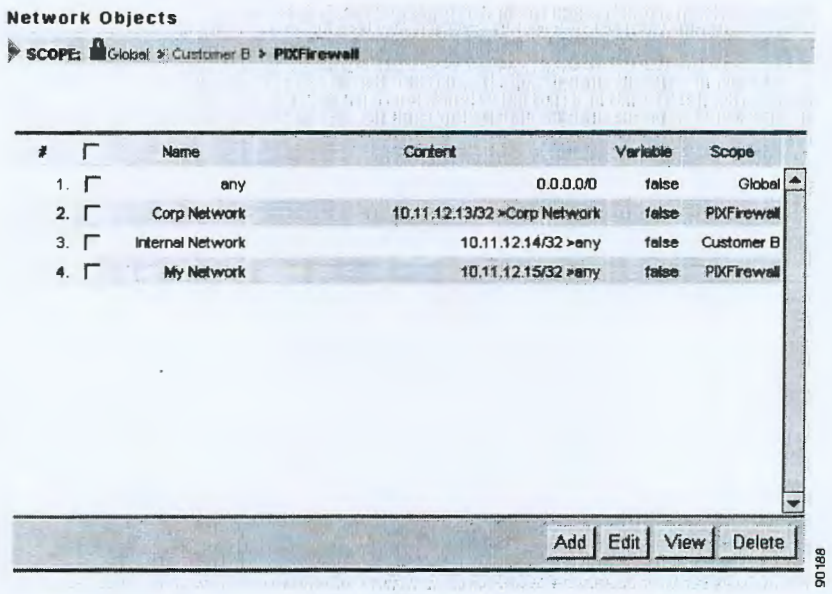


Table 6-1 shows the wizard used to configure network objects with the variable enabled.

Table 6-2 shows the wizard used to configure network objects with the variable disabled.

Table 6-1 Wizard Used to Add or Edit a Network Object (Variable Enabled)

	Wizard Page
Step 1	Enter Definition—Allows you to identify a network object.
Step 2	Summary—Allows you to verify configuration settings before committing settings to the database for deployment.

Table 6-2 Wizard Used to Add or Edit a Network Object (Variable Disabled)

	Wizard Page
Step 1	Enter Definition—Allows you to identify a network object.
Step 2	Enter IPs—Allows you to enter an IP address and mask.
Step 3	Select Network—Allows you to select available objects.
Step 4	Summary—Allows you to verify configuration settings before committing settings to the database for deployment.

Adding or Editing a Network Object

Before You Begin

- If workflow is enabled, select an activity. (See the "Understanding Activity Actions and States" section on page 9-6.)
- Using the Object Selector, select the scope for the devices to configure. (See the "Object Selector" section on page 2-18.)

Step 1 Select **Configuration>Building Blocks>Network Objects**.

The Network Objects page appears.

Step 2 Do one of the following:

- To add a row in the table, click **Add**.

  The Enter Definition page appears.
- To edit a row, select the check box for the row in the table, then click **Edit**.

  The Enter Definition page appears.

Step 3 Enter the network entity name to be assigned to network object.

Step 4 Enter a comment in the Description field.

ROS nº 03/2005 - CN
CPMI CORREIOS
Fls. Nº 362
Nº Doc. 3702

Step 5 Select the Variable check box to use a value in place of a defined building block. For more information, see the online help.

Note This feature allows different values to be set for a building block for different devices or groups; the values are substituted into the same rule as applied to those different devices and groups.

Step 6 Click **Next**.

The Enter IP(s) page appears.

Step 7 Enter the network IP address and mask.

No IP address and mask are needed if you plan to use only nested network objects.

Step 8 Click **Next**.

The Select Networks page appears.

Step 9 Select the available object, then click **Select =>**.

The object is moved to the Selected Objects column.

Step 10 Click **Next**.

The network objects summary page appears.

Step 11 Verify the information is correct, then click **Finish**.

Changes are applied to the assigned firewall device configuration files when they are generated. The configuration files are then downloaded to the firewall devices at deployment. (See Chapter 9, "Managing Activities and Jobs.")

Deleting a Network Object

Before You Begin

Make sure you have the necessary permissions to perform this function. (See Appendix B, "Understanding User Roles and Permissions.")

Step 1 Select **Configuration>Building Blocks>Network Objects**.

The Network Objects page appears.

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 363
Doc 3702

Step 2 Select the check box for the row in the table, then click **Delete**.

You are prompted to confirm the delete request.

Step 3 Click **OK**.

As the page refreshes, you are prompted with another popup window if access rules or translation rules are affected by the deletion. You will need to review the rules tables and make corrections as needed.

Step 4 Click **OK**.

The row is removed from the table, and the information is removed from the assigned firewall device configuration files when they are deployed. (See Chapter 9, "Managing Activities and Jobs.")

Configuring Service Definitions

The Service Definition feature allows you to create a single access rule that controls access to multiple protocols, for example, WWW.

Table 6-3 shows the wizard used to add or edit service definitions.

Table 6-3 Wizard Used to Add or Edit Service Definitions

	Wizard Page
Step 1	Specify Name and Select Transport—Allows you to enter service protocol information.
Step 2	Select ICMP Values—Used to define ICMP only.
Step 3	Summary—Allows you to verify configuration settings before committing settings to the database for deployment.

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 364
Nº Doc 3702

Adding or Editing a Service Definition

Before You Begin

- If workflow is enabled, select an activity. (See the "Understanding Activity Actions and States" section on page 9-6.)
- Using the Object Selector, select the scope for the devices to configure. (See the "Object Selector" section on page 2-18.)

Step 1 Select **Configuration>Building Blocks>Service Definitions**.

The Service Definitions table appears.

Step 2 Do one of the following:

- To add a row in the table, click **Add**.

  The Specify Name and Select Transport page appears.
- To edit a row, select the check box for the row in the table, then click **Edit**.

  The Specify Name and Select Transport page appears.

Step 3 Enter the name of the service.

Step 4 Enter an optional comment in the Description field.

Step 5 Select the transport protocol from the list box, then click **Next**.

Note Only IP requires an IP protocol number.

Step 6 Do one of the following:

- If you selected ICMP as the transport protocol, the select ICMP Values page appears. To select the ICMP values, go to Step 7.
- If you selected TCP or UDP as the transport protocol, the Select TCP/UDP Values page appears. To select the TCP/UDP values, go to Step 8.
- If you selected IP as the transport protocol, enter the IP protocol number, then click **Next**.

  The service descriptions summary page appears. Go to Step 9.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 365
Doc 3702

Step 7 Do the following:

a. Select the type of message from the list box.

b. Click **Next**.

The service descriptions summary page appears. Go to Step 9.

Step 8 **If you selected TCP or UDP as the transport protocol:**

The Select TCP/UDP Values page appears.

a. Enter the destination port or port range. Values are 0–65,535.

b. Enter the source port or port range. Values are 0–65,535.

c. Click **Next**.

The service descriptions summary page appears. Go to Step 9.

If you selected IP as the transport protocol:

a. Enter the IP protocol number, then click **Next**.

The service descriptions summary page appears.

Step 9 Verify the information is correct, then click **Finish**.

Changes are applied to the assigned firewall device configuration files when they are generated. The configuration files are then downloaded to the firewall devices at deployment. (See Chapter 9, "Managing Activities and Jobs.")

Deleting a Service Definition

Before You Begin

- Make sure you have the necessary permissions to perform this function. (See Appendix B, "Understanding User Roles and Permissions.")

Step 1 Select **Configuration > Building Blocks > Service Descriptions**.

The Service Descriptions page appears.

Step 2 Select the check box for the row in the table, then click **Delete**.

You are prompted to confirm the delete request.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 366
Doc 3702

Step 3 Click **OK**.

As the page refreshes, you are prompted with another popup window if access rules or translation rules are affected by the deletion. You will need to review the rules tables and make corrections as needed.

Step 4 Click **OK**.

The row is removed from the table, and the information is removed from the assigned firewall device configuration files when they are deployed. (See Chapter 9, "Managing Activities and Jobs.")

Configuring Service Groups

The Service Definitions feature allows you to create a single access rule that controls access to multiple services, for example, you can write a rule that permits traffic for Telnet and HTTP in a single rule.

Table 6-4 shows the wizard used to add or edit service groups.

Table 6-4 Wizard Used to Add or Edit Service Groups

	Wizard Page
Step 1	Add Name and Description—Allows you to define a service group.
Step 2	Select Service—Allows you to identify the services used for the defined service group.
Step 3	Summary—Allows you to verify configuration settings before committing settings to the database for deployment.

Adding or Editing a Service Group

Before You Begin

- If workflow is enabled, select an activity. (See the "Understanding Activity Actions and States" section on page 9-6.)
- Using the Object Selector, select the scope for the devices to configure. (See the "Object Selector" section on page 2-18.)

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 367
Doc 3702

16-366

Note Some elements in the main table might be grayed out. This is because they are defined at a higher scope and cannot be edited from this level.

Step 1 Select **Configuration>Building Blocks>Service Groups**.

The Service Groups page appears.

Step 2 Do one of the following:

- To add a new row in the table, click **Add**.

  The Add Name and Description page appears.
- To edit a row, select the check box for the row in the table, then click **Edit**.

  The Add Name and Description page appears.

Step 3 Enter the service group name.

Step 4 Enter an optional comment in the Description field.

Step 5 Click **Next**.

The Select Services page appears.

Step 6 Select the available object, then click **Select =>**.

The object is moved to the Selected Objects column.

Step 7 Click **Next**.

The service groups summary page appears.

Step 8 Verify the information is correct, then click **Finish**.

Changes are applied to the assigned firewall device configuration files when they are generated. The configuration files are then downloaded to the firewall devices at deployment. (See Chapter 9, "Managing Activities and Jobs.")

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 368
Doc. 3702

Deleting a Service Group

Before You Begin

Make sure you have the necessary permissions to perform this function. (See Appendix B, "Understanding User Roles and Permissions.")

Step 1 Select **Configuration>Building Blocks>Service Groups**.

The Service Groups table appears.

Step 2 Select the check box for the row in the table, then click **Delete**.

You are prompted to confirm the delete request.

Step 3 Click **OK**.

As the page refreshes, you are prompted with another popup window if access rules or translation rules are affected by the deletion. You will need to review the rules tables and make corrections as needed.

Step 4 Click **OK**.

The row is removed from the table, and the information is removed from the assigned firewall device configuration files when they are deployed. (See Chapter 9, "Managing Activities and Jobs.")

Configuring AAA Server Groups

Firewall MC lets you define separate groups of TACACS+ or RADIUS servers for specifying different types of traffic, for example, a TACACS+ server for inbound traffic and another for outbound traffic, or outbound HTTP traffic authenticated by a TACACS+ server and inbound traffic authenticated by RADIUS.

AAA server groups use tags, which are used to direct different types of traffic to each authentication server. If the first authentication server in the list fails, the AAA subsystem fails over to the next server in the tag group. You can have up to 14 tag groups, and each group can have up to 14 AAA servers, totaling up to 196 AAA servers.

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 369
Doc 3102

Configuring an AAA server group is a two-tier process. First, you create an AAA server group. Second, you define AAA servers within that group. You have the option of inserting an AAA server while you are creating an AAA server group.

Note In Firewall MC, the Group LOCAL protocol local scoped from Global entry represents the AAA group, named LOCAL, that exists by default on PIX Firewalls running version 6.2 or later. The default group cannot be modified or disabled. This group is used for administrative authentication and talks directly to the PIX Firewall instead of a separate AAA server. LOCAL specifies to use the PIX Firewall local user database for local command authorization. The LOCAL group is displayed in the configuration file as `aaa-server LOCAL protocol local.`

To set LOCAL for AAA Authentication, select **Configuration>Settings> AAA Admin Authentication**.

Table 6-5 shows the wizard used to create an AAA server group and insert an AAA server.

Table 6-5 Wizard Used to Create, Insert, or Edit an AAA Server Group

	Wizard Page
Step 1	Select Group Name—Allows you to define a new AAA server group.
Step 2	Define Server—Allows you to assign a server to the AAA server group.
Step 3	Summary—Allows you to verify configuration settings before committing settings to the database for deployment.

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 370
3702
Doc

Creating or Editing an AAA Server Group

Note While you are creating an AAA server group, you can insert an AAA server.

Before You Begin

- If workflow is enabled, select an activity. (See the "Understanding Activity Actions and States" section on page 9-6.)
- Using the Object Selector, select the scope for the devices to configure. (See the "Object Selector" section on page 2-18.)

Note The following procedure assumes you are defining a server group and identifying a server within that group.

Step 1 Select **Configuration>Building Blocks>AAA Server Group**.

The AAA Server Group page appears.

Step 2 Do one of the following:

- To add a server group in the table, click **Create**.

  The Select Group Name page appears.
- To add a server to a group in the table, select the check box for the row in the table after which you want to new row inserted, then click **Insert**.

  The Define Server page appears.
- To edit a group, select the check box for the row in the table, then click **Edit**.

  The Select Group Name page appears.
- To edit a server, select the check box for the row in the table, then click **Edit**.

  The Define Server page appears.

Step 3 Enter the AAA server group name. Spaces are not permitted. A maximum of 14 server groups is permitted.

Step 4 Click the Radius or TACACS protocol radio button to identify the authentication protocol used for the server group.

ROS nº 03/2005 - CPMI - CORREIOS
Fls. Nº 371
Nº 3702

Step 5 Click **Next**.

The Define Server page appears.

Step 6 Select the interface from the list box.

Step 7 Enter the IP address.

Step 8 Enter the server key. For more information, see the online help.

Step 9 Verify the timeout value. Default is 5 seconds.

Step 10 Click **Next**.

The AAA server group summary page appears.

Step 11 Verify the information is correct, then click **Finish**.

Changes are applied to the assigned firewall device configuration files when they are generated. The configuration files are then downloaded to the firewall devices at deployment. (See Chapter 9, "Managing Activities and Jobs.")

Deleting an AAA Server Group or Element

Before You Begin

Make sure you have the necessary permissions to perform this function. (See Appendix B, "Understanding User Roles and Permissions.")

Step 1 Select **Configuration>Building Blocks>AAA Server Group**.

The AAA Server Group page appears.

Step 2 Select the check box for the row in the table, then click **Delete**.

You are prompted to confirm the delete request.

Step 3 Click **OK**.

As the page refreshes, you are prompted with another popup window if access rules or translation rules are affected by the deletion. You will need to review the rules tables and make corrections as needed.

Fls. Nº 372
Nº 3702

Step 4 Click **OK**.

The row is removed from the table, and the information is removed from the assigned firewall device configuration files when they are deployed. (See Chapter 9, "Managing Activities and Jobs.")

Configuring Address Translation Pools

The Address Translation Pools feature allows you to create global address pools used in dynamic NAT rules.

Configuring address translation pools is a two-tier process. First, you create a pool. Second, you define the elements within that pool. You have the option of defining the elements while you are creating an address translation pool.

Table 6-6 shows the wizard used to create an address translation pool and insert a pool element in a single procedure.

Table 6-6 Wizard Used to Create or Edit an Address Translation Pool and Pool Element

	Wizard Page
Step 1	Enter Pool Name—Allows you to define an address pool.
Step 2	Define Element—Allows you to assign IP addresses and masks to the address pool.
Step 3	Summary—Allows you to verify configuration settings before committing settings to the database for deployment.

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 373
Doc 3702

Creating or Editing an Address Translation Pool

Note While you are creating an address translation pool, you can insert an address pool element as part of the procedure.

Before You Begin

- If workflow is enabled, select an activity. (See the "Understanding Activity Actions and States" section on page 9-6.)
- Using the Object Selector, select the scope for the devices to configure. (See the "Object Selector" section on page 2-18.)

Note The following procedure assumes you are defining an address translation pool and identifying a range of pool values within that pool group.

Step 1 Select **Configuration>Building Blocks> Address Translation Pools**.

The Address Translation Pool page appears.

Step 2 Do one of the following:

- To add a pool group to the table, click **Create**.

  The Enter Pool Name page appears.
- To add a pool element to the table, select the check box for the row in the table after which you want to new row inserted, then click **Insert**.

  The Enter Pool Element page appears.
- To edit a pool, select the check box for the row in the table, then click **Edit**.

  The Enter Pool Name page appears.
- To edit a pool range, select the check box for the row in the table, then click **Edit**.

  The Enter Pool Element page appears.

Step 3 Enter the pool name to identify the address translation pool, for example, external addresses.

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 374
Doc 3702

Step 4 Click **Next**.

The Enter Pool Element page appears.

Step 5 Select the interface from the list box.

Step 6 To use the interface address as the closing PAT address, select the PAT check box.

Step 7 Enter address ranges and masks. For more information, see the online help.

Step 8 Click **Next**.

The address translation pool summary page appears.

Step 9 Verify the information is correct, then click **Finish**.

Changes are applied to the assigned firewall device configuration files when they are generated. The configuration files are then downloaded to the firewall devices at deployment. (See Chapter 9, "Managing Activities and Jobs.")

Note Settings enabled during the configuration process are displayed as true in the wizard summary page.

Deleting an Address Translation Pool or Element

Before You Begin

Make sure you have the necessary permissions to perform this function. (See Appendix B, "Understanding User Roles and Permissions.")

Step 1 Select **Configuration > Building Blocks > Address Translation Pools**.

The Address Translation Pool page appears.

Step 2 Select the check box for the row in the table, then click **Delete**.

You are prompted to confirm the delete request.

Step 3 Click **OK**.

As the page refreshes, you are prompted with another popup window if access rules or translation rules are affected by the deletion. You will need to review the rules tables and make corrections as needed.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 375
3702
Doc

Step 4 Click **OK**.

The row is removed from the table, and the information is removed from the assigned firewall device configuration files when they are deployed. (See Chapter 9, "Managing Activities and Jobs.")

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 376
Doc 3702

16.247
L

Segurança Tipo 2 doc 8

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 377
Doc 3702

Resource Manager Essentials Applications

This chapter lists all the Essentials applications and the tasks that can be accomplished with each of these applications. The applications are:

- Device Views
- Availability
- Change Audit
- Configuration Management
- Contract Connection
- Case Management
- Data Extracting Engine (DEE)
- Device Navigator
- Inventory
- Job Approval
- Software Management
- Syslog Analysis

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 378
Doc 3702

Device Views

Essentials provides device views—logical groupings that are used to specify a device or group of devices. You can define views to group selected devices into logical groups. Device views allow you to quickly view reports on all devices of a certain type, or with specific characteristics, such as all Catalyst switches or all devices that you are responsible for.

Since almost every Essentials task requires the set of devices to be executed against, views provide a convenient way to create groups of devices. For example, before you can display an Inventory report, you must select the devices to be included in the report. Views can speed up the selection (instead of running the report for one device at a time).

Note Essentials graphical user interface (GUI) performance may be affected if the number of devices in the selected view is too large. You should avoid setting *all devices* views when the number of devices in the inventory is large. You can use system views or create custom views to keep the number of devices in a view from growing too large.

Creating a view using the Device Views application enables you to run reports for specific devices based on common attributes or user-defined characteristics.

Types of Views

Three categories of device views are available:

- System Views—Predefined and available immediately after you install Essentials. System views include most major classes of Cisco devices. For example all Catalyst switches, all Cisco 7000 Series routers, and all SwitchProbes.
- Custom Views—Defined by users and, when created, are available for use by anyone with the appropriate access to the server.
- PrivateViews—Defined by users, but are available only to the user.

ROS nº 03/2005 - CPMI - CORREIOS
Fls. Nº 379
Doc. 3702

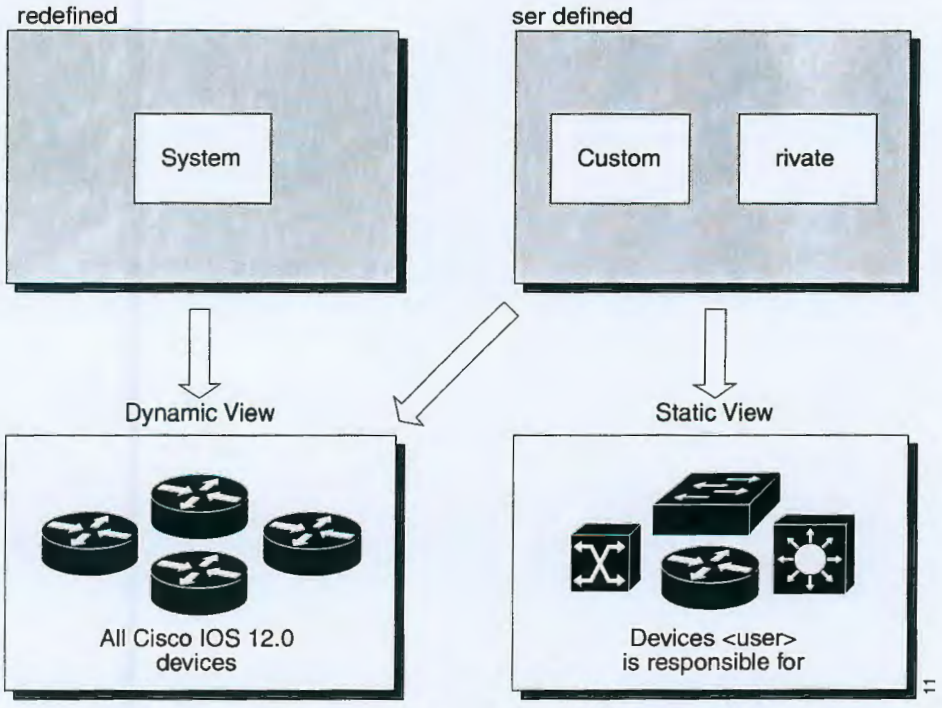
Two different types of views can be created within custom or private views:

- Dynamic Views
- Static Views

Dynamic views are logical groups based on device attributes, such as device class or software version. The devices in a dynamic view can change based on the attribute value of devices in the Inventory. An example of a dynamic view is all devices with Cisco IOS Version 12.0. Any device that currently has this attribute would be included in the device view. All system views are dynamic.

Static views are logical groups based on user-defined characteristics. Static views include any devices that you add to the view. The members of the group do not change unless you manually add or remove devices. Use static views when you do not want the membership to change automatically. See Figure 2-1.

Figure 2-1 Device Views



ROS nº 03/2005 CN
CPMI - CORREIOS
Fls Nº 380
Doc 3702

Table 2-1 shows the tasks that you can accomplish with the Device Views application.

Table 2-1 Device Views Tasks

Task	Purpose	Action
Add static views.	Create views to monitor a specific group of devices in your network inventory.	Select Resource Manager Essentials > Administration > Device Views > Add Static Views.
Add dynamic views.	Create views to monitor devices with common attributes, such as device type. **Note** Any new, managed device added to inventory that fits the listed attributes, is automatically incorporated into the dynamic view.	Select Resource Manager Essentials > Administration > Device Views > Add Dynamic Views.
Change static views.	Modify static views.	Select Resource Manager Essentials > Administration > Device Views > Change Static Views.
Delete views.	Delete any views you have created.	Select Resource Manager Essentials > Administration > Device Views > Delete Views.
Browse dynamic views.	Determine which devices belong to the dynamic views.	Select Resource Manager Essentials > Administration > Device Views> Browse Dynamic Views.
Browse device membership.	Determine which views a device belongs to.	Select Resource Manager Essentials > Administration > Device Views > Browse Device Membership.

Setting Device Credentials

It is important to configure the device credentials correctly on every Cisco device that you will manage and monitor using Essentials.

Table 2-2 lists all the applications and the device credentials required for proper functioning of the applications.

RQS nº 03/2005 - CN
CPMI CORREIOS
Fls. Nº 381
Doc 3702

Table 2-2 Applications and the Device Credentials

Application	Telnet Password	Enable Password	SNMP Read Only	SNMP Read / Write
NetConfig	Required	Required	Required	Required if configuration fetch is through TFTP
NetShow	Required	Required	Required	Not required
Config Editor	Required	Required	Required	Required if configuration fetch is through TFTP
ChangeAudit	Not required	Not required	Required	Not required
Configuration Management (Telnet)	Required	Required	Required	Not required
Configuration Management (TFTP)	Not required	Not required	Required	Required
Device Views	Not required	Not required	Required	Not required
Inventory	Not required[1]	Not required[2]	Required	Not required[3]
SWIM	Required[4]	Required[5]	Required	Required
Syslog	Not required	Not required	Required	Not required
Availability	Required	Required	Required	Not required
Case Management	Required	Not required	Required	Not required
Contract Connection	Required	Not required	Required	Not required

1. Inventory requires Telnet password to perform the check device attributes operation.
2. Inventory requires enable password to perform the check device attributes operation.
3. Inventory requires SNMP Read/Write string to perform the check device attributes operation.
4. Required in case of few devices.
5. Required in case of few devices.

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 382
Doc 3702

System Configuration

System Configuration lets you configure system-wide information on the CiscoWorks server. In this way, you can centrally locate information that is used by more than one Essentials application.

Note Network administrators should perform these tasks with care. If errors occur, users may not be able to log in.

Table 2-3 shows the tasks that you can accomplish with System Configuration.

Table 2-3 System Configuration Tasks

Task	Purpose	Action
Set up a proxy URL.	Enable applications to connect to Cisco.com. If the server access to the outside world is controlled through a proxy server, this must be configured.	Select Resource Manager Essentials > Administration > System Configuration, then select the Proxy tab.
Define SNMP timeouts and retries.	Specifies the timeout value and the number of retries while querying devices for inventory collection.	Select Resource Manager Essentials > Administration > System Configuration, then select the SNMP tab.
Define the SMTP server name.	Define your Simple Mail Transfer Protocol (SMTP) server in Essentials to use e-mail, to automatically notify network administrators when certain tasks and jobs are completed.	Select Resource Manager Essentials > Administration > System Configuration, then select the SMTP tab.
Define rcp usernames.	Specify the username to authenticate rcp transfers between the devices and the server for remote operations.	Select Resource Manager Essentials > Administration > System Configuration, then select the rcp tab.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 383
Doc 3702

Availability

The Availability application lets you monitor the reachability and response time of your network devices. You can view the availability of a selected group of devices, a summary of interface status, reports of reloads (reboots) and unreachable devices, and protocol distribution graphs.

Benefits of Availability

If you experience connectivity problems trying to reach certain resources or services on the network, one of the first things you must check is the status of a device. If a device is unreachable, you will want to find out when it was last operational and whether any abnormal reloads have occurred. This can be the first step in troubleshooting the exact location of the fault. Availability helps you track the reachability of devices on your network.

The Availability application periodically polls selected devices to determine device reachability, interface status, and response times. Availability reports display the status of devices, show devices that are offline for more than three hours, and summarize the percentage of Layer 3 protocol traffic forwarded on each Layer 3 device.

The Reloads Report shows the cause of the past five reloads for a device and includes a link to the Cisco.com Cisco Output Interpreter to help troubleshoot any device failures. Availability provides reports to quickly assess the status of selected devices on the network. Information can be tracked for all devices on the network, or only critical devices to reduce the load on the network and the network management system.

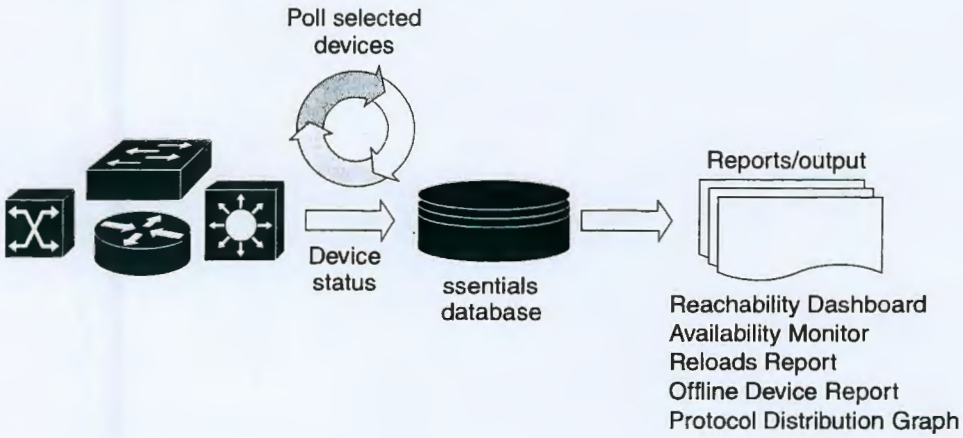
Availability Functional Flow

Before device availability information will be stored in Essentials, you must select the specific device views that needs to be monitored for Availability. When devices are selected to be included in Availability polling, Essentials will poll the devices according to the schedule set by the network administrator (only one schedule for all views). Devices will be polled for reachability, response time, interface status, reload, and protocol information.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 384
Doc 3702

This information will be updated in the Availability database after each scheduled poll, and can be viewed by displaying Availability Reports. Historical information on reachability and response times is also stored in the Essentials database and can be displayed in trend graphs under Availability Monitor. See Figure 2-2.

Figure 2-2 Availability Functional Flow



Availability Workflow

Figure 2-3 depicts the Availability workflow and associated tasks within Essentials:

- In order to retrieve Availability information from devices, each device must be in the Essentials Inventory with the proper SNMP read community string attribute.
- Polling options must be set, including selecting which device views are going to be polled for availability information. When devices are selected, availability information can be viewed in any of the Availability Reports within Essentials. Information is automatically purged according to the options you set, so no ongoing maintenance is required.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 385
Nº - Doc 3702

Figure 2-3 Availability Workflow

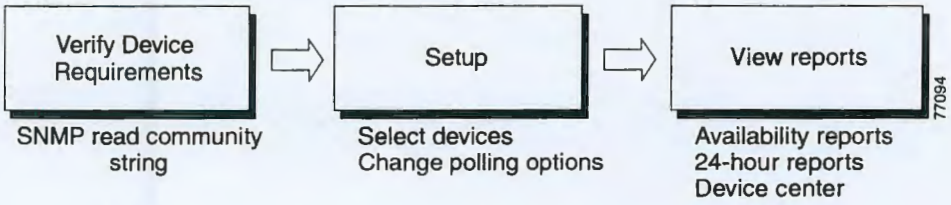


Table 2-4 shows the tasks you can accomplish with the Availability application.

Table 2-4 Availability Manager Tasks

Task	Purpose	Action
Set polling views and options.	Select views to be monitored. You must do this before you can monitor device availability. If your system performance is degraded by availability polling, you can add more system resources, poll fewer devices, or poll less frequently.	Select Resource Manager Essentials > Administration > Availability > Change Polling Options.
Change polling options.	Select default Availability polling option values or to select new values from the drop-down list boxes. The polling options you set, apply to all Availability views.	Select Resource Manager Essentials > Administration > Availability > Change Polling Options.
View the Reachability Dashboard.	View device status for all views set for availability monitoring. The dashboard continuously reports: • All views being polled and the number of devices in each view. • Device names of all devices in each view and the time they last responded.	Select Resource Manager Essentials > Availability > Reachability Dashboard.
Monitor device availability.	Continuously monitor selected devices and access interface availability details.	Select Resource Manager Essentials > Availability > Availability Monitor.

ROS nº 03/2005 - CPMI - CORREIOS
Fls. Nº 386
Doc 3702

Table 2-4 Availability Manager Tasks (continued)

Task	Purpose	Action
View the Reloads report.	Display the most recent reloads (up to 5) for selected devices. The report shows the reason for each reload and when it occurred.	Select Resource Manager Essentials > Availability > Reloads Report. To view reloads that occurred only within the past 24 hours, select Resource Manager Essentials > 24-Hour Reports > Reloads Report.
View the Cisco Output Interpreter Analysis.	Decode and analyze the device's stack dump, to enable troubleshooting of devices that reload unexpectedly. An unexpected reload is any reload that is neither initiated by you nor a result of a power-on. The Reloads report applies only to routers running Cisco IOS Release 10.2 or later and is available only for the most recent reload.	Select Resource Manager Essentials > Availability > Reloads Report. In the generated report, click on the reload reason. You may be prompted to enter your Cisco.com (CCO) username and password. See the Cisco home page to have your Cisco.com (CCO) profile updated or changed, or, after you log in, use the Cisco.com Profile button to update your Cisco.com profile.
View the Offline Device report.	Generate a report of managed devices that have not responded to polling for more than a specified period of time (3, 6, 12, 24, 48, or 72 hours).	Select Resource Manager Essentials > Availability > Offline Device Report. To view only devices that have been off line for the past 24 hours, select Resource Manager Essentials > 24-Hour Reports > Offline Device Report.
View the Protocol Distribution graph.	View the distribution of IP, AppleTalk, IPX, DECnet, VINES, and XNS packets for selected devices in a bar or pie chart. This report shows the Layer 3 protocol packet types that are forwarded by the devices.	Select Resource Manager Essentials > Availability > Protocol Distribution Graph.

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 387
Doc. 3702

Case Management

You can use Case Management to open and track a case for network problems that require assistance from Cisco Technical Assistance Centre. Case Management can collect critical network information, such as protocol, interface, and configuration data from Essentials and send to Cisco.com.

When you open a case, you can designate specific Telnet command data (if applicable) and SNMP inventory values to be collected from selected devices. Case Management will attach this information to the case description and forward it to Cisco.com, which can reduce the time it takes a Cisco representative to help resolve the problem.

Inquiries to Cisco TAC are categorized according to the urgency of the issue. New cases are automatically set to Priority level 3 (P3). If your case requires higher priority handling, you must contact the Cisco TAC or your sales engineer to request that the priority be raised. For more information on priority categories, see "Obtaining Technical Assistance" section on page -xvii.

Table 2-5 shows the tasks you can accomplish with the Case Management application.

Table 2-5 Case Management Tasks

Task	Purpose	Action
Open a case and attach network device statistics.	Open a case to Cisco.com through the CiscoWorks desktop	Select Management Connection > Case Management > Open Case.
View status of cases and update description.	View the history and status of your case and update description of problems.	Select Management Connection > Case Management > Query or Update Case.

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 388
Doc 3702

Change Audit

The Change Audit application lets you track and report network changes. It provides the capability for other Essentials applications to log change information to a central repository called the Change Audit log.

New Features in Change Audit

You can now delete change audit records that are older than a specified number of days.
For example, if you specify 15 days, change audit records that are over 15 days old (including today) will be deleted (**Resource Manager Essentials > Administration > Change Audit > Delete Change History**).

Change Audit Functional Flow

Change Audit tracks all changes discovered by the Inventory Manager, Software Manager, and Configuration Manager. Every time one of these applications detects a change, it sends a change record to the Change Audit Service, with details of who, when, and what type of change occurred. See Figure 2-4.

Inventory changes include any changes to device information stored in the Inventory database, such as chassis, interfaces, and system information. Software Management changes include upgrades to new software image versions. Configuration Management changes include all changes made to configuration files on devices. This includes changes made outside of Essentials tasks, detected by the Configuration Archive process, as well as changes made using Essentials functionality—NetConfig or Config Editor.

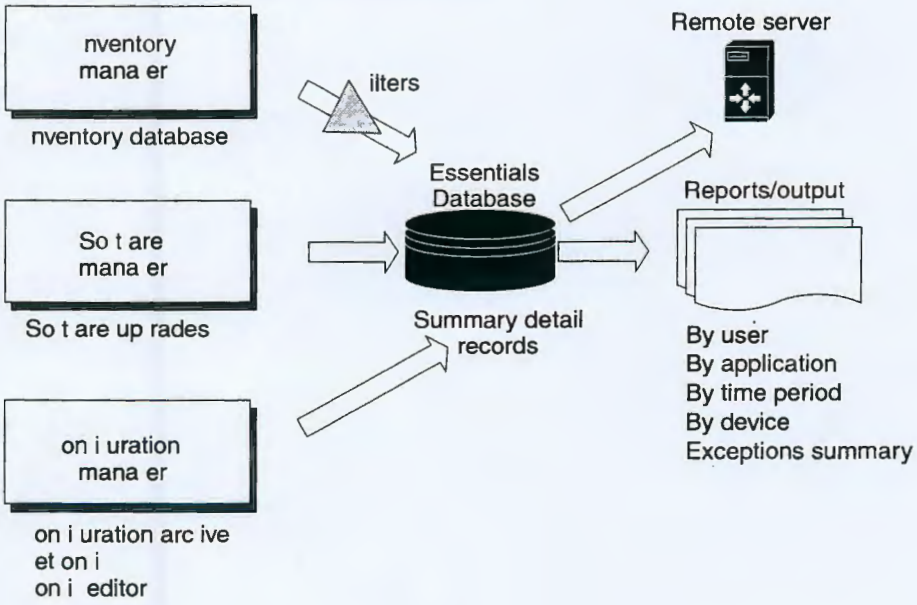
Inventory changes can be filtered to limit the types of changes that are stored in the Change Audit database. For example, you might not want to track every time the port status on a switch changes because users have shut down their computers connected to the switch. Software and configuration management changes cannot be filtered.

You can view change records or search for specific change records to determine who made a change or when a change was made. Change reports can also be time based to quickly report on changes that have, or have not, occurred during specified time periods—possibly detecting unauthorized change activity.

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 389
Doc 3702

The Change Audit Service application can also be configured to forward change records, in the form of SNMP traps to remote servers, allowing you to monitor and view changes from a remote network-management station that has event-collection capabilities, such as HP OpenView.

Figure 2-4 Change Audit Functional Flow



RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 390
Doc. 3702

Figure 2-5 Change Audit Work Flow

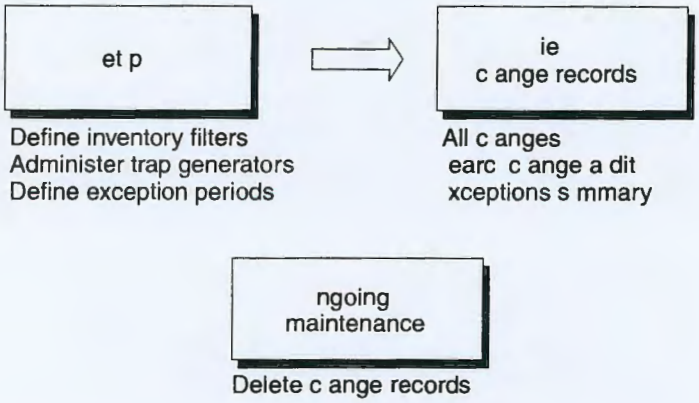


Figure 2-5 depicts the Change Audit workflow and associated tasks within Essentials. Change Audit automatically stores any change records sent from the Inventory Manager, Software Manager, and Configuration Manager applications. After these applications are set up, you can view change records at any time.

You need to perform Change Audit setup tasks only if you want to filter out specific Inventory changes, forward change records to a remote server, or report on changes during specific time periods every week. Change records are stored in the Essentials database until they are removed. Therefore, ongoing maintenance is required to delete old records from the database.

Table 2-6 shows the tasks that you can accomplish with the Change Audit application.

RQS nº 03/2005 - CN
CPMI CORREIOS
Fls Nº 391
Doc 3702

Table 2-6 Change Audit Tasks

Task	Purpose	Action
View Change Audit logs.	View the two log tables: Change Audit summary and Change Audit details.	Select Resource Manager Essentials > 24-Hour Reports > Change Audit Report. Or Select any report from Resource Manager Essentials > Change Audit.
Delete records from the log.	Delete or schedule deletion of change records from the Change Audit log.	Select Resource Manager Essentials > Administration > Change Audit > Delete Change History.
Convert change records to SNMP traps.	Convert some or all change notifications into SNMP V1 traps and send them to a destination you configure.	Select Resource Manager Essentials > Administration > Change Audit > Administer Trap Generator.
Define an exceptions period.	Specify a period of time when no network changes should occur.	Select Resource Manager Essentials > Administration > Change Audit > Define Exceptions Summary.
Set up filtering options.	Define one or more filter fields to filter report data.	Select Resource Manager Essentials > Change Audit > Search Change Audit.
View changes in an exception period.	Generate a report on changes that occurred in the network during a defined exception.	Select Resource Manager Essentials > Change Audit > Exceptions Summary.
View all change records.	Generate a report that enables you to view changed data in the Change Audit log.	Select Resource Manager Essentials > Change Audit > All Changes.
View a summary of changes made in the last 24-hours.	Generate a summary of changes made in the past 24 hours from Change Audit log data.	Select Resource Manager Essentials > 24-Hour Reports > Change Audit Report.

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 392
Doc 3702

Configuration Management

The Configuration Management application stores the current, and a user-specified number of previous versions, of the configuration files for all supported Cisco devices maintained in the Inventory. It automatically tracks changes to configuration files and updates the database if a change is made.

New Features of Configuration Management

The Configuration Management application has the following new features, that allow you to:

- Enable Job Password Policy for NetConfig, NetShow, and Config Editor Jobs
- Specify the Transport Protocol Order for NetConfig, Config Editor, and Network Show Jobs
- Quick Configuration Download from Configuration Archive
- Archive and Restore VLAN Configuration Files

For more details of the new features, see Configuration Management, in the Essentials online help.

Enable Job Password Policy for NetConfig, NetShow, and Config Editor Jobs

Essentials stores passwords in the database. While the job is run, the password is retrieved from the database for each of the selected devices. For example, if the TACACS server is managing the devices, the passwords in the TACACS server and the passwords in the Essentials database should be synchronized (with every password change).

You now have the option of entering a username and password for running a specific NetConfig, Network Show, or Config Editor job. If you enter a username and password, NetConfig, Network Show or Config Editor applications use this username and password to connect to the device, instead of taking these credentials from the Essentials database.

This option of entering the username and password for job execution is useful in high security installations where device passwords are changed at frequent intervals. In such instances, the passwords may be changed every 60-90 seconds.

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 393
Doc 3702

To use this option of entering a username and password for running a specific job, you should enable the job password policy for NetConfig, Network Show, or Config Editor jobs using the Password Policy tab of the Configuration Job Setup dialog box, in the Configuration Management application. To invoke the Configuration Job Setup dialog box, select **Resource Manager Essentials > Administration > Configuration Management > Configuration Job Setup**.

You can also set the job password to be mandatory, or user configurable.

If you do not enable the job password policy, then the NetConfig, Network Show, or Config Editor applications take the device credentials from the Essentials database to connect to the device.

For details about:

- Enabling the job password policy, see the Essentials online help. (In the left navigation pane of the Essentials online help, select **Resource Manager Essentials > Configuration Management > Configuration Management Administration > Password Policy for NetConfig, Config Editor and NetShow Jobs**).
- Usage Scenarios when the job password is configured on devices, see the Essentials online help. (In the left navigation pane of the Essentials online help, select **Resource Manager Essentials > Configuration Management > Configuration Management Administration > Usage Scenarios When Job Password is Configured on Devices**).

Specify the Transport Protocol Order for NetConfig, Config Editor, and Network Show Jobs

Essentials now provides you with the option of separately specifying the transport protocol order for the download operations of NetConfig, Config Editor and Network Show jobs, and for the fetch operations of NetConfig and Config Editor jobs.

You can use the Transport Protocol tab of the Configuration Management application (**Resource Manager Essentials > Configuration Management > Administration > Configuration Job Setup**) to specify the transport protocol order.

This option allows you to use your preferred protocols for downloading or fetching configurations.

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 394
Doc 3702

For example, you can use Telnet to download configuration to the device, and TFTP to fetch the configuration, thereby improving the overall performance of NetConfig.

You can select the fallback option for these protocols. If you select this option, and the first preferred protocol fails, the next protocol in the list is used for configuration download or fetch operations, and so on.

For details, see the Essentials online help.
(In the left navigation pane of the Essentials online help, select **Resource Manager Essentials > Configuration Management > Configuration Management Administration > Setting the Transport Protocol Order for NetConfig, Config Editor and NetShow Jobs**).

Quick Configuration Download from Configuration Archive

You can now create a job to immediately download a selected version of the running configuration, to a device from the Configuration Archive (**Resource Manager Essentials > Configuration Management > Search Archive by Device** or **Resource Manager Essentials > Configuration Management > Search Archive by Pattern**).

This method of download is useful when you know the version of the running configuration that has to be downloaded to the device.

For details, see the Essentials online help.
(In the left navigation pane of the Essentials online help, select **Resource Manager Essentials > Configuration Management > Configuration Management Administration > Making a Quick Download of a Device Configuration**).

Archive and Restore VLAN Configuration Files

For all Cisco devices that support VLAN configuration such as Catalyst IOS switches, Essentials creates a version of the VLAN configuration file (vlan.dat) for each version of the running configuration file of a device. That is, the running configuration and the vlan configuration files are archived in pairs.

You can download the vlan configuration file to the device, using the Command Line Interface.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 395
3702

You can view the status of the archived VLAN files using the VLAN Configuration tab of the Configuration Archive Status Summary window (**Resource Manager Essentials > Administration > Configuration Management > Archive Status**).

This table details the scenarios under which VLAN configuration is fetched.

Scenarios	VLAN Config Fetched/Not Fetched
On adding a device to Inventory	Fetched
On using the Update Archive option from GUI	Fetched
On receiving a Config Change syslog event	Fetched
Scheduled Config Polling	Fetched
Scheduled Config Collection	Fetched
Using the command cwconfig get from CLI	Fetched
Sync Config Archive Before Execution Policy of NetConfig/Config editor.	Fetched
Config Fetch following download of commands through NetConfig/Config Editor/Quick Config Restore /cwconfig command	Not fetched

(In the left navigation pane of the Essentials online help, select **Resource Manager Essentials > Configuration Management > Configuration Management Administration > Checking VLAN Configuration Archive Status**.)

Benefits of Configuration Management

One of the most difficult but important things to manage on network devices, is the device configuration. Often a change to the device configuration leads to network performance issues and faults. The device configuration is the key to how a device operates on the network and traffic is passed.

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 396
Doc: 3702

As the network administrator, you need to be able to control and track changes to device configurations to minimize errors and assist in troubleshooting problems. This can be very difficult if several different users are making changes to the device configurations. It can also become very repetitive and time-consuming. Configuration Management can help simplify and automate these tasks.

Configuration Management gives you easy access to the configuration files for all file-based or Cisco IOS-based Catalyst switches, FastSwitches, Cisco routers, Content Service Switches (CSS) and Content Engine (CE) devices in Essentials.

Configuration files are collected and stored in the Configuration Archive for all the devices supported by the Configuration Management application. (For the list of supported devices, on Cisco.com select **Products and Services > Network Management CiscoWorks > CiscoWorks Resource Manager Essentials > Technical Details > Device Support Tables.**)
When you change the configuration, an event is sent to the archive which automatically collects the latest configuration.

Before you can use the Configuration Archive, you must make sure you have completed all the necessary setup tasks. For information on these tasks, see:

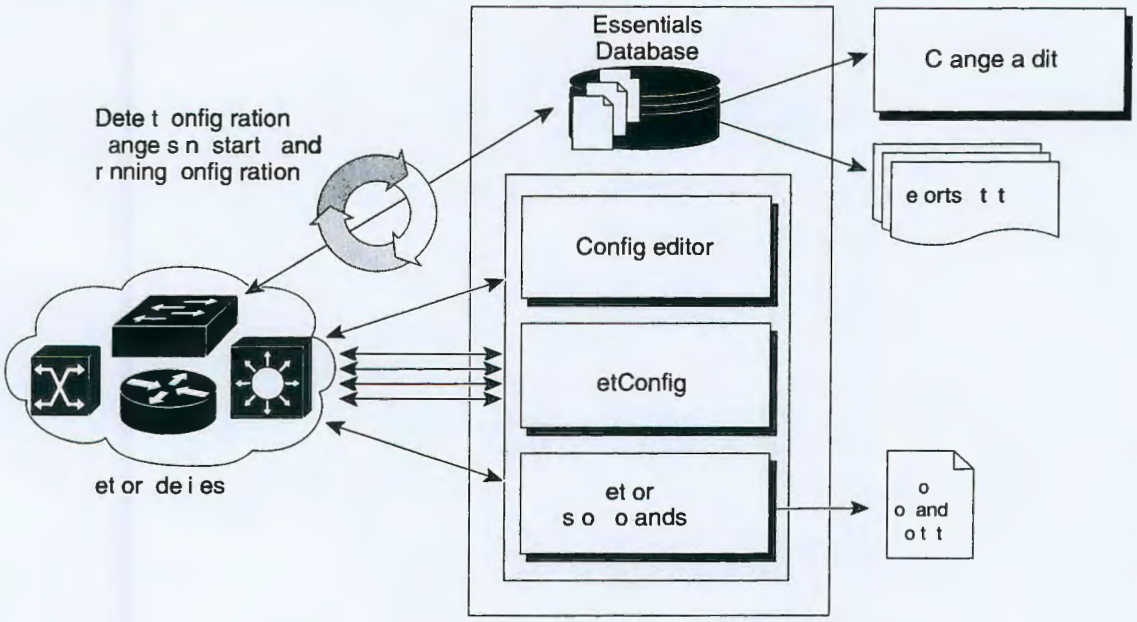
- Installation and Setup Guide for Resource Manager Essentials on Solaris.
- Installation and Setup Guide for Resource Manager Essentials on Windows.

Configuration Management Functional Flow

After you add or import devices into your inventory, the configuration files for each supported device are collected and stored in the Configuration Archive. When you change the configuration, an alert is sent to the archive which automatically collects the latest configuration information. In addition, a change record is sent to the Change Audit application, which collects and organizes all changes to network devices. This allows you to view all configuration changes made over any period of time or by any specific user. See Figure 2-6

RGS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 397
Doc 3702

Figure 2-6 Configuration Management Functional Flow



16.275

Figure 2-7 Configuration Management Workflow

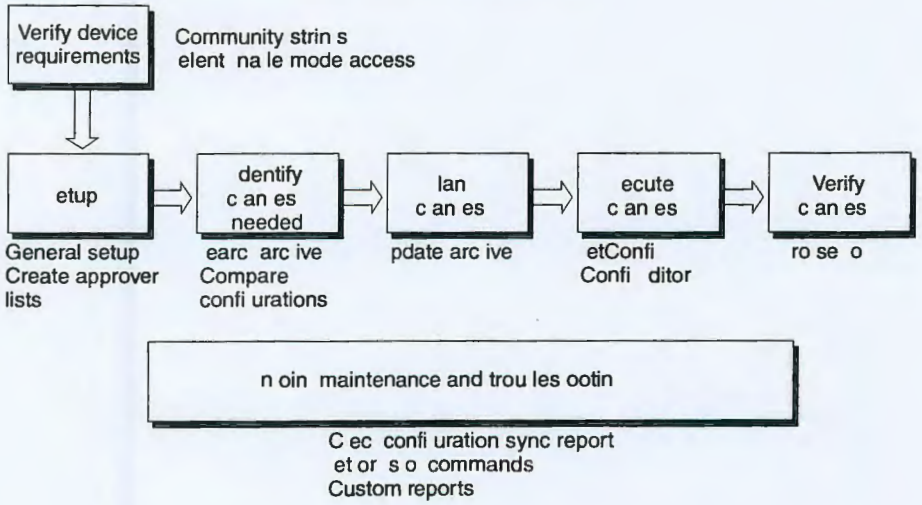


Figure 2-7 depicts Configuration Management workflow and associated tasks:

- Verify device requirements to ensure that Essentials is able to communicate with the devices.
- Create approver lists, if specific users are going to be required to approve configuration updates before they are executed and set Configuration Archive preferences (update schedule, number of copies to retain, and so on), and After the Configuration Archive is set up, it can be used to view device configurations and identify and plan necessary changes. Then, the NetConfig or Config Editor applications can be used to actually execute and confirm the changes.

  As ongoing maintenance, the Configuration Sync report should be checked daily to ensure that all running and startup configurations on devices match. In addition, the network administrator can use Network Show Commands and Custom reports to troubleshoot problems and gather information as needed.

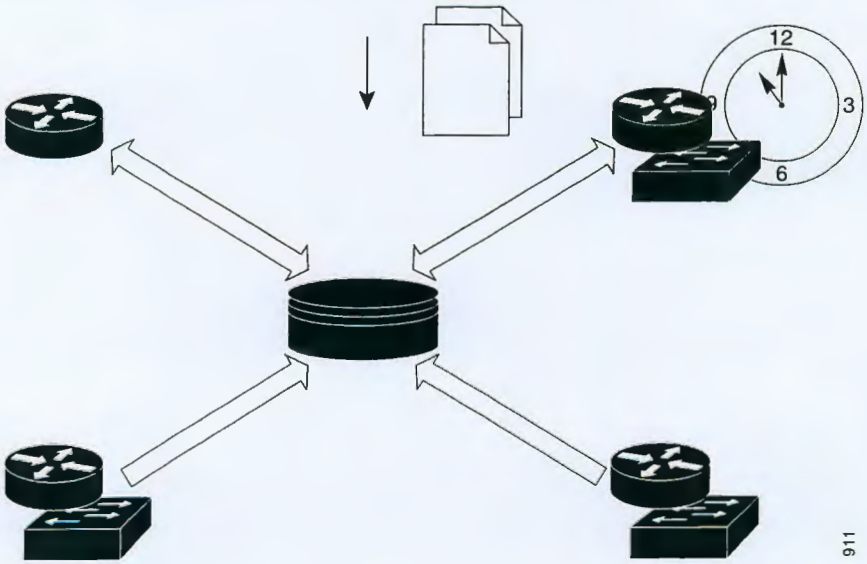
ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 399
Nº Doc 3702

Configuration Archive

The Configuration Archive maintains a history of configuration files for all managed devices on the network. The network administrator can specify how long files should be kept in the archive, how many versions should be maintained in the archive, and how often devices on the network should be polled for changes. In addition, there are multiple ways to detect changes on devices and trigger an update to the Configuration Archive.

For example, specific syslog messages sent from the device can indicate that a change has occurred and can trigger the Configuration Archive to retrieve the new configuration. The Configuration Archive can also be scheduled to poll all devices at a specific time each week.

Figure 2-8 Configuration Archive Functional Flow



NetConfig, Config Editor, and Network Show Commands

Two additional applications, NetConfig and Config Editor, are available to edit configuration files. The NetConfig application allows you to save sets of commands and execute those commands on multiple devices at the same time.

The Config Editor application can be used to edit any device configuration that is stored in the Configuration Archive, and then download the new configuration to the device. The new configuration is stored in the Configuration Archive and will also trigger a change record to be sent to Change Audit. Additional Configuration reports specific to active virtual private network (VPN) devices are also available.

The NetConfig application provides a set of wizard-based templates that can be used to update the device configuration on multiple devices all at once. The devices must already be managed by Essentials. The new configuration will be stored in the archive for each device changed, and associated change records will be created.

The Network Show Command application accesses network devices in real time to display output for common show commands. This can help in troubleshooting by allowing you to display interface statistics, routing tables, and system information for selected devices.

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 401
Doc 3702

Table 2-7 shows the archive-specific tasks you can accomplish with the Configuration Management application.

Table 2-7 Configuration Management Archive-Specific Tasks

Task	Purpose	Action
Search for configuration files.	Search for configuration files based on device name or text pattern.	Select Resource Manager Essentials > Configuration > Management > Search Archive by Device. or Select Resource Manager Essentials > Configuration Management > Search Archive by Pattern.
Create, run, modify, and delete custom reports.	Create and run custom reports that gather device configuration files from the archive for specified devices. You can also modify and delete custom reports.	Select Resource Manager Essentials > Configuration Management > Custom Reports.
Compare device configuration files.	Compare configuration files of two devices or two versions of a single file. Compare the starting and current configurations of a device. Compare the current and the most recently archived configurations of a device.	Select Resource Manager Essentials > Configuration Management > Compare Configurations.
Find out-of-sync configurations.	Determine whether a device's startup and running configurations are synchronized. The two configurations might differ if you change a device configuration after the device is booted.	Select Resource Manager Essentials > Configuration Management > Startup/Running Out of Sync Report or Select Resource Manager Essentials > 24 Hour Reports > Configuration Sync Report.

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 402
Doc 3702

Table 2-7 Configuration Management Archive-Specific Tasks (continued)

Task	Purpose	Action
Move the Configuration Archive.	Move the Configuration Archive to a new location.	Select Resource Manager Essentials > Administration > Configuration Management > General Setup, then select the Archive Setup tab.
Specify criteria for purging the archive.	Specify when to purge configurations from the archive. You can specify two criteria: • Age. Configurations older than the specified age are purged. • Maximum number of versions. The oldest configuration is purged when the maximum number is reached. You can also choose not to purge labelled files.	Select Resource Manager Essentials > Administration > Configuration Management > General Setup, then select the Archive Setup tab.
Modify Configuration Archive retrieval.	Modify how and when the Configuration Archive retrieves configurations.	Select Resource Manager Essentials > Administration > Configuration Management > General Setup, then select the Change Probe Setup tab.
Change the transport protocol order used by the Configuration Archive.	Change the order of the transport protocols the Configuration Archive uses to download configurations from devices to the archive. The default order is: • TFTP (Trivial File Transport Protocol) • Telnet • SSH • rcp (Remote Copy Protocol)	Select Resource Manager Essentials > Administration > Configuration Management > General Setup, then select the Transport Setup tab.

16.273
ROS nº 03/2006 - CN
CPMI - CORREIOS
Fls. Nº 403
Doc 3702

Table 2-7 Configuration Management Archive-Specific Tasks (continued)

Task	Purpose	Action
Update the Configuration Archive.	Update the archive manually if you make a significant change to a device configuration and want the archive to reflect the changes. The Configuration Archive retrieves configurations at 12.30 a.m. every Friday by default. It also listens to Syslog messages and fetches the configuration.	Select Resource Manager Essentials > Configuration Management > Update Archive.
Check the archive status.	Check archive status for the latest attempt to archive a device configuration (running or startup).	Select Resource Manager Essentials > Administration > Configuration Management > Archive Status.
Configure labels.	Select configuration files from different managed devices, group them, and label them as a set. You can also view, modify, and remove configuration labels.	Select Resource Manager Essentials > Administration > Configuration Management > Label Configuration.
Use the **cwconfig** command at the command line.	Access the Configuration Archive to update, export, and import configurations on devices and in the archive. For more information about the command syntax and parameters, see the cwconfig man page on UNIX systems, by entering: `man -M /opt/CSCOpx/man cwconfig`	This command cannot be entered from the desktop; use the command line.
Locate the Configuration Archive shadow directory.	Access the Configuration Archive shadow directory, which is an image of the most recent configurations gathered by the Configuration Archive.	The shadow directories cannot be accessed from the desktop. • On Solaris, as root or casuser, enter: `/var/adm/CSCOpx/files/archive/shadow` • On Windows, as admin, enter: *NMSROOT*`\files\archive\shadow`

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 404
Doc 3702

16.269

NetConfig Option

Using the NetConfig option, which runs as a separate application in its own window, you can make configuration changes to your managed network devices.

New Features of NetConfig

NetConfig application has the following new features:

- Job Password Option
- Job Retry Option
- Multiple Selection of Jobs for Deletion
- Separate Protocol Ordering for Configuration Download and Fetch Operations
- Support for New Templates
- Support for System- Defined Templates to Configure IPSec and SSH on Devices
- Support for Interactive and Multiline Commands

For more details of the new features, see the section, NetConfig, in the Essentials online help.

Job Password Option

Essentials stores passwords in the database. While the job is run, the password is retrieved from the database for each of the selected devices. For example, if the TACACS server is managing the devices, the passwords in the TACACS server and the passwords in the Essentials database should be synchronized (with every password change).

You now have the option of entering a username and password for running a specific job. If you enter a username and password, NetConfig uses this username and password to connect to the device, instead of taking these credentials from the Essentials database.

This option of entering the username and password for job execution is useful in high security installations where device passwords are changed at frequent intervals. In such instances, the passwords may be changed every 60-90 seconds.

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 405
Doc 3702

To use this option of entering a username and password for running a specific job, you should enable the job password policy for NetConfig jobs using the Password Policy tab of the Configuration Job Setup dialog box, in the Configuration Management application. To invoke the Configuration Job Setup dialog box, select **Resource Manager Essentials > Administration > Configuration Management > Configuration Job Setup**.

You can also set the job password to be mandatory, or user configurable.

If you do not enable the job password policy, then NetConfig takes the device credentials from the Essentials database to connect to the device.

For details about:

- Enabling the job password policy, see the Essentials online help.
  (In the left navigation pane of the Essentials online help, select **Resource Manager Essentials > NetConfig > NetConfig Administration > Password Policy for NetConfig Jobs**).
- Usage Scenarios when job password is configured on devices, see the Essentials online help.
  (In the left navigation pane of the Essentials online help, select **Resource Manager Essentials > Configuration Management > Configuration Management Administration > Usage Scenarios When Job Password is Configured on Devices**).
- The NetConfig usage scenario, see the topic, "Performing a NetConfig Job with the Job Password Policy Enabled", in this User Guide.

Job Retry Option

You now have the retry option for failed NetConfig jobs. When you retry a job, it runs the job on the failed devices, and retains the job ID of the failed job.

For details, see the Essentials online help.
(In the left navigation pane of the Essentials online help, select **Resource Manager Essentials > NetConfig > Browsing and Editing NetConfig Jobs > Browsing and Editing Jobs**.)

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 406
Doc. 3702

Multiple Selection of Jobs for Deletion

You can now select more than one job at a time, for deletion from the Job Browser.

For details, see the Essentials online help.
(In the left navigation pane of the Essentials online help, select
Resource Manager Essentials > NetConfig >
Browsing and Editing NetConfig Jobs > Browsing and Editing Jobs.)

Separate Protocol Ordering for Configuration Download and Fetch Operations

Earlier, the NetConfig application used Telnet to download configuration diffs to the device, and same session was used to fetch the entire configuration from the device. If the configurations are large (for example, ACLs) this adversely affected the overall performance of NetConfig.

For NetConfig jobs, you can now set the transport protocol order separately, for downloading configurations, and for fetching configurations.

This option allows you to use your preferred protocols for downloading and fetching the configuration. For example, you can use Telnet to download configuration to the device, and TFTP to fetch the configuration, thus improving the overall performance of NetConfig.

For downloading the configurations, the protocols used are Telnet and SSH.

The default order is,

- Telnet
- SSH (Secure Shell)

For fetching the configurations, the protocols used are Telnet, TFTP, SSH, and rcp. The default order is,

- TFTP (Trivial File Transport Protocol)
- Telnet
- rcp (remote copy protocol)
- SSH (Secure Shell)

You can change the transport protocol order for both downloading and fetching the configurations.

You can select the fallback option for these protocols. If you select this option, and the first preferred protocol fails, the next protocol in the list is used for configuration download or fetch operations, and so on.

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 407
Doc 3702

For details, see the Essentials online help.
(In the left navigation pane of the Essentials online help, select **Resource Manager Essentials > Configuration Management > Configuration Management Administration > Setting the Transport Protocol Order for NetConfig, Config Editor and NetShow Jobs**).

Support for New Templates

Resource Manager Essentials now supports eleven new templates, that can be used through the NetConfig application. They are:

IOS Templates. (These are global IOS templates. They can be applied to one or more IOS device at a time.)

- SNMP Security
- SNMP Traps Management

IOS-Interface-specific Templates. (These can be applied to only one IOS device at a time.)

- IGMP
- Interface IP Address

Cable Templates (These are global templates. They can be applied to one or more Cable-CMTS devices at a time.)

- Cable N+1 Redundancy
- Cable Spectrum Management

Cable Interface-specific Templates. (These can be applied to only one Cable-CMTS device at a time.)

- Cable BPI/BPI+
- Cable DHCP-GiAddr and Helper
- Cable DownStream
- Cable Interface Bundling
- Cable Upstream

For details, see the Essentials online help.
(In the left navigation pane of the Essentials online help, select **Resource Manager Essentials > NetConfig >Configuration Templates**).

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 408
Doc 3702

16,265

Support for System- Defined Templates to Configure IPSec and SSH on Devices

Essentials now supports system-defined templates for configuring IPSec and SSH on devices:

- Use the SSH system-defined template to configure SSH on devices.
- Use the Internet Key Exchange (IKE), Transform, Crypto Map system-defined templates to configure IPSec on devices.

For details, see the Essentials online help.
(In the left navigation pane of the Essentials online help, select **Resource Manager Essentials > NetConfig >Configuration Templates**).

Support for Interactive and Multiline Commands

You can now specify interactive and multi-line commands in user defined templates.

For example, as a part of user-defined templates in NetConfig, you can do the following:

- Enter an interactive command in the Enter CLI Commands area, using the following syntax:

  CLI Command<R>*command response 1* <R>*command response 2*

- Enter a multi-line command, using the following syntax:

  <MLTCMD> banner login *"Welcome to*

  CiscoWorks Resource Manager

  Essentials – you are using

  multiline commands" **</MLTCMD>**

Note The tags, <R>, <MLTCMD> and </MLTCMD>, are case sensitive and should always be uppercase.

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 409
Doc. 3702

Support for interactive and multi-line commands is not available through the NetConfig CLI.

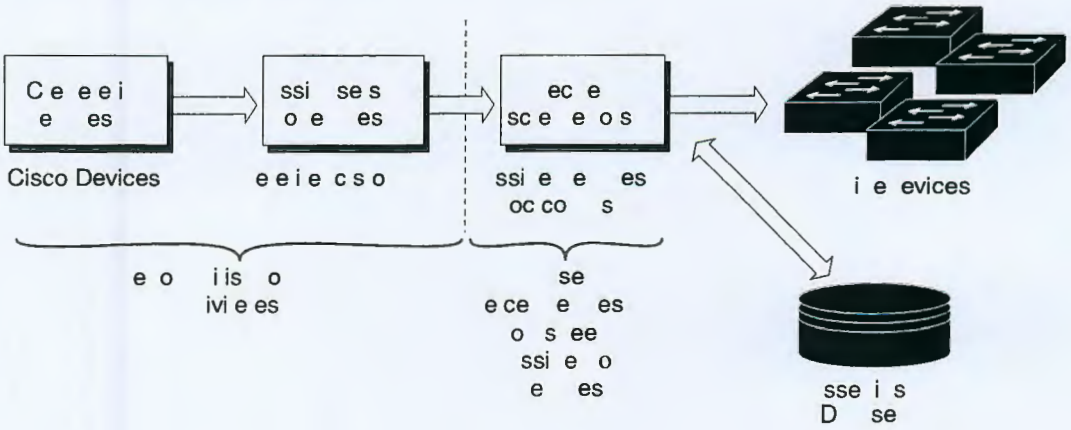
For details, see the Essentials online help.
(In the left navigation pane of the Essentials online help, select **Resource Manager Essentials > NetConfig >Defining and Scheduling a NetConfig Job > Handling Interactive Commands in NetConfig and Config Editor Jobs** and **Handling Multi-line Commands**).

Benefits of Netconfig

The NetConfig application provides you with wizard-based templates to simplify and reduce the time it takes to make global changes to network devices. These templates can be used to execute one or more configuration commands on multiple devices at the same time.

For example, if you want to change passwords on a regular basis to increase security on devices, you can use the appropriate password template to update passwords on all devices at once. A copy of all updated configurations will be automatically stored in the Configuration Archive. See Figure 2-9.

Figure 2-9 NetConfig Functional Flow



NetConfig uses configuration templates to create the configuration commands run on devices when a NetConfig job runs. There are three types of configuration templates:

- System-defined—Provided with NetConfig, these templates simplify the creation of common configuration commands.
- User-defined—Created by system administrators, these templates can contain any configuration commands.
- Adhoc—Allows you to add any configuration commands to a NetConfig job while you are defining it.

Caution NetConfig does not verify the commands entered in the user-defined and adhoc templates. These commands are executed on devices exactly as they appear in the template. If you enter incorrect configuration commands, you could misconfigure or disable the devices on which the job runs.

By default, only network administrators have access to configuration templates. Network administrators can assign template access privileges to the other system users. When you define or edit a job, the configuration templates to which you have access privileges, appear in the job definition wizard.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 411
Doc 3702

Table 2-8 shows the tasks that can be accomplished with the NetConfig option.

Table 2-8 NetConfig Tasks

Task	Purpose	Action
Define and schedule a NetConfig job.	Define a NetConfig job to make device configuration changes, and schedule it to run.	1. Select Resource Manager Essentials > Configuration Management > NetConfig > Jobs > New Job. or Click the New Job button. 2. Complete the job definition wizard.
Browse and edit NetConfig jobs.	Browse the NetConfig jobs that are registered on the system and edit them as necessary.	1. Select Resource Manager Essentials > Configuration Management > NetConfig > Jobs > Job Browser. or Click the Job Browser button. 2. Select a job record. 3. Click Edit Job, Copy Job, Remove Job, Stop Job, or Job Details.
View NetConfig job details.	View detailed information about a registered NetConfig job. You can also edit a job from its detailed view.	1. Select Resource Manager Essentials > Configuration Management > NetConfig > Jobs > Job Browser. or Click the Job Browser button. 2. Select a job record. 3. Click Job Details. 4. Click Edit Job, Copy Job, Remove Job, Stop Job, Retry Job (for failed jobs), or Print.

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 412
Nº
Doc 3702

Table 2-8 NetConfig Tasks (continued)

Task	Purpose	Action
Launch Essentials.	Launch Essentials if it is not already running.	Select Resource Manager Essentials > Configuration Management > NetConfig >Tools > Launch RME. or Click the Launch RME button.
Create and edit user-defined configuration templates.	Create and edit configuration templates that can contain any configuration commands.	Select Resource Manager Essentials > Configuration Management > NetConfig >Admin> Create/Edit User Templates.
Assign configuration template access privileges to users.	Assign access privileges to the system-defined and user templates on the system.	Select Resource Manager Essentials > Configuration Management > NetConfig > Admin > Assign Template Users.
Set default template policies.	Set the default policies for NetConfig jobs that are defined.	Select Resource Manager Essentials > Configuration Management > NetConfig > Admin > Set Template Policies.
View online help for the task you are performing.	View the online help for information about the task you are performing.	Select Resource Manager Essentials > Configuration Management > NetConfig > Help > Context-Sensitive Help. or Click the Help button.
Use the NetConfig command to make batch configuration changes.	Define and schedule NetConfig jobs from the command line.	Enter the NetConfig command at the command line with the appropriate syntax. For more information, see the online help and the netconfig man page. To view the man page, add the path `install_dir/CSCOpx/man` to the *MANPATH* variable.

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 413
Nº 3702
Doc

Network Show Commands Option

As a network administrators you must be familiar with *show commands* used on Cisco routers and switches. Network show commands represent a set of read-only commands that you can run on routers, Catalyst switches, Content Engine, Content Service Switches, FastSwitchs and PIX devices. These commands display configuration or status information. You can run Network Show commands from the GUI or from the command line interface.

New Features in Network Show

Network Show has the following new features:

- Job Password Option
- Multiple Selection of Jobs for Deletion
- Protocol Ordering for Running Network Show Commands

For more details of the new features, see NetConfig, in the Essentials online help.

Job Password Option

Essentials stores passwords in the database. While the job is run, the password is retrieved from the database for each of the selected devices.
For example, if the TACACS server is managing the devices, the passwords in the TACACS server and the passwords in the Essentials database should be synchronized (with every password change).

You now have the option of entering a username and password for running a specific job. If you enter a username and password, Network Show uses this username and password to connect to the device, instead of taking these credentials from the Essentials database.

This option of entering the username and password for job execution is useful in high security installations where device passwords are changed at frequent intervals. In such instances, the passwords may be changed every 60-90 seconds.

ROS nº 03/2006 - CN
CPMI - CORREIOS
Fls Nº 414
Nº - Doc 3702

To use this option of entering a username and password for running a specific job, you should enable the job password policy for Network Show jobs using the Password Policy tab of the Configuration Job Setup dialog box, in the Configuration Management application. To invoke the Configuration Job Setup dialog box, select **Resource Manager Essentials > Administration > Configuration Management > Configuration Job Setup**.

You can also set the job password to be mandatory, or user configurable.

If you do not enable the job password policy, then Network Show takes the device credentials from the Essentials database to connect to the device.

For more details about:

- Enabling the job password policy, see the Essentials online help. (In the left navigation pane of the Essentials online help, select **Resource Manager Essentials > Configuration Management > Configuration Management Administration > Password Policy for NetConfig, Config Editor and NetShow Jobs**).
- Job password for Network Show jobs, see the Essentials online help. (In the left navigation pane of the Essentials online help, select **Resource Manager Essentials > Network Show > Network Show Batch Reports > Network Show Batch Reports Tasks > Scheduling a Report**).
- Usage Scenarios when the job password is configured on devices, see the Essentials online help. (In the left navigation pane of the Essentials online help, select **Resource Manager Essentials > Configuration Management > Configuration Management Administration > Usage Scenarios When Job Password is Configured on Devices**).

Multiple Selection of Jobs for Deletion

You can now select more than one job at a time, for deletion from the Job Browser.

For details, see the Essentials online help. (In the left navigation pane of the Essentials online help, select **Resource Manager Essentials > Network Show > Network Show Batch Reports > Network Show Batch Reports Tasks > Browsing Jobs**).

ROS nº 03/2005 - Cia
CPMI - CORREIOS
Fls Nº 415
Nº Doc 3702

Protocol Ordering for Running Network Show Commands

You can now set the transport protocol order for running network show commands on devices.

For running the commands, the protocols used are Telnet and SSH. The default order is,

- Telnet
- SSH (Secure Shell)

This option allows you to use your preferred protocol order for running network show commands on devices. If you select the fallback option for these protocols and the first preferred protocol fails, the next protocol in the list is used for running the show commands, and so on.

For details, see the Essentials online help.
(In the left navigation pane of the Essentials online help, select **Resource Manager Essentials > Configuration Management > Configuration Management Administration > Setting the Transport Protocol Order for NetConfig, Config Editor and NetShow Jobs**).

Benefits of Network Show Commands

As an Essentials user, you can execute Show commands against many devices and view the results from Essentials, using the Network Show Commands application.

This application can be used to display Show command output for multiple devices in two modes:

- Immediate execution—Run the selected set of Show commands for the selected devices immediately.
- Batch mode—Schedule a set of Show commands to be run against a selected set of devices.

You can use the Network Show tasks to organize and save one or more related Show commands into logical groups, called command sets. These command sets can then be applied to devices whenever specific configuration or status information is needed. You specify which commands you want to group together and run the commands on one or many devices. The output is displayed in a browser window.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 416
Doc

All users have access to the following predefined command sets, which ship with Essentials. Some of the most common Show commands used in monitoring and troubleshooting a network are:

- `show interface info`
- `show IP routing info`
- `show protocol info`
- `show switch VLAN info`
- `show system info`
- `show system performance`
- `Show Interfaces Rate-Limit Info`
- `Show Cable QoS Profile Info`
- `Show Cable Modulation-Profile`
- `Show Cable Hop Info`
- `Show Cable Tech Info`
- `Show HCCP details Info`
- `Show IGMP Info`
- `Show SNMP Users and Groups Info`
- `Show Cable Spectrum Info`
- `Show Cable Modem Info`

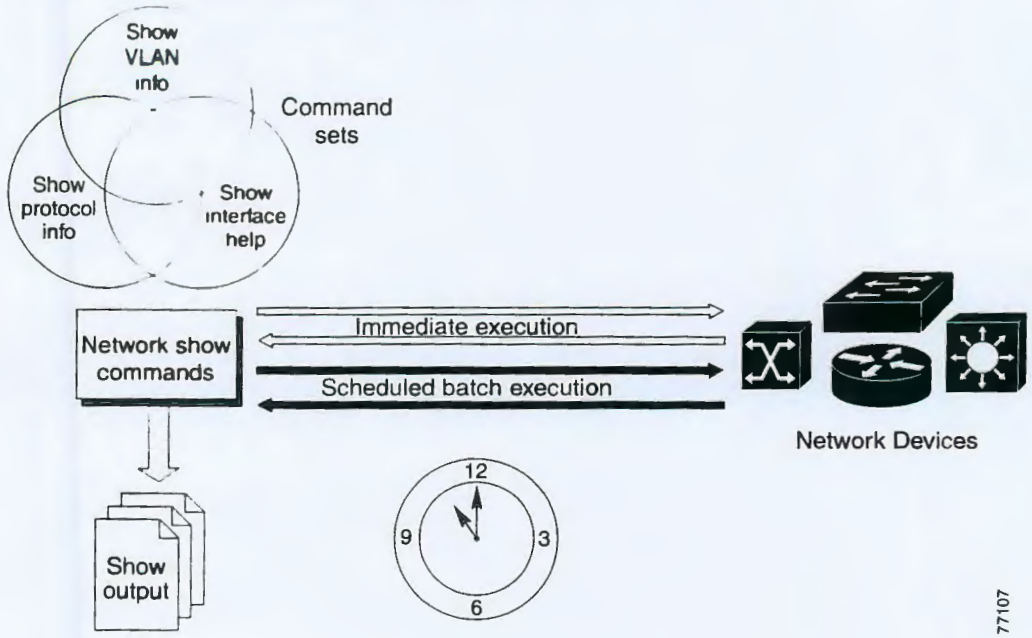
For details of all the available Show commands, see the Essentials online help. (In the left navigation pane of the Essentials online help, select **Resource Manager Essentials > Network Show > The Basics > List of Network Show Commands**).

In order to display output for other Show commands within Essentials, you must first define the command set, and then assign users to be able to access the command set.

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 417
Doc 3702

Essentials ships with a set of default network command sets, which you cannot edit or delete. See Figure 2-10.

Figure 2-10 Network Show Commands Functional Flow



ROS nº 03/2006 - CN
CPMI - CORREIOS
Fls. Nº 418
Doc 3702

Table 2-9 shows the tasks you can accomplish with the Network Show Commands option.

Table 2-9 Network Show Commands Tasks

Task	Purpose	Action
Create a network show command set.	Create, edit, and delete a logical group of custom commands for a user or a set of users.	Select Resource Manager Essentials > Administration > Configuration Management > Network Show > Define Command Set.
Assign users to the network show command set.	Specify which user or set of users can run network show commands.	Select Resource Manager Essentials > Administration > Configuration Management > Network Show > Assign Users.
Execute a network show command set immediately.	Run network show commands on one or more devices.	Select Resource Manager Essentials > Configuration Management > Network Show Commands > Immediate Execution.
Define a batch report.	Create a batch report containing command sets and remote console commands that can be run on a set of devices to generate a report. You can also modify or delete existing reports.	Select Resource Manager Essentials > Configuration Management > Network Show Commands > Batch Reports > Define Reports.
Schedule a batch report.	Schedule reports in batches and generate these batch reports at a specified time.	Select Resource Manager Essentials > Configuration Management > Network Show Commands > Batch Reports > Schedule Reports.
View report output.	View the output of a batch report.	Select Resource Manager Essentials > Configuration Management > Network Show Commands > Batch Reports > View Report Output.

ROS nº 03/2005 - CPMI - CORREIOS
Fls Nº 419
Doc 3702

Table 2-9 Network Show Commands Tasks (continued)

Task	Purpose	Action
Browse network show jobs.	Browse the network show jobs that are registered on the system and view job details. You can also edit or delete jobs.	1. Select Resource Manager Essentials > Configuration Management > Network Show Commands > Batch Reports > Job Browser. 2. Select a job record. 3. Click Edit Job, Stop Job, Remove Job, Copy Job, or Job Details.
Set job policies.	Each network show job has properties that define how the job runs. You can configure a default policy for these properties that apply to all future jobs.	Select Resource Manager Essentials > Configuration Management > Network Show Commands > Batch Reports > Set Job Policies.
Use the **cwconfig netshow** command.	Define and execute command sets command sets to be run against a set of devices.	Enter the **cwconfig netshow** command at the command line. For more information, see the online help and the cwconfig netshow man page.
Use the **cwconfig netshow** batch command.	Define and schedule reports, comprising multiple network show command sets to be run against a set of devices.	Enter the **cwconfig netshow** batch command at the command line. For more information, see the online help and the cwconfig netshowbatch man page.

Config Editor Option

You can edit configuration files stored in the Configuration Archive and download files to devices, using the Config Editor option. This option runs as a separate application in its own window.

RDS nº 03/2004 - CN
CPMI - CORREIOS
Fls Nº 420
3702
Doc

New Features of Config Editor

Config Editor has the following new features:

- Job Password Option
- Multiple Selection of Jobs for Deletion
- Separate Protocol Ordering for Configuration Download and Fetch Operations
- Support for Interactive Commands

For more details, see the Essentials online help.

Job Password Option

Essentials stores passwords in the database. While the job is run, the password is retrieved from the database for each of the selected devices.
For example, if the TACACS server is managing the devices, the passwords in the TACACS server and the passwords in the Essentials database should be synchronized (with every password change).

You now have the option of entering a username and password for running a specific job. If you enter a username and password, Config Editor uses this username and password to connect to the device, instead of taking these credentials from the Essentials database.

This option of entering the username and password for job execution is useful in high security installations where device passwords are changed at frequent intervals. In such instances, the passwords may be changed every 60-90 seconds.

To use this option of entering a username and password for running a specific job, you should enable the job password policy for Config Editor jobs using the Password Policy tab of the Configuration Job Setup dialog box, in the Configuration Management application. To invoke the Configuration Job Setup dialog box, select **Resource Manager Essentials > Administration > Configuration Management > Configuration Job Setup**.

You can also set the job password to be mandatory, or user configurable.

If you do not enable the job password policy, then Config Editor takes the device credentials from the Essentials database to connect to the device.

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 421
Nº 3702
Doc

For more details about:

- Enabling the job password policy, see the Essentials online help. (In the left navigation pane of the Essentials online help, select **Resource Manager Essentials > Configuration Management > Configuration Management Administration > Password Policy for NetConfig, Config Editor and NetShow Jobs**).
- Job password for Config Editor jobs, see the Essentials online help. (In the left navigation pane of the Essentials online help, select **Resource Manager Essentials > Config Editor > Config Editor Tasks > Configuring Job Properties**).
- Usage Scenarios when the job password is configured on devices, see the Essentials online help. (In the left navigation pane of the Essentials online help, select **Resource Manager Essentials > Configuration Management > Configuration Management Administration > Usage Scenarios When Job Password is Configured on Devices**).

Multiple Selection of Jobs for Deletion

You can now select more than one job at a time, for deletion from the Job Browser.

For details, see the Essentials online help.
(In the left navigation pane of the Essentials online help, select **Resource Manager Essentials > Config Editor > Config Editor Tasks > Working with Files > Displaying the Job Status**).

Separate Protocol Ordering for Configuration Download and Fetch Operations

For Config Editor jobs, you can now use your preferred transport protocols, separately, for downloading configurations, and for fetching configurations.

For example, you can use Telnet to download configuration to the device, and TFTP to fetch the configuration, thus improving the overall performance of Config Editor.

For downloading the configurations, the protocols used are Telnet and SSH.

The default order is,

- Telnet
- SSH (Secure Shell)

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 422
Nº 3702
Doc

For fetching the configurations, the protocols used are Telnet, TFTP, SSH, and rcp. The default order is,

- TFTP (Trivial File Transport Protocol)
- Telnet
- rcp (remote copy protocol)
- SSH (Secure Shell)

You can change the transport protocol order for both downloading and fetching the configurations.

You can select the fallback option for these protocols. If you select this option, and the first preferred protocol fails, the next protocol in the list is used for configuration download or fetch operations.

For details, see the Essentials online help.
(In the left navigation pane of the Essentials online help, select **Resource Manager Essentials > Configuration Management > Configuration Management Administration > Setting the Transport Protocol Order for NetConfig, Config Editor and NetShow Jobs**).

Support for Interactive Commands

Interactive commands can be edited using Config Editor.

For example, you can enter an interactive command in the Enter CLI Commands area, using the following syntax:

CLI Command<R>*command response 1* <R>*command response 2*

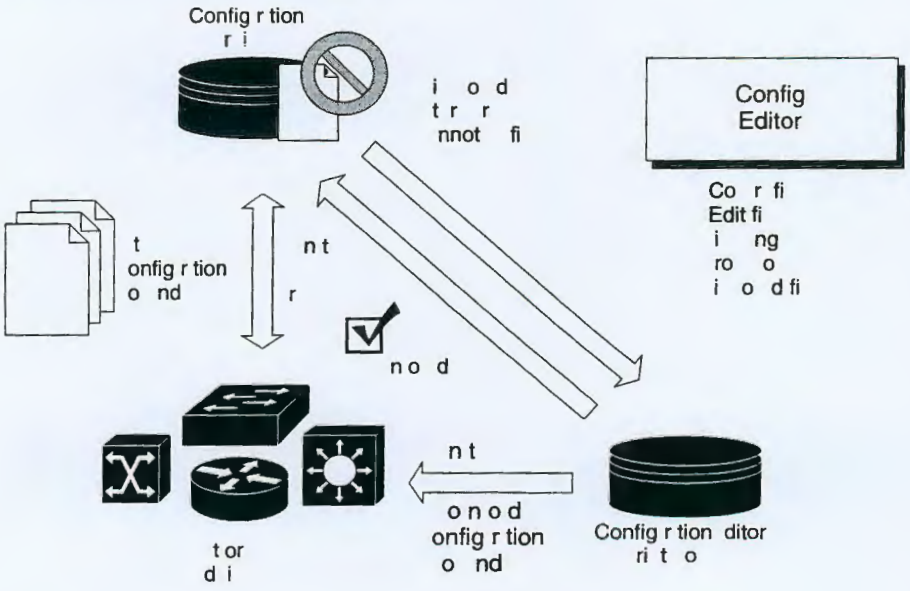
Benefits of Config Editor

Config Editor allows you to edit and download configuration files to devices using a GUI instead of the command line interface (CLI). Use Config Editor to edit individual device configurations within Essentials and then download them back to a device. A copy of the updated configuration will automatically be stored in the Configuration Archive.

RGS nº 03/2005 - CN
CPMI - CORREIOS
Fls: 3702423
Doc

When a configuration file is opened with Config Editor, the file is locked so that other users will not be able to make changes at the same time. While the file is locked, it is maintained in a *private* archive available only to the user who checked it out. If other users attempt to open the file to edit it, they will be notified that the file is already checked out and they can open only a *read only* copy. The file will remain locked until it is downloaded to the device or manually unlocked within Config Editor. See Figure 2-11.

Figure 2-11 Config Editor Functional Flow



Note Many applications rely on access to configuration file within the Configuration Archive (NetConfig, ACL Manager). Hence, you must ensure that all files have been unlocked before exiting Config Editor.
Select **Resource Manager Essentials > Configuration Management > Config Editor > Tools > List Checked Out Files** before exiting Config Editor to get a list of files that have to be checked in.

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 424
Doc 3702

Table 2-10 shows the tasks you can accomplish with the Config Editor option.

Table 2-10 Config Editor Tasks

Task	Purpose	Action
Edit configuration files from the archives.	Check out a file from the archive, and edit it.	Select Resource Manager Essentials > Configuration Management > Config Editor > File > Open.
Schedule download jobs.	Define and schedule a download job.	Select Resource Manager Essentials > Configuration Management > Config Editor > File > Download.
Print configuration files.	Print a configuration file.	Select Resource Manager Essentials > Configuration Management > Config Editor > File > Print.
Configure job policies.	Configure a default policy for job properties that applies to all future jobs. You can also specify if the property can be configured by other users.	Select Resource Manager Essentials > Configuration Management > Config Editor > Edit > Set Job Policies.
Set up editing preferences.	Set up your editing preferences. Config Editor remembers your preferred mode even across different invocations of the application. After you open a file in a specific mode, you can view it only in that mode until you unlock it.	Select Resource Manager Essentials > Configuration Management > Config Editor > Edit > Preferences.
View changes.	View the changes to the checked out file. Essentials compares the current file with the checked out version.	Select Resource Manager Essentials > Configuration Management > Config Editor > Tools > Show Changes Made.
Compare versions of the configuration files.	Compare the current file with any version in the Configuration Archive.	Select Resource Manager Essentials > Configuration Management > Config Editor > Tools > Compare.
Enter comment lines.	Enter comment lines while editing a configuration file.	Select Resource Manager Essentials > Configuration Management > Config Editor > Tools > Insert Comment Line.

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 425
3702
Doc

Table 2-10 Config Editor Tasks (continued)

Task	Purpose	Action
List checked out files.	View a list of files checked out by all users.	Select Resource Manager Essentials > Configuration Management > Config Editor > Tools > List Checked Out Files.
Browse and edit Config Editor jobs.	Browse the Config Editor jobs that are registered on the system and edit them as necessary.	1. Select Resource Manager Essentials > Configuration Management > Config Editor > Tools > Job Browser. 2. Select a job record. 3. Click Edit Job, Copy Job, Remove Job, Stop Job, or Job Details.
View job details.	View detailed information about a registered Config Editor job. You can also edit a job from its detailed view.	1. Select Resource Manager Essentials > Configuration Management > Config Editor > Tools > Job Browser. 2. Select a job record. 3. Click Job Details. 4. Click Edit Job, Copy Job, Remove Job, Stop Job, or Print Job.

Contract Connection

Contract Connection lets you verify which of your Cisco IOS devices are covered by a service contract, and when they will expire. Contract Connection uses Inventory Manager, Cisco Connection Online (Cisco.com) and Contract Agent, Cisco's internal tracking service, to provide the status of your service coverage.

To view contract status, however, you must have login privileges to the Cisco.com web site and a Cisco.com profile that enables access to the Contract Agent.

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 426
Nº 3702
Doc

Contract Connection Workflow

Contract Connection checks the devices in your Essentials Inventory against devices logged in the Cisco Contract Agent and displays a summary. You can also view a detailed report on the contract status, which shows when the contract was initiated and when it will expire.

Three different serial numbers can be associated with a device. This determines how Contract Connection works:

- Shipment serial number—The number tagged on the device when it is shipped from Cisco. Also the number logged in the Cisco Contract Agent.
- Managed serial number—The number stored in the Essentials Inventory database. It is entered or retrieved from the device when a device is added or imported into the database.
- Electronic serial number—The number stored in the device MIB. It can be set or modified through the command line interface (CLI) on the device.

For Contract Connection to work properly and display contract details, the managed serial number in the Essentials Inventory must match the shipment serial number logged with the Cisco Contract Agent. If these numbers do not match, select **Resource Manager Essentials > Administration > Inventory > Change Device Attributes**, to edit the serial numbers.

Table 2-11 shows the task you can accomplish with the Contract Connection application.

Table 2-11 Contract Connection Task

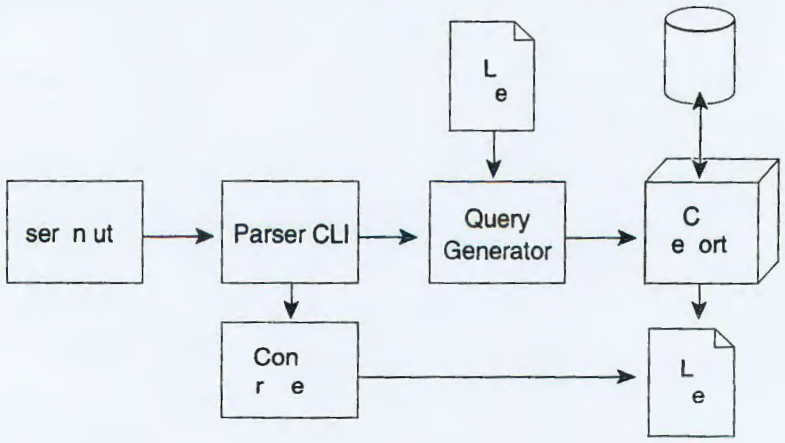
Task	Purpose	Action
Check the status of a contract.	Check which of your Cisco IOS managed devices are covered by a service contract and review contract details.	Select Resource Manager Essentials > Contract Connection > Check Contract Status.

Data Extracting Engine (DEE)

Data Extracting Engine (DEE) is a tool that enables you to extract detailed device inventory and running configuration information in XML format from the Essentials server. See Figure 2-12.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 427
Doc 3702

Figure 2-12 Data Extracting Engine Functional Flow



Using DEE, you can extract data, in the following ways:

- Through a command line utility
- Through a servlet utility, which can be accessed by any client script through HTTP or HTTPS.

Benefits of Data Extracting Engine

DEE has the following benefits. You can:

- Generate inventory data in the XML format.
  DEE has servlet access and command line utilities that can generate inventory data for devices managed by the Essentials server.
- Generate configuration data in XML format.
  DEE uses existing Configuration Archive APIs and generates latest configuration data from the Configuration Archive in XML format. Elements in the XML file are created at the configlet level in the current Configuration Archive. Predefined rules that currently exist in the Configuration Archive are used to get the configlets data. The exported data contains the entire running configuration data.

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 428
Nº 3702
Doc

16.245
L

- Archive XML Data.
  By default, the data generated through CLI is archived at the following location:

  For Inventory,

  PX_DATADIR/archive/cwexport/*timestamp*inventory.xml

  For Config,

  PX_DATADIR/archive/cwexport/*timestamp*config.xml

  Where *PX_DATADIR* is the *NMSROOT*/files directory, and *NMSROOT* is the Essentials installed directory.

  You can also specify a directory to store the output. This application does not have a feature to automatically delete the files created in the archive. You should manually delete the files when necessary. While generating data through the servlet, the output will be displayed in the client terminal.
- Generate and download inventory and configuration data in XML format using the servlet.
  You have to upload a payload XML file, which contains the cwexport command options and CiscoWorks user credentials. You have to write your own script to invoke the servlet with a payload of this XML file and the servlet returns the exported file in XML format, if the credentials are correct and options are valid.
  For details of payload XML file, see the DEE online help.

Device Navigator

Device Navigator lets you access a device that has a Hypertext Transfer Protocol (HTTP) server enabled, directly from a Web Browser. You can select a device and go to the device home page to perform some operations typically performed by Telnet and CLI. You must have the appropriate permissions to access these features.

All Cisco routers and access servers with Cisco IOS 11.0(6) or later have an embedded HTTP server that allows you to access the device from a Web Browser.

From the device web page, you can view the configuration and connectivity information, and even modify the device configuration.

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 429
Nº 3702
Doc

The Device Navigator allows you to connect to the HTTP server on a device directly from Essentials.

In order to utilize this feature, the HTTP server must be enabled on the device. TTP server is 80.

To enable the HTTP server, use the following Cisco IOS global configuration command:

```
router(config)# ip http server
```

To change the default port used to access the device Web page, use the following global configuration command:

```
router(config)# ip http port number
```

Table 2-13 shows the tasks you can accomplish with the Device Navigator application.

Table 2-12 Device Navigator Tasks

Task	Purpose	Action
Browse Device	Allows you to access a device that has a Hypertext Transfer Protocol (HTTP) server enabled, directly from a Web Browser.	Select Management Connection > Device Navigator > Browse Devices.
Configure Fallback Port.	Enables you to configure a fallback port. Typically, the HTTP server for a device is configured to run on port 80. However, you can configure it to run on any port.	Select Management Connection > Device Navigator > Configure Fallback Port.

Benefits of Device Navigator

With the Device Navigator you can:

- Browse Devices
- Configure a Fallback Port

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 430
Doc 3702

Browse Devices

When the HTTP server is enabled on a device, you can use the Device Navigator to display the device home page in Essentials:

1. Select **Management Connection > Device Navigator > Browse Device** from the CiscoWorks desktop.
2. Select the required device, and click **Next**.

   The Device Login dialog box appears.
3. Enter the enable password to access the device and click **OK**. You do not need to enter a username.

   The home page for the device appears.

The device home page provides links to the following configuration and connectivity information:

Telnet	Opens a telnet sessions
Show Interfaces	Displays command output
Show Diagnostic Log	Displays show logging command output
Monitor the router	Provides drill-down menus to execute configuration commands
Connectivity test	Pings the device
Show Tech Support	Displays the command output

There are also links to additional resources and Cisco tech support information at the bottom of the Web page.

Configure a Fallback Port

Typically the HTTP server for a device is configured to run on Port 80. However you can configure the HTTP server to run on any port, in case Port 80 is used by another service.

When browsing the device, the Device Navigator will attempt to connect to Port 80 first.

ECT nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 431
Doc 3702

16.242
L

If this fails, Device Navigator attempts to connect to the fallback port, if one has been configured in Essentials.

To select a fallback port for Device Navigator, select **Management Connection > Device Navigator > Configure Fallback Port** from the CiscoWorks desktop.

Inventory

Networks are a mix of heterogeneous and geographically dispersed systems. Tracking of hardware and software assets in such an environment is very critical. Inventory details are essential as a basic requirement for all network management applications.

Having all the information about all of your devices in a central place, makes it easier to locate necessary information, resolve problems quickly, and provide detailed information to interested parties.

New Features of Inventory

The Inventory application has the following new features:

- The length of the user fields (**Resource Manager Essentials > Administration > Inventory > Add Device**) has been increased to contain 128 characters. You can now use these fields to enter specific notes about the device. For example, you can enter information about the device, such as, its location, the contact person for the device, the asset tag of the device, etc.
- You can customize the labels for the user fields (**Resource Manager Essentials > Administration > Inventory > Add Device**) by editing the mapping.properties file.

  The mapping.properties file is in *NMSROOT*/htdocs.

  The changes that you make to these field labels are reflected in the:

  - Inventory reports (In the Custom Reports, Hardware Reports, Software Reports, Chassis Slot Details Reports and MultiService Port Details Reports).
  - GUI (In the GUI for Add Devices, Change Device Attributes, and in the Custom Reports search criteria field selection GUI).

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 432
Doc 3702

For example, in the mapping.properties file, you can change the user fields to show meaningful names in the reports and in the GUI, as follows:

- User Field 1 = Purchase Date
- User Field 2 = Price
- User Field 3 = Vendor
- User Field 4 = Contract Details

For details, see the Essentials online help.
(In the left navigation pane of the Essentials online help, select **Resource Manager Essentials > Inventory > Add, Import, and Delete Devices > Adding Devices.** In this topic, Step 2 of Procedure, click the link, "device access, user, and serial number".

Benefits of Inventory Management

As a network administrator, you need to be able to quickly troubleshoot problems on the network, identify when network capacity is being reached, and provide information to management on the number and types of devices being used on the network. If the network goes down, one of the first things you will need to know is what devices are running on the network.

Most Essentials tasks are performed against a set of devices. Hence, information about a particular device must be available in the Essentials database. Inventory Manager is used to specify which devices to manage.

Since Essentials takes advantage of many different management services to collect device information (for example, SNMP, TFTP, Telnet), each device placed into the Essentials database (Inventory) must include the necessary parameters (device attributes) for various management services (community strings, passwords). When this information is included in the Essentials Inventory, the device is considered to be managed by Essentials, and data collection from the device takes place.

Therefore, nothing happens in Essentials until the devices and their attributes are included in the inventory. Inventory Manager is the starting point for all Essentials applications.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 433
Doc 3702

16 240
L

When devices are added to Essentials, Inventory Manager (and other applications within Essentials) proceed to contact the device and collect necessary information to be stored in the database. Inventory Management can now be configured to automatically poll devices on the network to look for any changes.

If any changes are detected in hardware or software components, the inventory database will be updated and a change audit record will be created to inform the network manager of the change, and to document the event. This helps to ensure that the information displayed in the Inventory reports reflects the current state of network devices.

The Inventory application lets you:

- Import devices from databases or files.
- Export device information to files.
- Add, delete, change, and list devices in your network inventory.
- Delete devices listed in a CSV file
- Poll, update and schedule collection on devices to update your network inventory.
- Display reports and graphs of your hardware and software inventory and create Inventory custom reports.
- Check and change device attributes.
- Display a Year 2000 compliance report.
- Change system-wide configuration for SNMP, SMTP, proxy and rcp settings.
- Allow other network management systems to manipulate Essentials devices.

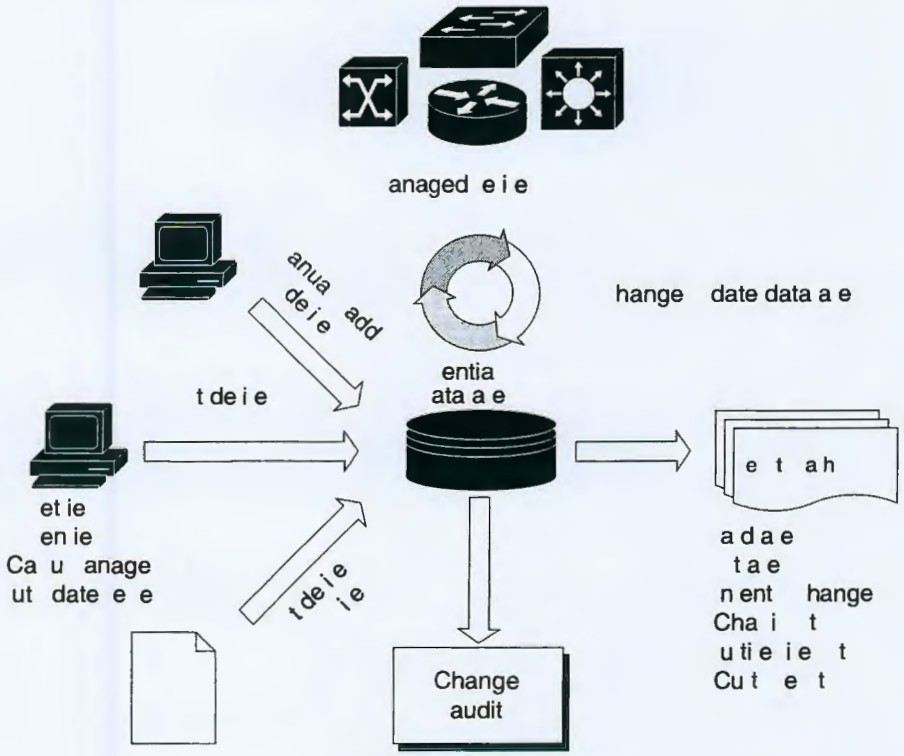
Inventory Management Functional Flow

To use Essentials at its full potential, the device attributes of the devices in the network must be included in the Inventory. Essentials does not auto–discover devices on the network. Devices must be manually added or imported into the Inventory database before information can be displayed in reports.

To simplify the process of populating the Inventory database, device information can be imported from a supported network management system, such as HP OpenView, or from a formatted text file. Essentials can also import the device data directly from Campus Manager Topology Services, which can auto–discover devices. For detailed information, see *User Guide for Campus Manager.*

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 434
Doc 3702

Figure 2-13 Inventory Management Functional Flow



You can use the various tasks in the Inventory Manager to populate the database, start tracking any changes to the inventory, and produce inventory reports. The database or inventory population is also the starting point for using other Essentials applications. See Figure 2-13.

Figure 2-14 Inventory Management Workflow

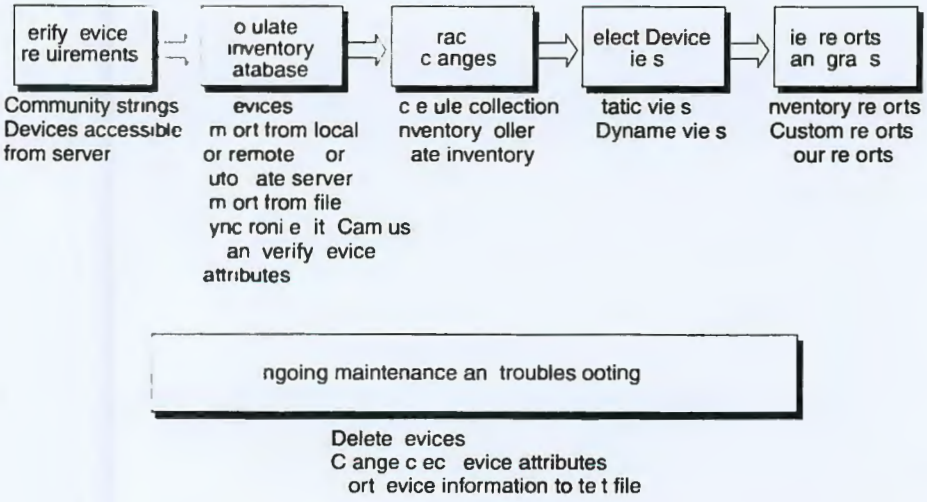


Figure 2-14 depicts the Inventory Management workflow and Essentials tasks:

- Verify device requirements to ensure that Essentials is able to communicate with the devices.
- Add or import device information into the Essentials database. An extremely important part of this step is associating device attributes with the imported or added devices. These attributes include the device community strings and appropriate passwords. These are required parameters for many of the management services (for example SNMP, Telnet) used by the various Essentials applications.
- Schedule periodic polling of devices to track changes, and keep the database up-to-date.
- Create device views to facilitate running of reports against numerous associated devices at one time.

Note The network administrator should perform ongoing maintenance, such as deleting devices that are no longer on the network, and checking device attributes to ensure that login and Telnet authentication information is correct in the Inventory database.

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 436
Doc 3702

Table 2-13 shows the tasks you can accomplish with the Inventory application.

Table 2-13 Inventory Manager Tasks

Task	Purpose	Action
List managed devices.	Determine whether a particular device is managed by displaying devices that have inventory data.	Select Resource Manager Essentials > Administration > Inventory > List Devices.
Add devices.	Add devices individually by specifying basic device information for each.	Select Resource Manager Essentials > Administration > Inventory > Add Devices.
Import devices from a file.	Import devices in bulk from a comma separated values (CSV) file or a data integration file (DIF) instead of adding them individually.	Select Resource Manager Essentials > Administration > Inventory > Import from File.
Import device data from a local host.	Import device data from a supported network management system (NMS) database residing on the local host. Device import supports these NMS databases: • HP OpenView (Solaris, and Windows only) • Cisco WAN Manager (Solaris only) • Tivoli NetView (Solaris, and Windows only)	Select Resource Manager Essentials > Administration > Inventory > Import from Local NMS.

ROS nº 03/2005 CN
CPMI - CORREIOS
Fls Nº 437
3702
Doc

Table 2-13 Inventory Manager Tasks (continued)

Task	Purpose	Action
Import device data from a remote host.	Import device data from a supported NMS database residing on a remote host. Device import supports these NMS databases: • CiscoWorks for Switched Internetworks (CWSI) • HP OpenView • Cisco WAN Manager (Solaris only) • Tivoli NetView (running on remote Solaris hosts only)	Select Resource Manager Essentials > Administration > Inventory > Import from Remote NMS.
Proxy Management	Import devices from AutoUpdate Server	Select Resource Manager Essentials > Administration > Inventory > Proxy Management.
Check status of import from local host, remote host, or file.	Determine whether a device import was successful and rectify the import if the device remains unmanaged.	Select Resource Manager Essentials > Administration > Inventory > Import Status.
Delete managed devices.	Delete managed devices, including all the related device information, that you no longer track.	Select Resource Manager Essentials > Administration > Inventory > Delete Devices.
Delete devices from a file.	Delete a group of devices from a comma separated values (CSV) file instead of deleting them individually.	Select Resource Manager Essentials > Administration > Inventory > Delete from File.
View status of deleted devices.	View the status of deleted devices and see which ones are in a suspended state.	Select Resource Manager Essentials > Administration > Inventory > Delete Device Status.

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 438
Doc 3702

Table 2-13 Inventory Manager Tasks (continued)

Task	Purpose	Action
Change device attributes.	Change these device attributes on selected devices: • SNMP read and write community strings • Telnet passwords • TACACS usernames and passwords • Enable TACACS usernames and passwords • Enable secret passwords • Local usernames and passwords • User fields • Device serial numbers	Select Resource Manager Essentials > Administration > Inventory > Change Device Attributes.
Export devices to a file.	Export your device and device access information to an output file in CSV or DIF format.	Select Resource Manager Essentials > Administration > Inventory > Export to File.
Exporting Data for AVVID Tool	AVVID Solution Analysis Tool provides a feature that allows you to export data from the Essentials inventory database. This option allows you to export the data in the format required by AVVID Solution Analysis Tool for analysis.	Select Resource Manager Essentials > Administration > Inventory > Export Data for AVVID Tool.

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 439
Doc 3702

Table 2-13 Inventory Manager Tasks (continued)

Task	Purpose	Action
Create and view inventory custom reports.	Create a customized report that gathers all or any of this information about specified devices: • IP address • User field • RAM size • Flash size • Port count • Hardware version • Card type • Serial number • SAA (Service Assurance Agent) information	Select Resource Manager Essentials > Administration > Inventory > Custom Reports. To view a previously-created report, select Resource Manager Essentials > Inventory > Custom Reports.
Define filters for change reports.	Define filters that determine what data is displayed in your inventory change reports.	Select Resource Manager Essentials > Administration > Inventory > Inventory Change Filter.
Schedule inventory collection.	Schedule polling and collection to update your network inventory.	Select Resource Manager Essentials > Administration > Inventory > Schedule Collection.
Update inventory collection.	Run inventory collection as a one-time event for specific devices.	Select Resource Manager Essentials > Administration > Inventory > Update Inventory.
Schedule device polling.	Schedule periodic polling of managed devices. Since the poller uses fewer network resources, you should schedule inventory polling to run more frequently than inventory collection.	Select Resource Manager Essentials > Administration > Inventory > Inventory Poller.
Run an inventory 24-hour report.	Determine what inventory changes were made in the last 24 hours.	Select Resource Manager Essentials > 24-Hour Reports > Inventory Change Report.

16.234
ROS nº 03/2005 - CPMI - CORREIOS
Fls. Nº 440
Doc 3702

Table 2-13 Inventory Manager Tasks (continued)

Task	Purpose	Action
View a hardware report.	View user-specified hardware information for each device.	Select Resource Manager Essentials > Inventory > Hardware Report.
View a software report.	View user-specified software information for each device.	Select Resource Manager Essentials > Inventory > Software Report.
View information about devices.	View detailed hardware, software, chassis, and interface information for multiple devices.	Select Resource Manager Essentials > Inventory > Detailed Device Report.
View a device Y2K compliance report.	View which managed devices are compliant to the year 2000. Compliance is determined by device type and software version.	Select Resource Manager Essentials > Inventory > Year 2000 Report.
View device information within device classes.	View a bar chart of the distribution of all managed devices among the recognized device classes.	Select Resource Manager Essentials > Inventory > Hardware Summary Graph.
View the software versions in each device class.	View a bar chart of the distribution of the major and minor software versions running on your selected devices in each device class.	Select Resource Manager Essentials > Inventory > Software Version Graph.
View device information in each device class.	View a bar chart showing the distribution of your selected devices in each device class.	Select Resource Manager Essentials > Inventory > Chassis Summary Graph.
View a summary of chassis slots.	View the total number of selected devices and the number of devices with free slots for each device class that supports capacity planning.	Select Resource Manager Essentials > Inventory > Chassis Slot Summary.
View the chassis slot details.	View the total slots, available slots, location, and userfield information for each device.	Select Resource Manager Essentials > Inventory > Chassis Slot Details.

ROS nº 03/2005 - CPMI - CORREIOS
Fls. Nº 441
Doc 3702

Table 2-13 Inventory Manager Tasks (continued)

Task	Purpose	Action
View details on multiservice ports.	Check the switch multiservice ports, which support voice traffic, to make sure the power supply is adequate for the number of multiservice modules installed in each switch.	Select Resource Manager Essentials > Inventory > MultiService Port Details.
Verify community strings, usernames, and passwords.	Ensure that the database used to store the community strings and passwords remains synchronized with the actual devices. Detect errors made when devices were added or imported.	Select Resource Manager Essentials > Administration > Inventory > Check Device Attributes.
View attribute check results.	View the results of updated device attributes.	Select Resource Manager Essentials > Administration > Inventory > View Check Results.
View historical data.	View all historical data associated with scheduled inventory collection. It shows the last run, duration, devices scanned, and average scan time.	Select Resource Manager Essentials > Inventory > Scan History.

ROS nº 03/2005 - CPMI - CORREIOS
Fls Nº 442
Doc 3702

Job Approval

Software Management and Configuration Management tasks allow you to set up approval checkpoints before you run a job that will change a configuration or update the software image on a device. This can help increase the security on your network, by forcing these types of high-impact jobs to be approved before they are scheduled or executed. Moreover, other CiscoWorks applications can also take advantage of this feature (for example, ACL Manager).

Job Approval is used by other applications to ensure that a job be approved before it can run. Job Approval sends job requests via e-mail to the users on the approver list of a job. If none of the approvers approves the job by its scheduled run time, or if an approver rejects the job, the job is moved to the rejected state and will not run.

When Job Approval is enabled, applications that use it require that the user do the following for each job that is scheduled:

- Assign one or more approver lists to the job
- Schedule the job to run in the future, rather than immediately

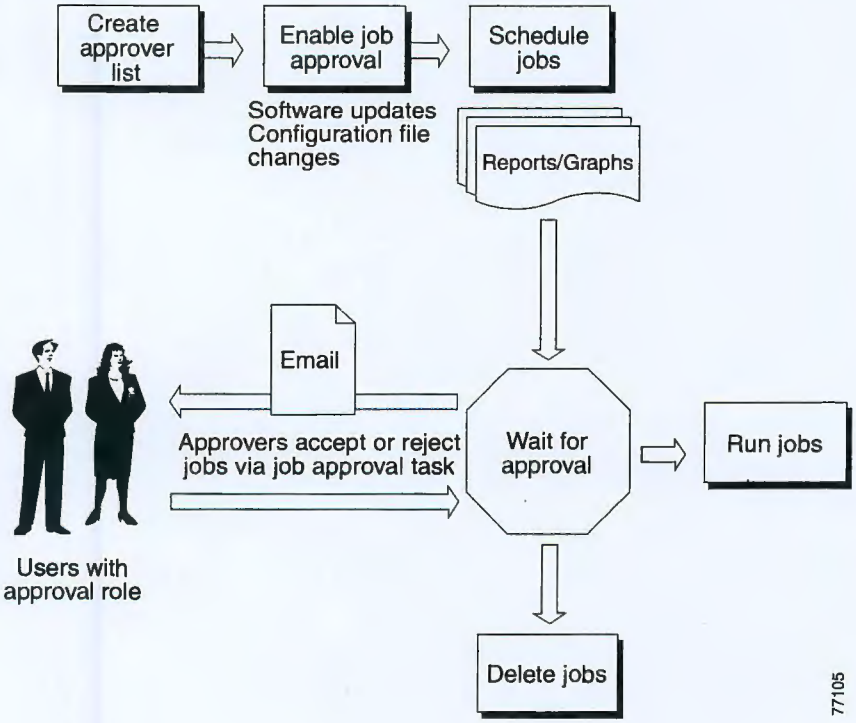
Job Approval Process

The job approval process requires that you first create an approver list; a list of CiscoWorks user accounts that must approve the job before it can be run. Users must have the role of approver to be included in an approver list.

After you have created at least one approver list, you can enable the job approval feature for Software Management, Configuration Management, or both. See Figure 2-15.

ROS nº 03/2006 - CN
CPMI - CORREIOS
Fls. Nº 443
Doc. 3702

Figure 2-15 Job Approval Workflow



The user must have the user role of system administrator or network administrator to perform this task. You must create at least one approver list before you can enable job approval. Only users who have been assigned the approver role, will be displayed in the list of valid user accounts for approval.

For Software Management, you can also be specific as to the types of jobs that require approval (new image distribution, undo image distribution, retry image distribution).

ROS nº 03/2005 - CPMI - CORREIOS
Fls Nº 444
Doc 3702

During scheduling of a job that requires job approval, the user will be queried to select an approver list. When scheduling is complete (the job must be scheduled for the future and not for immediate execution), an e-mail will be sent to all users on the approver list and the job will be placed in the job execution queue with a wait for approval status. The job will not run until at least one user on the approval list has accepted it. If anyone rejects the job, or if no one accepts the job by its scheduled time, the job will not run. The URL to this task is included in the e-mail.

The approver can only accept or reject the job and cannot change any of the operational parameters of the job. All approvers on the list and the creator of the job will receive e-mail notification when the job is either accepted or rejected.

Table 2-14 shows the tasks that can be accomplished with the Job Approval application.

Table 2-14 Job Approval Tasks

Task	Purpose	Action
Approve or reject jobs.	Approve or reject a job for which you are an approver.	Select Resource Manager Essentials > Administration > Job Approval > Approve or Reject Jobs.
Set up Job Approval.	Enable or disable the option.	Select Resource Manager Essentials > Administration > Job Approval > Edit Preferences.
Create an approver list.	Create a new approver list.	Select Resource Manager Essentials > Administration > Job Approval > Create Approver List.
Edit an approver list.	Edit an existing approver list.	Select Resource Manager Essentials > Administration > Job Approval > Edit Approver List.
Enable jobs	Enable all imported Essentials jobs.	Select Resource Manager Essentials > Administration > Job Approval > Enable Jobs.

For information on how to perform the Job Approval tasks, see the online help.

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 445
Doc 702

16.223
2

Software Management

The Software Management application automates the steps associated with upgrade planning, scheduling, downloading software images, and monitoring your network.

New Features of Software Management

The Software Management application has the following new features:

- With the remote staging and distribution feature you can select a software image, store it temporarily on a device, and then distribute the staged image to the devices that require an upgrade, in your network (**Resource Manager Essentials > Software Management > Remote Staging**).

  After the device is successfully upgraded, the stored image on the remote stage device is deleted automatically, if delete and squeeze operations are supported by the device.

  The remote staging feature is useful when the Resource Manager Essentials server and the devices (including the remote stage device you have chosen) are distributed across a WAN.

  For details, see the Essentials online help.
  (In the left navigation pane of the Essentials online help, select **Resource Manager essentials > Software Management > Remote Staging**).

- With the image-centric distribution feature, you can now select a software image and use it to perform an image upgrade on homogenous devices in your network (**Resource Manager Essentials > Software Management > Distribution > Distribute by Images**).

  For details, see the Essentials online help.
  (In the left navigation pane of the Essentials online help, select **Resource Manager essentials > Software Management > Distribution > Distributing by Images**).

ROS nº 03/2005 - CA
CPMI - CORREIOS
Fls. Nº 446
Doc - 3702

56-227
L

Benefits of Software Management

The Software Management application provides tools making it easier to store backup copies of all Cisco software images running on network devices. It also helps you to store any additional software images that you may wish to maintain, and to plan and execute software image upgrades to multiple devices on the network at the same time.

It gives you flexibility in upgrading devices with software images. You can either select a set of devices and perform an image upgrade, or select a software image and select a set of devices on which to perform the upgrade. You can even select one of your devices as a remote stage to temporarily store a software image.

It can analyze devices against software image requirements to determine device compatibility and make recommendations before performing a software upgrade.

The Software Management application can also download and list applicable images from Cisco.com, while recommending an image for the device upgrade. You should select the Cisco.com filters in Administration preferences, to avail this benefit.

If any errors occur during a software image upgrade, Software Management will allow you to roll back to the previous version. Optionally, for added security and change-management control, software images will not be downloaded unless approved by specifically assigned users. Software Management reports also allow you to track all software upgrades and monitor known bugs in the software versions running on your network.

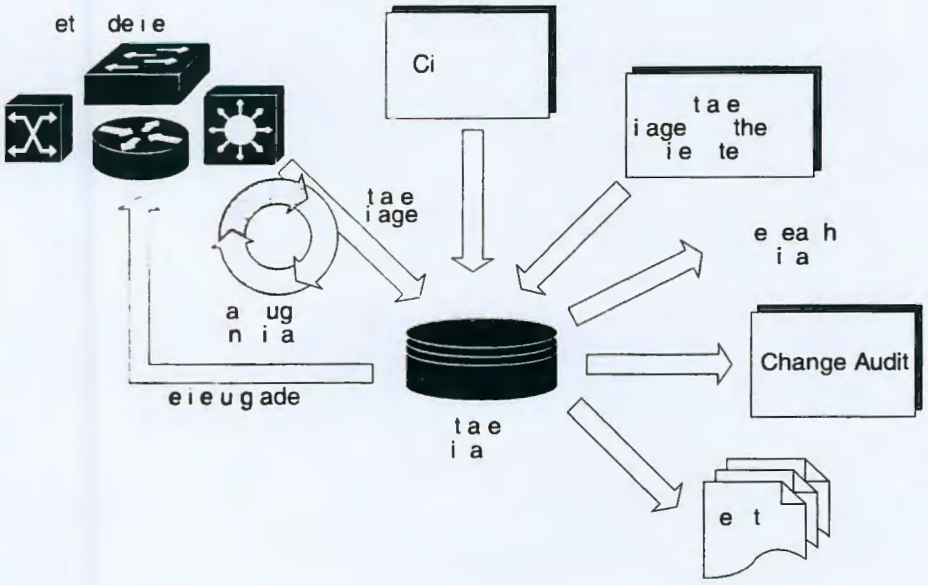
Software Management Functional Flow

Software images must be imported into Essentials to be maintained in the Software Image Library. Images can initially be imported to the Essentials Software Library from all managed Cisco devices on the network to create a baseline backup copy of all software images running on your network.

Images can also be imported from Cisco.com or the local machine to be used for software image upgrades. See Figure 2-16.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 447
Doc 3702

Figure 2-16 Software Management Functional Flow



After images are imported into the Software Image Library, the Software Management application can be configured to automatically poll devices on the network and produce a report of images running on devices that are not stored in the Essentials database. This ensures that for disaster recovery purposes, there is a backup of all software images running on the network in the software library at all times.

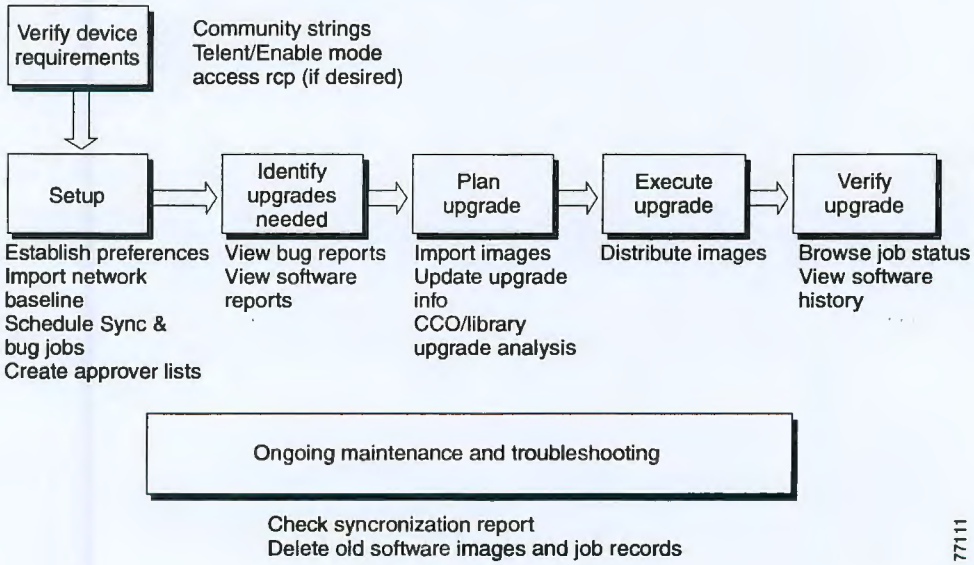
Any image that is stored in the Software Image Library can be used to perform a software upgrade. Each step of the process is recorded in the distribution, so if there is a failure, the network administrator will know the reasons for the failure. Software Manager maintains a log of all software upgrades, to make it easy to identify and track when software modifications are made to devices.

In addition, whenever a change is made to the software image on a device, a change record is sent to the Change Audit application, which collects and organizes all changes to network devices.

Software Management can also be configured to periodically check Cisco.com for known software bugs, and produce a report to show all bugs that affect devices on your network.

RQS nº 03/2005 - CPMI - CORREIOS
Fls Nº 448
3702
Doc

Figure 2-17 Software Management Workflow



The image depicts the Software Management workflow and associated tasks within Essentials (see Figure 2-17):

- Device requirements must be verified to ensure that Essentials will be able to access the devices to retrieve and upgrade software images.
- Perform setup tasks to begin using Software Management. Setup tasks include setting preferences that will be used for all Software Management import and upgrade jobs, creating any approver lists that will be used to approve software jobs, and scheduling jobs to periodically synchronize the software library with network devices and check Cisco.com for known software bugs.
- When Software Manager is set up, software and bug reports can be used to help identify when software upgrades might be needed.
- If a software upgrade is required, Software Management features can be used to analyze whether or not devices can accommodate the new image, and to actually distribute the new images to devices on the network.
- In addition, ongoing maintenance should be performed to ensure that a copy of every image running on the network is stored in the Essentials Software Library, and to remove images no longer needed from the Software Library.

CPMI - CORREIOS
Fls Nº 449
3702
Doc

16.224
2

Table 2-15 shows the tasks you can accomplish with the Software Management application.

Table 2-15 Software Management Tasks

Task	Purpose	Action
Set up your Software Management preferences.	Specify information such as history page size, the directory where images are stored, the pathname of the user-supplied script to run before and after each device software upgrade. Specify if the images on Cisco.com should also be included during image recommendation of the device, and also specify the Cisco.com filters so that only those images that match the filter criteria are selected.	Select Resource Manager Essentials > Administration > Software Management > Edit Preferences.
Add images to the library.	Import images from all Software Management supported devices in your network into the Software Image Library.	Select Resource Manager Essentials > Software Management > Library > Add Images.
	Download images from Cisco.com into the Software Image Library.	
	Add images from a file system to the Software Image Library.	
Browse the library.	Generate a report of all the images in the Software Image Library. You can also delete images from the image library and edit image attributes.	Select Resource Manager Essentials > Software Management > Library > Browse Images.
Search the library.	Generate a report of a subset of images in the Software Image Library, based on details such as, device type, image type, and version. You can also delete images from the image library and edit image attributes.	Select Resource Manager Essentials > Software Management > Library > Search for Images.

CPMI - CORREIOS
Fls. Nº 450
Nº 3702
Doc

Table 2-15 Software Management Tasks (continued)

Task	Purpose	Action
View a synchronization report.	Generate a synchronization report to determine which Software Management-supported devices are running software images not in the Software Image Library.	Select Resource Manager Essentials > Software Management > Library > Synchronization Report.
Schedule a synchronization job.	Specify the date, time, and frequency of a synchronization job. Cancel a scheduled synchronization job.	Select Resource Manager Essentials > Administration > Software Management > Schedule Synchronization Job.
Create approver lists.	Specify who can approve the various tasks necessary during a software upgrade.	Select Resource Manager Essentials > Administration > Job Approval > Create Approver List.
Edit or delete approver lists.	Edit and delete the list specifying who can approve tasks during a software upgrade.	Select Resource Manager Essentials > Administration >Job Approval > Edit Approver List.
Schedule image upgrade jobs.	Select devices and schedule software image upgrades to those devices.	Select Resource Manager Essentials > Software Management > Distribution > Distribute by Devices.
	Select a software image and use it to perform an image upgrade on the suitable devices in your network.	Select Resource Manager Essentials > Software Management > Distribution > Distribute by Images.
	Select a software image and use one of your devices as a remote stage to temporarily stage the image. Then upgrade suitable devices in your network with this staged image.	Select Resource Manager Essentials > Software Management > Remote Staging > Remote Staging and Distribution.
	Undo the upgrade and roll back to the previous image, after you have scheduled and completed upgrading the image.	Select Resource Manager Essentials > Software Management > Job Management > Browse Jobs.
Plan an upgrade from Cisco.com.	Determine the impact to and prerequisites for a new software deployment using images that reside in Cisco.com.	Select Resource Manager Essentials > Software Management > Distribution > CCO Upgrade Analysis.

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 451
Doc 3702

16.222
L

Table 2-15 Software Management Tasks (continued)

Task	Purpose	Action
Plan an upgrade from the library.	Determine the impact to and prerequisites for a new software deployment using images in your software library.	Select Resource Manager Essentials > Software Management > Distribution > Library Upgrade Analysis.
Review scheduled jobs or undo an upgrade.	Review, or remove scheduled jobs. If the job is in the pending state, you can modify the schedule time. You can also retry failed jobs and undo completed image upgrade jobs.	Select Resource Manager Essentials > Software Management > Job Management > Browse Jobs.
View consolidated job information.	View a report of device upgrade results for selected jobs.	Select Resource Manager Essentials > Software Management > Job Management > Consolidated Job Report.
View recent software upgrade results.	Generate a report summarizing the most recent device software upgrade results stored in the history database.	Select Resource Manager Essentials > 24-Hour Reports > Software Upgrade Report.
Mail or copy log files.	Mail or copy log files if requested to do so by Cisco Support after you report abnormal Software Management behavior. Delete unnecessary log files after mailing or copying them.	Select Resource Manager Essentials > Software Management > Job Management > Mail or Copy Log File.
Browse history.	Generate a summary of device software upgrades stored in the history database.	Select Resource Manager Essentials > Software Management > History > Browse History.
Search history by device.	Generate a summary of software upgrades for selected devices.	Select Resource Manager Essentials > Software Management >History > Search History by Device.
Search history by user.	Generate a summary of software upgrades performed by a particular user.	Select Resource Manager Essentials > Software Management > History > Search History by User.

BOS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 452
3702

Table 2-15 Software Management Tasks (continued)

Task	Purpose	Action
Browse bugs.	Compare images running on Software Management supported devices in your network with the images on Cisco.com and report catastrophic and severe bugs specific to your network. Identify devices running deferred software images.	Select Resource Manager Essentials > Software Management > Bug Reports > Browse Bugs.
Schedule a Browse Bugs job.	Specify the date, time, and frequency of a Browse Bugs job. Cancel a scheduled Browse Bugs job.	Select Resource Manager Essentials > Administration > Software Management > Schedule Browse Bugs Job.
Browse bugs by device.	Generate a summary of software image bugs for a group of devices.	Select Resource Manager Essentials > Software Management > Bug Report > Browse Bugs by Device.
Locate devices by bugs.	Search for known bugs that could affect the devices on your network.	Select Resource Manager Essentials > Software Management > Bug Report > Locate Devices by Bugs.
Update upgrade information.	Update the source for upgrade knowledge base files. The source can be either Cisco.com or a local file.	Select Resource Manager Essentials > Administration > Software Management > Update Upgrade Info.

Syslog Analysis

The Syslog Analysis application lets you centrally log and track system error messages from Cisco devices. Use logged error message data to analyze router and network performance. You can store a maximum of 1 million messages for up to 14 days.

Before you can use Syslog Analysis, you must configure your devices to forward messages either to the Essentials server directly or to a system on which you have installed a Syslog Analyzer Collector (SAC).

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 453
Doc 3702

The collector filters and forwards the messages to the Essentials server. For more information on configuring network devices for Syslog Analysis, and for installing a remote SAC, see the online help.

New Features of Syslog Analysis

The Syslog Analysis application has the following new features:

- You can now store syslog messages in the database for a maximum of 14 days, including today (**Resource Manager Essentials > Administration > Syslog Analysis > Change Storage Options**).

  For details, see the Essentials online help.
  (In the left navigation pane of the Essentials online help, select **Resource Manager Essentials > Syslog Analysis > Administrative Procedures > Changing Storage Options**)

- You can back up the purged syslog messages at a location that you have specified (**Resource Manager Essentials > Administration > Syslog Analysis > Change Storage Options**). The messages will be stored in the CSV format.

  If you choose to back up the purged messages, you will also be allowed to select the size of the backup file. You can also specify the email addresses, for receiving an email notification, after the backup file crosses the size limit that you have specified.

  For details, see the Essentials online help.
  (In the left navigation pane of the Essentials online help, select **Resource Manager Essentials > Syslog Analysis > Administrative Procedures > Changing Storage Options**)

- The Remote Syslog Analyzer Collector (RSAC) now avoids restart, by sensing the reboot of its specified server.

  When the server goes down, the RSAC goes into the polling mode and re-connects automatically when its specified server restarts. When the server is down RSAC sends the messages to a local log file. The default location for this log file is the RSAC installed directory.

  For details, see the Essentials online help.
  (In the left navigation pane of the Essentials online help, select **Resource Manager Essentials > Syslog Analysis > Administrative Procedures > Remote Syslog Analyzer Collector (RSAC)).**

46 219

Syslog Analysis Functional Flow

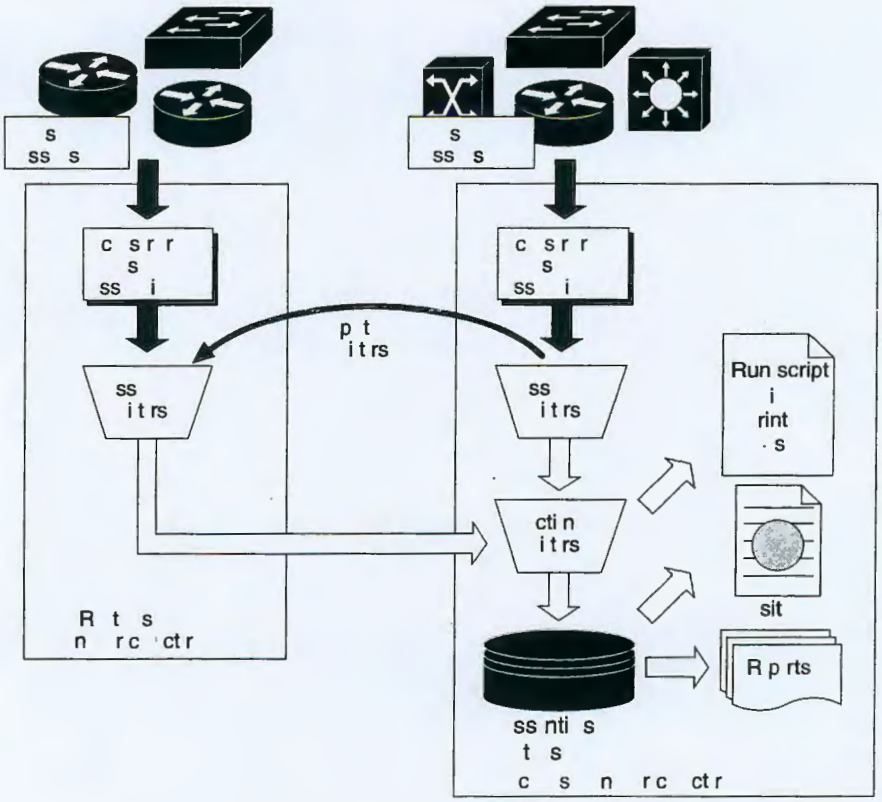
To use the Syslog Analysis features, devices must be configured to forward syslog messages to the Essentials server. When devices are configured correctly, all syslog messages will be forwarded to the Essentials server or a remote SAC.

These messages are stored on the server and are periodically read by the Syslog Analyzer process (approximately every 30 seconds). The Syslog Analyzer reads and processes the messages in the Syslog file, applies any filters that have been defined, and writes remaining messages to the Essentials Syslog message database. All syslog messages that can be read, and that are not filtered out, will be written to the Essentials Syslog database. The database is then used to produce Syslog reports and initiate user-defined scripts.

To reduce the load on the network and the CiscoWorks Server, SACs can be configured on remote workstations to collect and periodically forward syslog messages to the Essentials server. Any filters that have been defined on the Essentials server will be synchronized on SACs during scheduled updates. See Figure 2-18.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 455
Doc 3702

Figure 2-18 Syslog Analysis Functional Flow

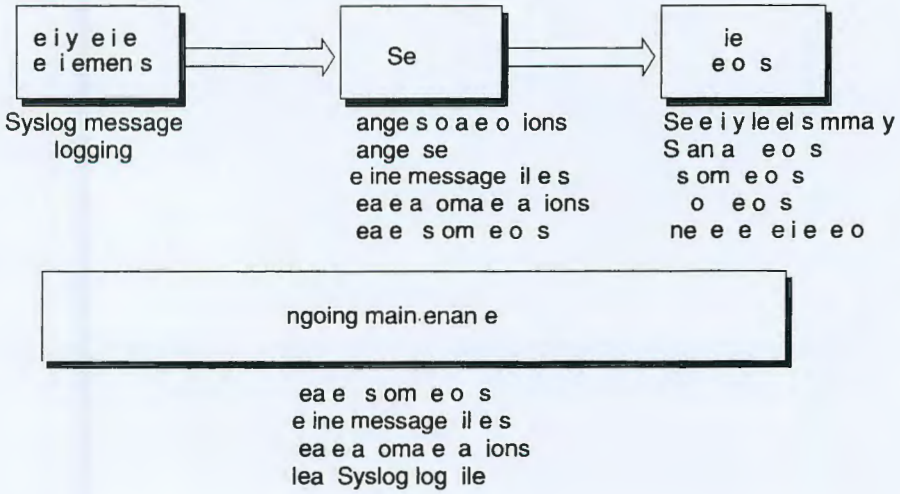


Syslog Analysis on Windows

Since system message logging is not part of the Windows operating system, CiscoWorks adds a logging service—CMF Syslog Service, when it is installed on Windows systems. All system messages are stored in the Syslog.log file under the ciscoworks/log directory on the server. The Syslog Analyzer then reads this file to populate the syslog database. See Figure 2-19.

Syslog Analysis Workflow

Figure 2-19 Syslog Analysis Workflow



The above chart depicts the Syslog Analysis workflow and associated tasks within Essentials. Syslog Analysis will automatically store any supported syslog messages that are forwarded from devices. You must ensure that devices are configured to forward messages to the Essentials server or a remote SAC.

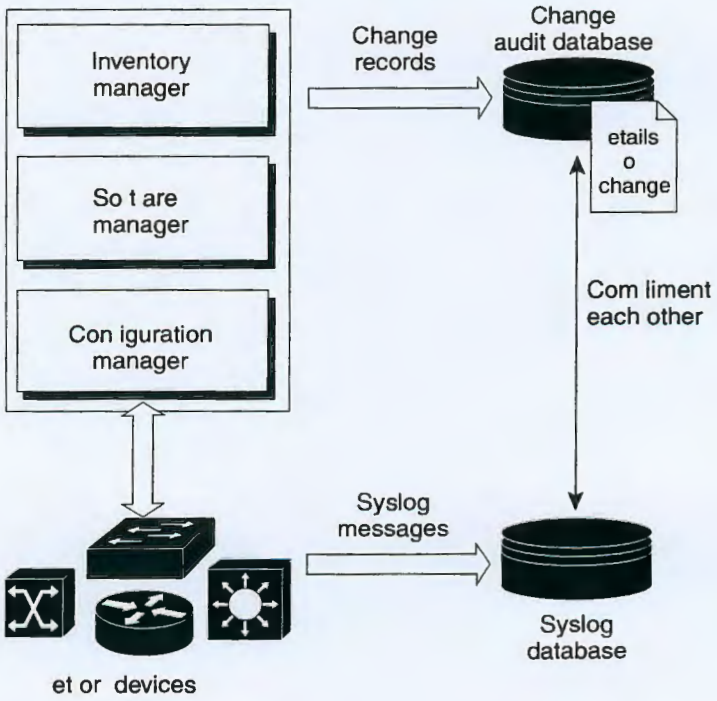
After the devices are configured properly, you can view Syslog reports at any time. You are required to perform Syslog Analysis setup tasks only if you want to filter out specific syslog messages, change how long syslog messages are stored, display syslog messages in a custom URL, group syslog in a custom report, or execute a user-defined script when specified syslog messages are detected.

Syslog Vs. Change Audit

Many actions that trigger change audit records will also trigger generation of syslog messages. Change Audit complements syslog message logging by providing additional details about some changes, tracking changes for devices, and providing multiple ways to organize and view changes to network devices. See Figure 2-20.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 457
3702
Doc

Figure 2-20 Syslog Analysis Vs. Change Audit Workflow



Changes in the network, such as a configuration change or the upload of a new Cisco IOS software image, can result in a device triggering a syslog message.

Some of these syslog messages in turn cause the inventory or the configuration management applications to poll the device and update the Essentials data appropriately. These applications will also log a record with the change audit application.

Besides, if the inventory or the configuration management applications independently detect changes to the network, they will poll the device, update the Essentials data, and log a change audit record.

For example, when a device sends a syslog message about a change in device configuration, this is passed on to Configuration Management, which determines the exact nature of the change. It retrieves the new configuration file, and then writes a change record into the Change Audit log.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls: 458
Nº 3702
Doc:

Table 2-16 shows the tasks you can accomplish with the Syslog Analysis application.

Table 2-16 Syslog Analysis Tasks

Task	Purpose	Action
Set up data storage options.	Configure how long to store data, the maximum number of messages to store, and the message source. You should restart daemon manager and CMF Syslog Service (CRM Logger) for the Message Source changes to take effect. If you want to back up the purged data, you can specify the back up details—the backup directory, backup file size, email address for notification when the backed up file exceeds the specified size, etc.	Select Resource Manager Essentials > Administration > Syslog Analysis > Change Storage Options.
Define custom reports.	Create new reports and select the message types to be included in each report. Modify the standard reports provided with Essentials Delete reports that you no longer use. You can also enable 24-hour reporting.	Select Resource Manager Essentials > Administration > Syslog Analysis > Define Custom Reports.
Define automated actions.	Add and modify command-line instructions to be executed automatically whenever Syslog Analyzer receives a specific message type. Modify existing actions and delete actions you no longer use. You can also enable or disable actions.	Select Resource Manager Essentials > Administration > Syslog Analysis > Define Automated Action.
Define message filters.	Exclude messages you do not want reported. Enable or disable filtering. Modify or delete filters.	Select Resource Manager Essentials > Administration > Syslog Analysis > Define Message Filter.

Table 2-16 Syslog Analysis Tasks (continued)

Task	Purpose	Action
View status.	View the status of your Syslog Collector. You can view the status of the local and all the remote collectors that have been configured to use the Essentials server as the forwarding server.	Select Resource Manager Essentials > Administration > Syslog Analysis > Syslog Collector Status.
Change your URL.	Link your message reports to a customized web page. You can do this only if you know basic CGI programming.	Select Resource Manager Essentials > Administration > Syslog Analysis > Change User URL.
Generate a severity level summary.	Generate summaries of messages about selected devices sorted by severity level.	Select Resource Manager Essentials > Syslog Analysis > Severity Level Summary.
Generate a standard report.	Generate a system message report for a device or a set of devices. You can generate the report for the current date, or for any date in the previous week, or for all dates. You can include all the messages, or choose the severity level or alert type for which the report should be generated.	Select Resource Manager Essentials > Syslog Analysis > Standard Reports.
Generate a custom report.	Generate a full custom syslog report. You can select a report from the custom syslog reports that are defined in Administration.	Select Resource Manager Essentials > Syslog Analysis > Custom Reports.
	Generate a summary custom syslog report. You can see a summary of the various reports.	Select Resource Manager Essentials > Syslog Analysis > Custom Report Summary.
Generate a report for unmanaged devices.	Generate a syslog information report on all unmanaged devices in your network.	Select Resource Manager Essentials > Syslog Analysis > Unexpected Device Report.

CPMI - CORREIOS
Fls Nº 460
3702

Table 2-16 Syslog Analysis Tasks (continued)

Task	Purpose	Action
Generate a report for workflow devices.	Capture syslog messages that are generated from MCS servers running WF application.	Select Resource Manager Essentials > Syslog Analysis > WorkFlow Report.
Generate a 24-hour syslog report.	Generate a report for the past 24 hours. The report can be a custom report created by a system administrator or a default report.	Select Resource Manager Essentials > 24-Hour Reports > Syslog Messages.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 461
Nº 3702
Doc

16.166

Segurança Tipo 2 doc 11

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 462
3702

Cisco Systems

White Paper

CiscoWorks **VPN/Security Management Solution** (VMS) 2.1 Deployment Guide

Introduction

The Challenge

One of the challenges of network management is the ability to have a solution that is flexible and can adapt to the changing needs of a network. While it makes sense to have applications that provide basic network management functionality regardless of function, the network environment must also be considered. In this case, it makes more sense to have a focused set of tools for management. For example, a tool that focuses on managing Quality of Service (QoS) levels is not necessarily (and most likely not) going to be very good at managing a server farm topology.

Growth and Enhancements in Network Security

If we look at the network as a strategic asset to the enterprise, network management clearly becomes an important factor in the success of the company. When we consider the evolution of business applications running across the traditional data network including e-commerce, business-to-business transactions, voice over IP (VoIP), the need to provide secure network connections grows. As a result, we have witnessed a proliferation in virtual private networks (VPNs) and an enhanced awareness of network security, setting the stage for reliable security management.

Paper Objective

The purpose of this paper is to provide guidance on how to effectively deploy CiscoWorks VPN/Security Management Solution (VMS). Covered topics include: server, installation, and operating system requirements; reference topology; metrics to monitor; and device configuration considerations. This is intended to supplement the CiscoWorks VMS Quick Start Guide and User Manual. We address such questions as: Which products are included and what are they used for? How many servers will be needed? What devices can be managed with this application? By answering these questions, we can provide some basic best practices for managing specific Cisco security technology.

What It Does Not Do

This paper does not replace User Guides (and other product documentation). It does not go into comprehensive detail about the various features or capabilities of the products.

Intended Audience

This paper is intended for audiences who are already familiar with network security, VPNs, firewalls, and intrusion detection. The audience should already have a basic understanding of these concepts and tools; our goal is to show how best to deploy CiscoWorks VMS in a production environment.

RDS nº 03/2005 - CD
CPMI CORREIOS
Fls. Nº 463
Nº 3702
Doc

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

High-level Overview of CiscoWorks VMS 2.1

What Does It Do?

The CiscoWorks VMS solution is a set of integrated tools that provide a comprehensive solution for VPN and security management. CiscoWorks VMS features are positioned for configuring, monitoring, and troubleshooting enterprise VPNs, firewalls, and network- and host-based intrusion detection systems (IDS). VMS provides key features to assist customers in the deployment, monitoring, and management of their security-specific hardware. It also provides the operational management support, software distribution, configuration archive, change-audit, and syslog management for different elements of a Cisco security infrastructure. VMS provides a scalable solution that addresses the needs of small- and large-scale VPN and security deployments.

CiscoWorks VMS 2.1 Components

The CiscoWorks VPN/Security Management Solution (CiscoWorks VMS) consists of installable software components for flexible deployment options. Table 1 lists the different CiscoWorks VMS modules and their basic usages.

Table 1 CiscoWorks VMS 2.1 Modules

VMS Module	Usage
Auto Update Server	Permits configurations to be pulled from update server
CD-One/CiscoView	Provides graphical device management
Cisco IDS Host Sensor and Console	Configures host-based IDS to protect critical servers
Cisco Secure Policy Manager	Configures Cisco PIX Firewall, Cisco IOS Software firewall, and VPN
Common services	Provides a set of common software and services for the Management Centers
Management Center for IDS Sensor	Configures network-based IDS
Management Center for PIX Firewalls	Configures PIX Firewalls
Management Center for VPN routers	Configured VPN routers
Monitoring Center for Security	Monitors network and host-based IDS events, IOS and PIX syslog
Resource Manager essentials	Provides operational management, such as software distribution, change audit, syslog analysis
VPN Monitor	Monitors IPSec-based site-to-site and remote access VPN

These components can be classified into three distinct categories: Core asset management applications, monitoring applications, and security configuration applications. This section details some of the basic features associated with each product.

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS
CPMI CORREIO
Fls. Nº 464
Nº 3702
Doc:

Core Asset Management Applications

CD-One (CiscoView)

CD-One software provides the Common Management Foundation (CMF) for CiscoWorks. This includes basic components on the management server such as the web server, common database, polling engine, and so forth. In many deployments, this is the first CD to be installed from CiscoWorks VMS since it is the prerequisite for other applications. In addition to the CMF, CD-One provides the web-based CiscoView application. CiscoView provides graphical browser-based access to real-time devices status and simple network management protocol (SNMP) configuration capabilities.

CiscoWorks Resource Manager Essentials

CiscoWorks Resource Manager Essentials (RME) provides the basic network management tools for day-to-day network management, including inventory, configuration, change audit, and syslog. RME also provides additional VPN management capabilities. Network administrators can now produce device configuration, software image, and syslog reports specific for VPN environments.

Security Monitoring Applications

CiscoWorks VPN Monitor

CiscoWorks VPN Monitor allows users to monitor the status of their VPN devices and tunnels. This application collects, stores, and reports statistics for VPN-capable devices, including Cisco VPN routers, and the Cisco VPN 3000 Series Concentrator. The VPN Monitor supports the two major classes of VPNs (site-to-site and remote access) as well as multiple tunneling protocols, including Layer 2 Tunneling Protocol, Point-to-Point Tunneling Protocol (PPTP), and IP security (IPsec).

CiscoWorks Monitoring Center for Security

The CiscoWorks Monitoring Center for Security, or Security Monitor, monitors IDS events from various Cisco devices. These include network IDS sensor appliances, Cisco Catalyst® 6000 IDS modules, Cisco IOS® Software IDS syslog messages, Cisco PIX® Firewall syslog messages, and Cisco host IDS events.

Security Configuration Applications

CiscoWorks Common Services Software

CiscoWorks Common Services Software includes basic components of the management server such as the Web server, common database, polling engine, and so forth. In many deployments, this is the first CD to be installed because it is the prerequisite for the Management Center tools in the CiscoWorks VMS bundle.

CiscoWorks Management Center for VPN Routers

CiscoWorks Management Center for VPN Routers (Router MC) is a VPN configuration and deployment tool for Cisco VPN routers with Cisco IOS Software. Router MC is a Web-based application installed on top of Common Services.

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

ROS nº 03/2005
CPMI CORREIOS
Fls. Nº 465
Nº 3702
Doc

CiscoWorks Management Center for PIX Firewalls

Management Center for PIX Firewalls (PIX MC) is a complete firewall and access rule policy configuration tool Cisco PIX Firewalls. You can configure new Firewalls and import configurations from existing firewalls. PIX M also provides a powerful tool for controlling changes made to your network, showing configuration and status changes. PIX MC is a Web-based application installed on top of CiscoWorks Common Services.

CiscoWorks Auto Update Server

The CiscoWorks Auto Update Server (AUS) is used to store and upgrade device configuration files and software images. Cisco PIX Firewall devices periodically contact the AUS to request configuration and software updates. I this way. PIX Firewall devices are actively kept up to date. AUS is a Web-based application installed on top of CiscoWorks Common Services.

CiscoWorks Management Center for IDS Sensors

CiscoWorks Management Center for IDS sensors (IDS MC) is an IDS configuration and deployment tool for Cisc IDS sensor appliances and Cisco IDS Modules. IDS MC is a web-based application installed on top of Common Services.

Cisco IDS Host Sensor

Working as a complementary technology to IDS MC and Security Monitor, the Cisco Host Intrusion Detection System (HIDS) application protects critical servers and hosts by integrating with the operating system. By intercepting system calls to the kernel, Cisco HIDS software can protect the users' hosts by identifying attacks and preventing access to resources and unauthorized transactions.

Cisco Secure Policy Manager

Cisco Secure Policy Manager (CSPM) is a policy-based application that allows network and security administrators to define and deploy perimeter security policies on mixed Cisco PIX Firewalls and Cisco IOS routers with the firewall feature set. CSPM also facilitates the deployment of site-to-site, mixed-environment VPN topologies.

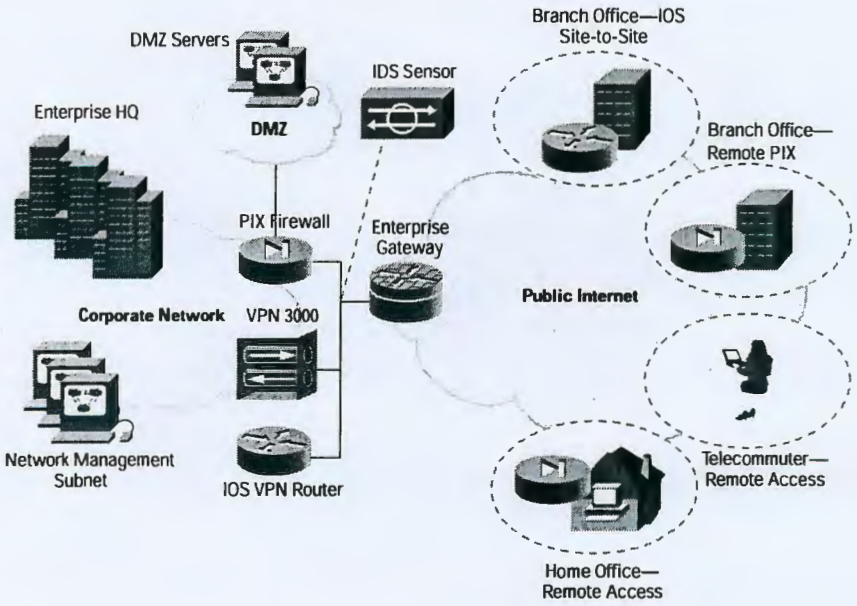
Reference Topology

In order to describe how best to deploy the CiscoWorks VMS, we will use a reference network topology that shows the different aspects of VPN and network security (Figure 1). While obviously not identical to most customer environments, it does serve to provide a holistic view of a secure network. The intent is that by providing this reference, readers will be able to select the different components that best represent their topology and hence, understand how best to deploy CiscoWorks VMS in their environment.

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN
CPMI - CORREIOS
466
Nº Doc 3702

Figure 1
Reference Security Topology



The infrastructure involved:

a. Enterprise Gateway: This is a Cisco IOS router with the firewall feature set. The main purpose of this device is to perform the gateway routing and the basic frontline firewall functionality.

b. Cisco PIX Firewall: The Cisco PIX Firewall provides the comprehensive firewall functionality for this enterprise network. By strategically placing these devices at network access points, the corporate network resources are protected as a result of this firewall.

c. Cisco 800, 1700, 2600, 3600, 7100 or 7200 Series routers: Cisco routers act as site-to-site VPN termination points. In a hub-and-spoke VPN topology, the high-end VPN routers act as hubs, and the small- to medium-sized routers act as spokes.

d. Cisco VPN 3000 Series Concentrator: The VPN 3000 Series Concentrator is designed to provide scalable remote access VPN termination. In this topology the concentrator terminates VPN connections with a variety of remote access environments, VPN client software, and tunneling protocols (IPSec, L2TP, PPTP).

e. Cisco VPN remote-access client software: This software allows remote access users to connect to the corporate network via VPNs.

f. Cisco IDS Network Sensor: This device sits on a network segment and passively "listens" to the traffic, inspecting it against a database of common attack signatures. It forwards IDS event information to the monitoring station.

g. Cisco host-based IDS agents: Software that sits on critical network servers that protect individual hosts from intrusion and attacks. Events are forwarded to a central monitoring console.

h. Network Management Subnet: This subnet represents a dedicated network segment for the network management servers. The components of CiscoWorks VMS will reside in this subnet to manage the different pieces of the infrastructure.

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

i. Demilitarized zone (DMZ) Servers: This subnet represents a dedicated network segment for publicly accessible network servers. Generally, this includes e-mail, Web, File Transfer Protocol (FTP) servers, and in our case will include the Auto Update Server.

Within our reference topologies, we will be focusing on several pieces of the infrastructure that CiscoWorks VMS manages. That is not to say that the network management applications within VMS cannot manage other pieces (such as Cisco Catalyst switches), but these are the components that should be the focal point of VMS. These components include:

Enterprise HQ

This includes the network management servers, internal firewalls, VPN termination points (both hub routers and VPN concentrators), and IDS sensors. Access to the DMZ portion of the network will be controlled by internal firewalls and also have publicly accessible servers.

Remote Access Sites

The remote access sites in our topology contain the remote Cisco PIX Firewalls, remote IOS VPN routers, and remote VPN clients. These pieces of the infrastructure are responsible for VPN termination and firewall access policy at the remote site.

Software Requirements for CiscoWorks VMS

CiscoWorks VMS is composed of a series of tools that reside on a network management server (or servers). This section covers the prerequisite software needed in order to install and run the components within VMS. Primarily, this refers to operating system (OS) support. For almost every application in the VMS bundle, the supported OS is Windows 2000 Professional or Server. This is summarized in Table 2.

Table 2 Supported OS for CiscoWorks VMS Modules

CiscoWorks VMS Module	Windows Support	Solaris Support
CD-One	X	X
Resource Manager Essentials	X	X
VPN Monitor	X	X
Common Services	X	
Management Center for PIX Firewalls	X	
Auto Update Server	X	
Management Center for VPN routers	X	
Management Center for IDS Sensor	X	
Monitoring Center for Security	X	
Cisco IDS Host Sensor and Console	X[1]	
Cisco Secure Policy Manager	X	

1. Windows NT 4.0 Server, Enterprise Server (SP4 or later), Windows 2000 Advanced Server

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RGS nº 03/2003 - CN
CPMI - CORREIOS
Fls. Nº 468
Doc 3702

To run the CiscoWorks VMS components on a Windows 2000 system, the following requirements must be considered:

- Windows 2000 (Service Pack 2 or later)
- IE 5.5 SP2 or later
- ODBC Driver Manager 3.510 or later
- NTFS File System
- Do not install VMS on a server that is a:
  - Primary domain controller
  - Backup domain controller
  - Terminal server

Mitigating Threats

Now that we have the basic hardware and software requirements, we must consider how to configure the servers themselves to be ready for management. As a general security axiom, to secure hosts, pay careful attention to each of the components within the systems. Keep all systems up to date with the latest patches, fixes, and so forth. In the particular case of VMS, it is important to have the latest Windows 2000 patches and hot-fixes for security. Following is a detailed checklist of items to make sure the Windows 2000 server is ready to be used as a management server:

- Install the operating system on its own partition
- Use strong passwords
- Avoid creating network shares
- Disable unnecessary accounts
- Secure the Registry
- Apply all hot-fixes and security patches
- Disable unused and unneeded services (at a minimum, Windows requires the following services to run: DNS Client, Event Log, Plug & Play, Protected Storage, and Security Accounts Manager. Do not install IIS.)
- Disable all network protocols except Internet Protocol (TCP/IP)
- Monitor the security of your system regularly
- Limit physical access to your server
- Do not install remote access or administration tools on the server
- Periodically run a virus scanning application on the server

Hardware Considerations for CiscoWorks VMS

Along with the software requirements, be aware of the hardware requirements for the CiscoWorks VMS bundle. Then the inherent challenge is deciding how best to deploy the different applications in the solution. Since there are eleven installable software applications, there are numerous combinations in which to deploy them.

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 469
Nº 3702
Doc

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Platform and Specs

The following server system requirements are specified in the VMS bundle documentation:

- Pentium III 1GHz CPU
- 1 GB RAM
- 2 GB virtual memory
- 9 GB free hard disk space

These are minimum requirements, and consideration should be given to the difference in recommended system specifications based upon different sized networks and configurations. For example, consider three different sized configurations: small, medium, and large. The first thing to think about is scalability. In other words, how many devices equate to a small, medium, and large configuration?

Scaling

Each application within CiscoWorks VMS has a different scalability metric. Table 3 provides the theoretical maximum for each of the applications.

Table 3 Theoretical Scale Limits for CiscoWorks VMS Applications

CiscoWorks VMS Module	Scalability Metric (tested up to[1])
IDS MC	300 IDS sensors
Security Monitor	500 events/sec[2]
PIX MC	1000 PIX Firewalls
AUS	1000 PIX Firewalls
Router MC	1000 VPN routers
CSPM	200 devices
RME	5000 devices inventory, 1000 devices availability
VPN Monitor	30 devices on dashboard (hard limit)
Cisco IDS Host Console	300 host agents

1. The theoretical scale limits define what the tools have been tested up to. The numbers are stated as a guideline to guarantee reasonable performance and user experience. Although possible, it is not recommended to exceed these metrics.
2. If the volume of security events exceeds 500/second for extended periods of time, it is recommended that users consider a monitoring product from a partner-vendor that can handle higher event volumes.

These are not software-imposed limits, but rather the scale limitations based on testing maximums. For example, if a user wants to add device number 1001 to Router MC, the software will allow it. However, from a support standpoint, we do not recommend doing this.

Also note that the specifications for the minimum recommended hardware system for CiscoWorks VMS are based on testing and performance statistics for ONE (not all) of the applications in the bundle. For example, if you are using IDS MC to manage 300 sensors (the theoretical maximum), we do NOT recommend using any other applications on that server. If you plan to heavily use more than one application within VMS, it is highly recommended to put them on separate servers.

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

The following tables list some of the more resource-intensive applications within the bundle, and configuration is broken down into small, medium, and large configuration metrics in Tables 4-6, respectively.

Table 4 Small Configuration Metrics (reflects restricted CiscoWorks VMS license model)

CiscoWorks VMS Module	Scalability Metric (up to)
IDS MC	20 IDS sensors
Security Monitor	200 events/sec
PIX MC	20 PIX Firewalls
AUS	20 PIX Firewalls
Router MC	20 VPN routers
CSPM	20 devices

Table 5 Medium Configuration Metrics (This configuration represents the majority of the CiscoWorks VMS customer base):

CiscoWorks VMS Module	Scalability Metric (up to)
IDS MC	100 IDS sensors
Security Monitor	300 events/sec
PIX MC	100 PIX Firewalls
AUS	100 PIX Firewalls
Router MC	100 VPN routers
CSPM	50 devices

Table 6 Large Configuration (Reflects the theoretical maximum scalability metrics.)

CiscoWorks VMS Module	Scalability Metric (up to)
IDS MC	300 IDS sensors
Security Monitor	500 events/sec
PIX MC	1000 PIX Firewalls
AUS	1000 PIX Firewalls
Router MC	1000 VPN routers
CSPM	200 devices

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

16.156
L

Server Sizing

Based on these factors, a closer examination of the recommended server sizing for each configuration is now possible. It is important to note that these specifications are minimum requirements for individual applications and are frequently exceeded in many deployments. The general rule of thumb here is, if it is necessary to choose one metric that will have the greatest affect on performance, then increase the amount of RAM. It is also important to pay attention to the scale limits of each application. If you are approaching some of those theoretical limits, it might be a good idea to increase the horsepower of your VMS server(s). For example, it is not out of the question to see a P4 2.2GHz CPU with 4 GB of RAM running VMS applications. For a general guideline, please see Table 7.

Table 7 Server Recommendations for CiscoWorks VMS Configurations

Configuration	Small	Medium	Large
CPU	PIII 1GHz	PIII 1.4GHz	P4 2.0GHz
RAM	1 GB	1.5 GB	2 GB
Virtual memory	2 GB	3 GB	4 GB
Hard disk space	9 GB	20 GB	40 GB

Server Deployment Rules of Thumb

In terms of application compatibility, there are several rules to follow:

- CD-One, RME, and VPN Monitor MUST reside on the same server.
- Router MC, IDS MC, Security Monitor, PIX MC, and AUS must be installed on top of Common Services. However, since more than one instance of Common Services can be installed, these can still be deployed across different servers.
- CD-One MUST be installed before Common Services.

Given these conditions, CiscoWorks VMS can have extremely flexible deployments. All of the components can be installed and run on a single server. On the other side of the spectrum, each of these components can be installed on its own individual server. This extreme is not practical and deployment will generally depend on a number of factors, including the following four:

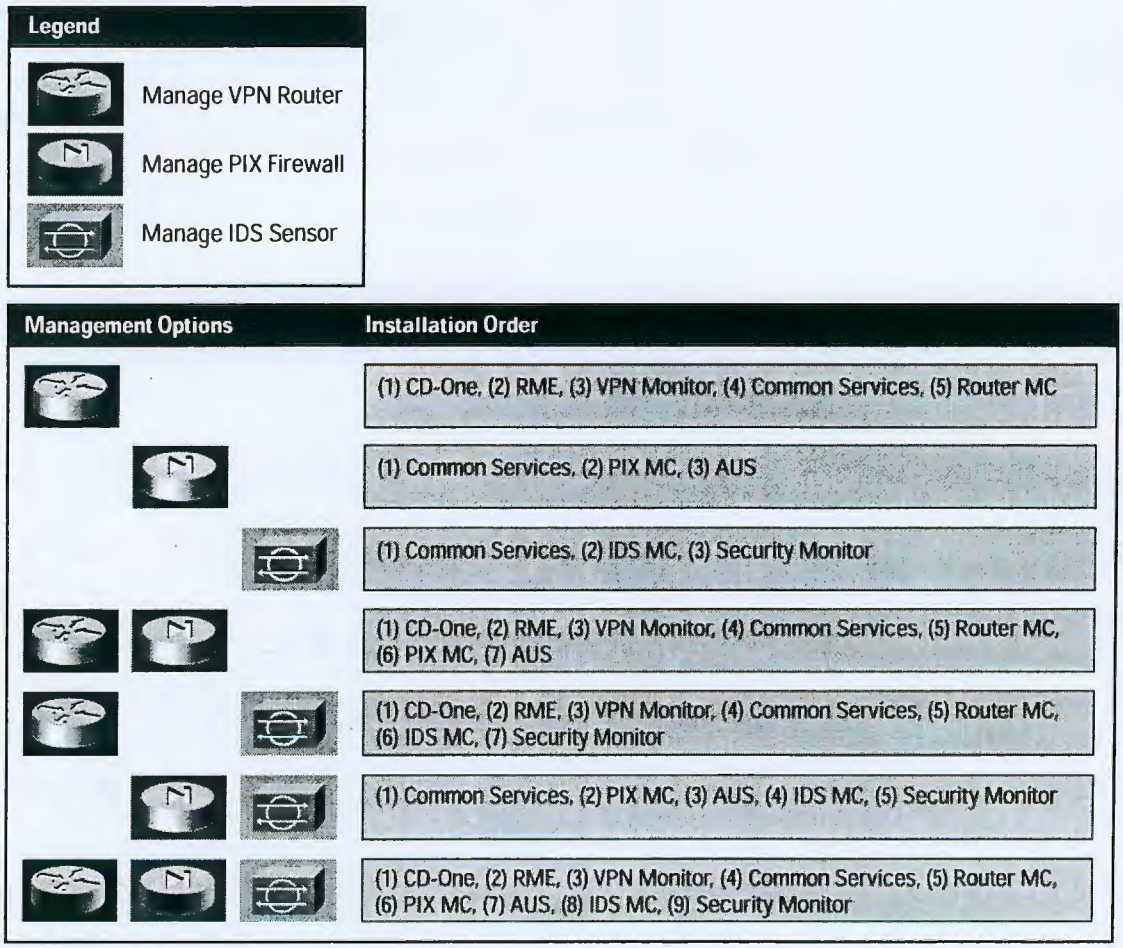
1. Which applications do you actually need?

Although VMS provides a rich, comprehensive management solution, it is possible (and perhaps even probable) that users will not need every single tool. The first question that should be asked is: Which applications do I actually need? Once this has been determined, users can choose to install only the modules that are needed. Figure 2 shows a table that provides the installation order based upon the different management options provided they are installed on a single server.

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 472
Doc: 3702

Figure 2
CiscoWorks VMS Module Installation Matrix



Note: This table provides basic guidelines. Obviously, not all the combinations and tools within VMS are covered—just those with installation order dependencies.

- Installation Option 1: For VPN management, it is the monitoring component that is covered by CD-One, RME, and VPN Monitor. If monitoring is not necessary, these modules do not need to be installed.
- Installation Option 2: For PIX management, AUS is only necessary in order to take advantage of the auto-update feature for PIX configuration and software deployment.

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

473
Doc 3702

16 154
L

2. How many devices will each application manage?

If one of the applications being used is approaching its theoretical scale limits, it is a good idea to dedicate a server to that application. For obvious reasons of resource allocation and task distribution, it is best not to have other applications using valuable CPU resources when trying to manage a large number of devices.

For example, if an instance of PIX MC is installed that is managing 800 PIX Firewalls, and the user is also trying to roll out a hub and spoke VPN deployment across 600 router spokes, it is probably a good idea to break these applications apart onto dedicated servers.

3. How many administrators will me using these applications?

In some multi-administrator environments, it makes sense to explore different deployment options for VMS. Because there are so many applications involved, and they each have a very distinct purpose, it is possible that there will be different security administrators using different applications. In this case, it is probably better to split these applications onto dedicated servers. This way, if one application is busy with a resource-intensive task such as generating configuration files, the second application will not suffer any degradation in performance.

4. What types of cost restrictions exist in terms of server procurement?

Does the organization using CiscoWorks VMS have (or have the ability to get) multiple servers? In some cases, there may only be enough budget to allocate to one server. If this is the case, then it is always better to shoot for a high-end server that exceeds the minimum system requirements. This allows room for growth, as well as improved performance.

More is Better

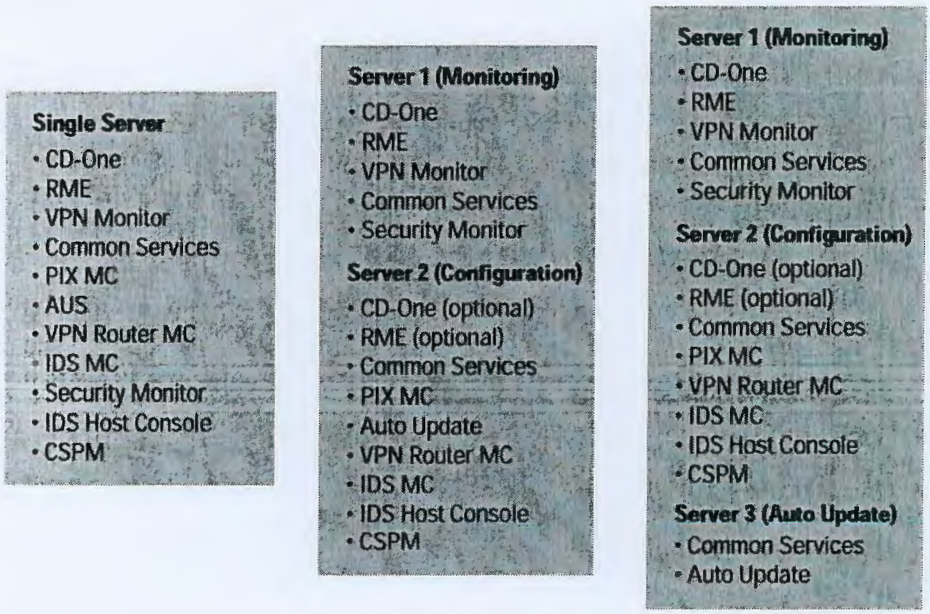
The bottom line is, if at all possible, use multiple servers and split the applications across them as they make sense. Generally, for better scalability, resource allocation, task distribution, and room for growth, more is better as long as it doesn't become cumbersome and unmanageable. Also keep in mind that if you decide to combine multiple applications onto a single server, you will need to pay special attention to the hardware requirements of each application and adjust accordingly.

The following figure and section breaks down some basic deployment options and provides some general guidelines covering most customer scenarios (Figure 3). Note that these are simply recommendations, and do not necessarily indicate that CiscoWorks VMS must be deployed in this manner.

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS N° 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 474
Doc. 3702

Figure 3
Server Deployment Options



Option 1: Single Server Deployment

For small-scale security environments with a single network security administrator, a single server deployment is recommended. This has the benefit of being low cost to the organization and guarantees ease of administration.

Option 2: 2 Servers: Configuration and Monitoring

This deployment option breaks down the VMS applications across function. One server is dedicated for monitoring and the second server is dedicated for configuration.

Server 1: Configuration

This security management server is designed to combine all of the CiscoWorks VMS applications that assist in configuration. Whether the infrastructure is VPN Router, PIX Firewall, IDS Sensor, or Host IDS Agent, this server's primary function will be configuration. The relevant applications are:

- Common Services
- PIX MC
- AUS[1]
- VPN Router MC
- IDS MC
- Cisco Host IDS Console
- Cisco Secure Policy Manager (CSPM)

1. AUS primarily provides configuration and software updates to remote PIX Firewalls. For this reason, it is frequently recommended to place the AUS within the organization's DMZ. If this is the case, we recommend using a dedicated server for AUS.

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

File No 475
Doc 3702

Server 2: Monitoring

The second server in this deployment option is dedicated for monitoring. VPN Monitor is used for IPsec MIB monitoring and Security Monitor is used for consolidated event viewing of Post Office IDS, Host IDS, PIX, and IOS Syslog messages. The applications for this server are:

- CD-One
- RME
- VPN Monitor
- Common Services
- Security Monitor

Option 3: 3 Servers: Security Application Function

The third deployment option centers around splitting up the CiscoWorks VMS application according to security technology (or infrastructure) managed. The first server deals with VPNs, and generally this covers IOS-based VPN routers. The second server contains the applications used to manage the PIX Firewall. Finally, the third server is dedicated to the management and monitoring of IDS—both network-based and host-based IDS.

Server 1: VPN

- CD-One
- RME
- VPN Monitor
- Common Services
- VPN Router MC

Server 2: Firewall

- Common Services
- PIX MC
- AUS
- CSPM

Server 3: IDS

- Common Services
- IDS MC
- Security Monitor
- Cisco Host IDS Console

Option 4: 4 Servers: Granular Management Control

For greater granularity and scalability benefits, further divide the deployment. The main difference with this option is the use of a dedicated server for AUS, since it is placed within a different subnet of the network. The other difference is the use of a dedicated server for the policy management tool CSPM. This makes sense because CSPM does not have any natural integration with the other products in the bundle and it is also resource intensive. As such, it is recommended to split it up and have a dedicated system for policy management across mixed environments.

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

INOS nº 03/2015 - CN
CPMI - CORREIOS
Fls. Nº 476
Doc 3702

Server 1: Configuration

- Common Services
- PIX MC
- VPN Router MC
- IDS MC
- Cisco Host IDS Console

Server 2: Monitoring

- CD-One
- RME
- VPN Monitor
- Common Services
- Security Monitor

Server 3: Remote Management (placed in DMZ)

- Common Services
- AUS

Server 4: Policy

- CSPM

Again, keep in mind that these are only recommendations. There are numerous combinations and deployment options available and each case should be considered on an individual basis. There will likely be many cases where customers don't even want to use all of the possible applications within VMS.

CiscoWorks VMS Applied

Now that we have determined how to deploy the components of CiscoWorks VMS from an installation perspective, we need to take a look at how these applications should be deployed from a functional standpoint. Three basic questions will be addressed in this section:

1. What is the management function of each application?
2. What devices can I manage?
3. What types of services do I need to enable?

The first question requires a detailed look into the capabilities of each product. This information is used to figure out what aspects of security management can and should be managed by each of the components within VMS. Answering the second question will clarify confusion surrounding the variances in device support by the component applications. Finally, the last question looks at how each application touches the device(s) that it manages. By examining the communication protocols being used, we can compile a list of requirements that ensures a successful deployment of VMS. For the sake of clarity, we will examine each of the questions on a product/server basis.

Note: The components of a Cisco network infrastructure are diverse and varied; however, for this discussion surrounding security, we will focus on five classes of objects: IOS routers, PIX Firewalls, VPN concentrators, IDS sensors, and IDS host agents. This does not imply that VMS is not able to manage other elements, simply that these are the pieces we must pay special attention to for security issues.

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

ROS nº 03/2005 - CPMI - CORREIOS
Fls. Nº 477
Doc 3702

A Word About Management Subnets (Out-of-Band Management)

In many networks, it is desirable to design a separate management subnet. This is commonly referred to as out-of-band management and describes a situation where the management stations reside on an isolated subnet separate from the network elements they are trying to manage. This is attractive to many network administrators due to the inherent higher level of security and clear functional division within their network.

As is the case with all network management tools, however, CiscoWorks VMS requires network access to the devices that it is trying to manage. So when making this decision, consider that, while it might be desirable to have a completely isolated management subnet, it will do no good unless there is IP connectivity to the rest of the network. This must be carefully planned out when deploying VMS in such an environment.

CD-One (CiscoView)

What is the management function?

CiscoView provides graphical Web-based device management. Users of CiscoView see a graphical representation on their computer screen and are able to monitor real-time device status, and in certain cases make configuration changes to those devices. From a CiscoWorks VMS perspective, CiscoView is positioned as a troubleshooting tool. If there is a problem within the network, and that problem has been isolated to a single device or interface, then CiscoView can be used to take a look at the statistics associated with that device and potential configure variable(s) to solve the problem.

What devices does it manage?

CiscoView provides support for the majority of the Cisco IOS routers, Cisco VPN 3000 Series Concentrators, and the Cisco PIX Firewall 501 and 506 Series.

Which services do I need to enable? (Application protocol requirements)

CiscoView relies entirely on SNMP get/set operations (UDP port 161) for its functionality. From the CiscoView server to the device, you need to enable SNMP traffic. Furthermore, the devices that you are managing must be configured to support SNMP. The Cisco IOS Software devices can support both get and set operations (for both monitoring and configuration), so both read and write community strings are configured separately to provide this level of granularity. For the VPN 3000 Concentrators and the PIX Firewalls, only SNMP read operations are supported—so while you can monitor these devices, configuration using CiscoView is not possible.

Resource Manager Essentials

What is the management function?

Describing the functions of Resource Manager Essentials (RME) would take an entire paper by itself. In general (and from a security perspective), this application provides basic network management operations and administration. Basically, this tool provides:

- Inventory management to keep track of the devices within the infrastructure
- Configuration management to manage configuration of the network devices
- Change audit control to keep track of any changes (configuration or otherwise) occurring in the network
- Software image management to facilitate the maintenance of software versions
- Syslog management to receive and analyze syslog messages sourced from the network devices

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

CPMI 03/2005 DN
CPMI CORREIOS
Fls Nº 478
Doc 3702

This list confirms that RME functionality provides benefits beyond the scope of security infrastructure management. For the purposes of this discussion, focus is on the benefits it provides to our reference environment. Of special interest is the fact that RME can generate configuration reports, software image upgrade analysis, and syslog reports specific to VPN-related infrastructure and environments.

What devices does it manage?

RME provides support for Cisco IOS routers, VPN 3000 Concentrators, and PIX Firewalls (506, 515, 520, and 525 Series). For the concentrators, RME does NOT support configuration management and only provides limited support for software image management. For the PIX Firewalls, RME provides limited support for syslog management. Refer to the diagram of our reference topology and notice this covers all aspects of our network with the exception of the IDS sensor. For this reason, RME is frequently referred to as our "core" management application.

Which services do I need to enable? (Application protocol requirements)

RME depends on several protocols to manage its devices. These include SNMP, Telnet, TFTP, and Syslog, among others. Because the subcomponents of RME are so varied, along with the different devices, we've summarized the application protocol requirements for this tool in Table 8.

Table 8 CiscoView and RME Protocol Requirements

Application	Traffic Flow	Service(s)	TCP/UDP Port Number
CiscoView		SNMP	UDP 161
Inventory Manager		SNMP	UDP 161
Configuration Manager		Telnet TFTP SNMP	TCP 23 UDP 69 UDP 161
Software Image Manager		Telnet TFTP SNMP	TCP 23 UDP 69 UDP 161
Change Audit Services		Syslog	UDP 514
Availability Manager		Telnet SNMP ICMP	TCP 23 UDP 161 N/A
Syslog Analyzer		Syslog	UDP 514

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

16 148

Based on this matrix, it is necessary to make sure the devices being managed with RME are configured to provide the proper information. SNMP read (and write where applicable) community strings need to be configured. The Telnet service, along with a login password, needs to be enabled. Finally, the devices need to be configured to point their syslog messages at the RME server.

Common Services

What is the management function?

Common Services is a server environment that provides a common set of services and management functions to a suite of client applications—the Management Centers. These services and functions include the following:

- Data storage and management
- A web infrastructure
- Session management
- User authentication/permission management
- Common environment for multiple client applications

Common Services must be installed on the server before any of the MCs, Security Monitor, or AUS can be installed. These applications integrate with Common Services and use the services and management functions provided by Common Services.

Note: To install Common Services and CD-One on the same system, CD-One MUST be installed first! Common Services can be installed on top of an existing CD-One Edition 5 installation, which allows the user to install and access applications such as RME and Router MC from a single server.

What devices does it manage?

Common Services provides the server environment, and does not directly manage any particular network devices. The management is typically handled by the applications that sit on top of Common Services.

Which services do I need to enable? (Application protocol requirements)

Common Services is responsible for the web infrastructure of the VMS MC applications, so in terms of application protocols, it is important to maintain the connection from the Web client to the Web server. Typically this will be HTTP and HTTPS traffic through pre-assigned port numbers:

- TCP 1741
- TCP 1742
- TCP 1751

For a comprehensive list of TCP and UDP port numbers used by Common Services, please consult the product documentation "Installing CiscoWorks Common Services on Windows 2000."

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

ECT Nº 03/2006 - CN
CPMI - CORREIOS
Fls. Nº 480
Doc 3702

16 147

Management Center for VPN Routers

What is the management function?

Management Center for VPN Routers (Router MC) provides an easy management interface to set up and maintain VPN connections between multiple supported Cisco IOS Software devices in a hub-and-spoke topology. Router MC allows network managers to quickly and easily provision all critical connectivity, security, and performance parameters for a site-to-site, large-scale VPN. Utilizing a point-and-click web-based interface and preconfigured components for VPN creation, Router MC also allows the quick configuration of smaller, simpler VPNs. In addition to configuring hub and spoke VPNs, Router MC also lets users replace leased line connections with VPN connections, or prepare VPN configurations for routers not yet on the network

What devices does it manage?

Router MC is used to manage VPNs across Cisco IOS Routers. In general, the application is hardware-platform agnostic. It only cares about the version of Cisco IOS Software and the supported feature set. The basic rule is that the routers have to support IPsec, SSH, and named access lists. Table 9 lists the Cisco IOS Software versions that have been tested with Router MC.

Table 9 Supported Cisco IOS Software Versions in Router MC

Cisco IOS Software Platform	Minimum Cisco IOS Software Version
7100, 7200 (Hub)	12.1(9)E
3640/60 (Hub)	12.2(2)T, 12.2(3)
7100, 7200 (Spoke)	12.2(2)T, 12.2(3)
2610/20/50 and 3620/40/60	12.2(2)T, 12.2(3)
1720/50	12.2(2)T, 12.2(3)
806	12.2(1)XE
803	12.2(2)XH

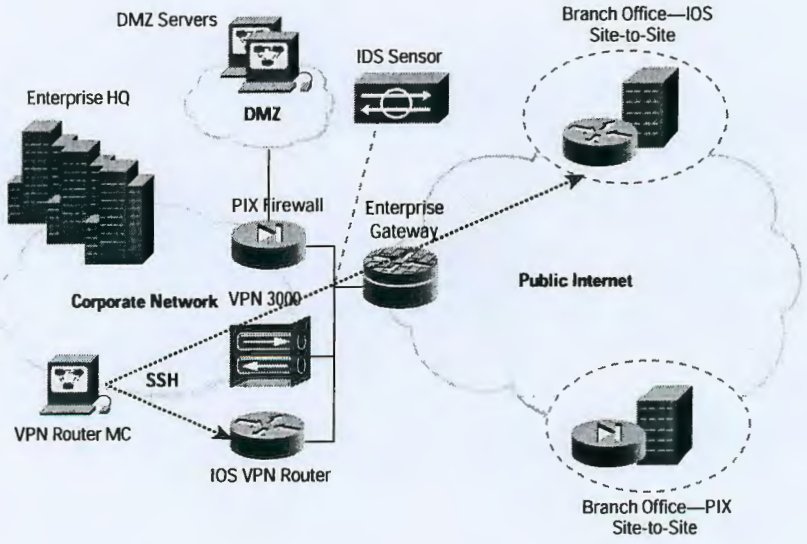
Which services need to be enabled? (Application protocol requirements)

Router MC uses SSH (TCP port 22) to configure the IOS routers. The SSH session is established when devices are initially imported into Router MC. Then when configurations are pushed out to the devices, this session is also encrypted via SSH. Figure 4 shows how Router MC is applied to our reference topology.

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Fls. Nº 481
Doc 3702

Figure 4
Router MC Applied



Management Center for PIX Firewalls

What is the management function?

Management Center for PIX Firewalls (PIX MC) enables Cisco PIX Firewall infrastructure management by configuring new firewalls and importing configurations from existing firewalls. Firewall device settings, access rules, and translations rules can be configured, and these configuration changes can then be deployed to the firewalls on the network. PIX MC also provides a powerful tool for controlling changes made to the network, showing configuration and status changes.

What devices does it manage?

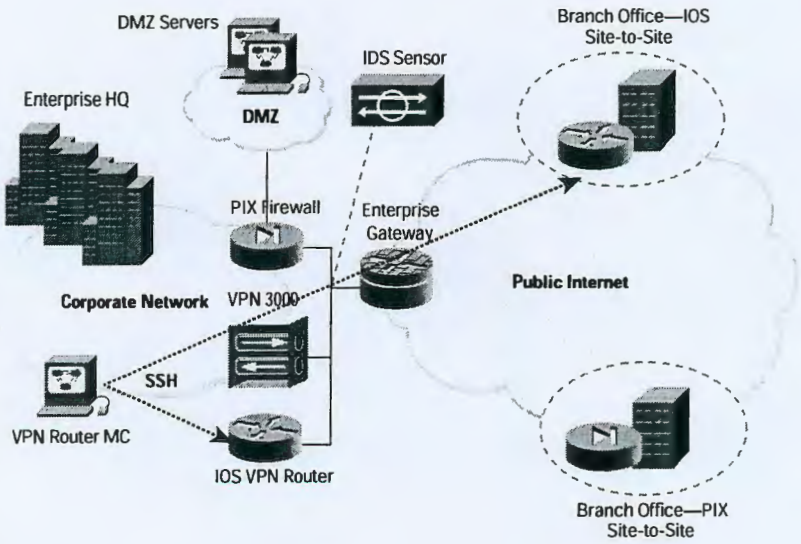
PIX MC is used to manage the PIX Firewall deployed throughout the network. These include all the PIX platforms: 501, 506E, 515E, 525, and 535 Series. The PIX MC supports the command sets for PIX OS version 6.1, and supports the Auto Update and the Easy VPN command sets found in version 6.2.

Which services must be enabled? (Application protocol requirements)

PIX MC uses an encrypted session to manage its PIX Firewall devices. The protocol that it uses is SSL (or HTTPS) and the port number assigned for this connection is TCP port 443. Therefore, it is necessary to permit TCP 443 to a PIX Firewall (from the management interface) in order for PIX MC to properly manage the device. Figure 5 shows how PIX MC is applied to our reference topology.

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Figure 5
PIX MC Applied



Auto Update Server

What is the management function?

AUS is responsible for storing configurations and software images for PIX Firewalls. Firewalls operating in auto-update mode periodically contact AUS to upgrade software images, configurations, and versions of PDM, and to pass device information and status to AUS. Using AUS also facilitates managing devices that obtain their addresses through Dynamic Host Configuration Protocol (DHCP) or that sit behind Network Address Translation (NAT) boundaries. Typically, because of this management function, the AUS is deployed in a publicly accessible DMZ which the remote side PIX Firewalls can contact directly.

What devices does it manage?

PIX MC is used to manage the PIX Firewalls deployed throughout your network. These include all the PIX platforms: 501, 506E, 515E, 525, and 535 Series. AUS requires that PIX Firewalls run OS version 6.2 since it requires the Auto Update feature.

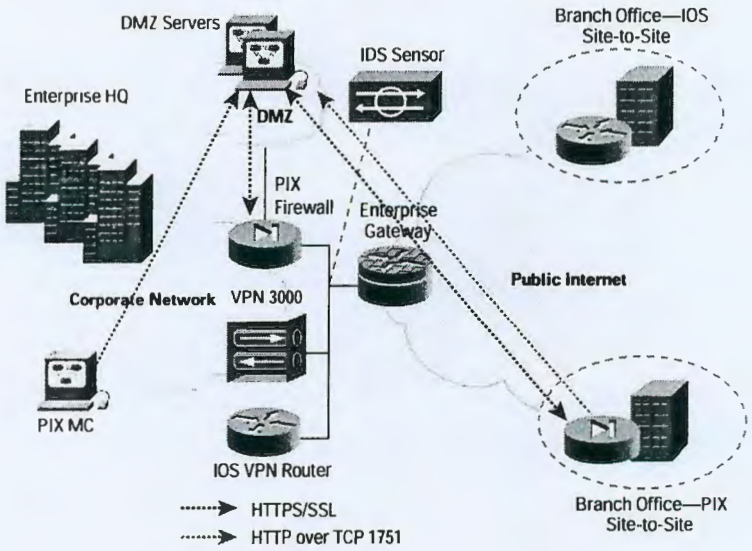
Which services need to be enabled? (Application protocol requirements)

AUS talks to two different pieces in our topology diagram. The first piece it talks to is the PIX MC server. If these two applications are installed on the same system, no changes are necessary to the communication architecture. However, if they are installed on different servers, the PIX MC server will push configuration files to AUS using SSL, making it necessary to open up TCP 443 to the AUS system.

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

The second piece is the actual communication between the AUS and the PIX Firewall itself. In this scenario, there is two-way communication and both occur via SSL. Therefore, it is not only necessary to open up TCP 443 to the AUS from the PIX, but also vice versa. For transfer of binary images (PIX and PDM software), this will be transferred via standard HTTP over TCP 1751 (this can optionally be changed to SSL). Figure 6 illustrates how AUS is applied to our reference topology.

Figure 6
AUS Applied



Management Center for IDS

What is the management function?

Management Center for IDS (IDS MC) manages configurations for Cisco Intrusion Detection System Sensors. All aspects of sensor configuration can be managed through a series of Web-based screens, including individual sensors or a group of sensors having a common configuration. The sensor configuration data resides in a database. IDS MC can also perform signature updates by downloading the update archives from the Cisco web location and then distributing these signature updates to the appropriate sensor groups.

A separate but closely related product, Monitoring Center for Security (Security Monitor), provides event collection, viewing, and reporting capability for network devices. This is covered in the next section.

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

484
Doc 3702

What devices does it manage?

IDS MC manages the Cisco IDS appliance sensors as well as the Cisco IDS Module for the Catalyst 6500. The IDS software required for the application depends on the platform (See Table 10).

Table 10 Required IDS Sensor Software for IDS MC

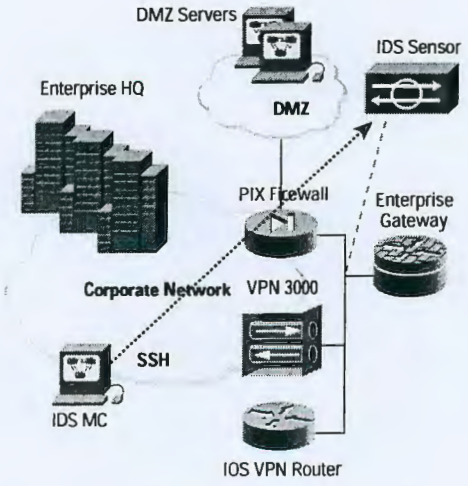
IDS Sensor Platform	Minimum Required Software
Cisco IDS Appliance Sensor	3.0.1[1]
Catalyst 6000 IDS Module	3.0.5[1]

1. IDS 4.0 software will be supported in a future release of IDS MC and Security Monitor.

Which services need to be enabled? (Application protocol requirements)

IDS MC uses two protocols to manage the IDS sensors: First, it uses Secure Shell (SSH) to secure remote login to the sensors. Second, it uses SCP to secure the transfer of the actual sensor configuration files. Session-Control Protocol (SCP) uses SSH for data transfer, so TCP 22 needs to be allowed to the sensors. Figure 7 illustrates how IDS MC is applied to our reference topology.

Figure 7
IDS MC Applied



Security Monitor

What is the management function?

Monitoring Center for Security (Security Monitor) provides a Web-based interface for event collection, viewing, and monitoring for the following devices:

- Cisco Intrusion Detection System Sensor running Post Office software
- Cisco IOS router running IDS software
- Host IDS Sensor via the Console
- PIX Firewall

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

The Security Monitor displays events on a customizable event viewer, and allows the user to write some basic event correlation rules to consolidate events. These rules can also be set up to kick off real time notifications.

What devices does it manage?

Security Monitor can receive security events from five sources with the following software requirements:

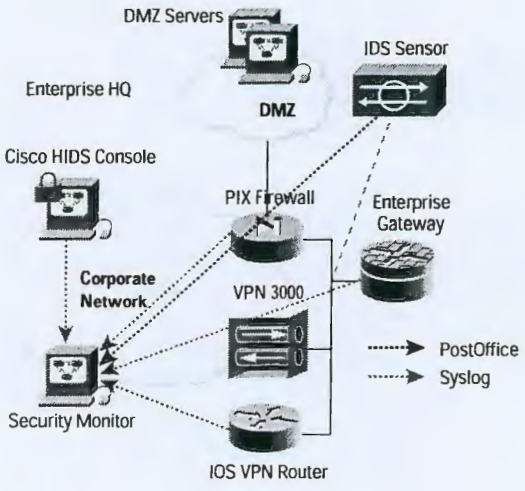
Table 11 Required Software for Security Monitor Devices

Security Event Source	Minimum Software Required
Cisco IDS Appliance Sensor	3.0.1
Catalyst 6000 IDS Module	3.0.5
IOS router	IOS with IDS features set
PIX Firewall	Any version that supports syslog
Host IDS Console	2.5 or later with integrator software

Which services do I need to enable? (Application protocol requirements)

Because of the number of data inputs, consider each of these individually in terms of application protocol requirements. For the Post Office devices (sensor appliance and IDS module), Security Monitor uses Post Office protocol to forward events. For the other data sources (Cisco IOS Software, PIX and Host IDS), the events are sent to Security Monitor via syslog. So make sure to allow Post Office (UDP 45000) and syslog (UDP 514) to the Security Monitor server. Figure 8 illustrates how Security Monitor is applied to our reference topology.

Figure 8
Security Monitor Applied



Cisco Systems, Inc.
All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

16 14

VPN Monitor

What is the management function?

VPN Monitor provides monitoring statistics for the enterprise head-end VPN devices—this means the "hubs" of a hub-and-spoke VPN topology. In our reference topology, this refers to both the Cisco 7X00 Series Router and the VPN 3000 Concentrator, so proper connectivity from the VPN Monitor server to those devices is necessary. This application provides statistical VPN information in both graphical and tabular format. It can also be used as a graphical notification tool when certain VPN-related thresholds (that are user configurable) are violated. With VPN Monitor, network administrators can get an overall view of how their VPNs are doing by looking at metrics that include encrypted traffic statistics, secure handshake negotiations, packet replays, and so on.

What devices does it manage?

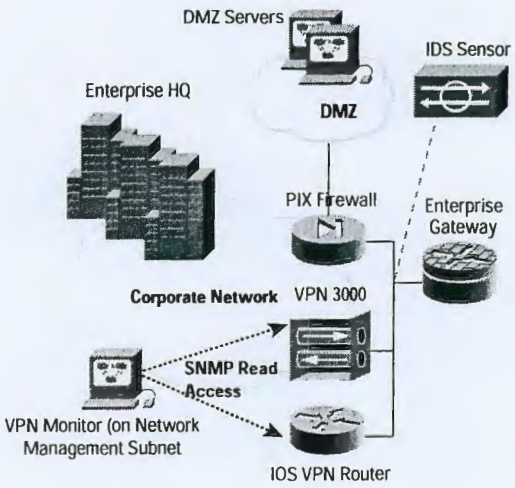
VPN Monitor supports Cisco IOS VPN routers with the necessary IPSec MIB support as well as VPN 3000 Concentrators. Currently, the application supports the Cisco1700, 2600, 3600, 7100, and 7200 Series routers. The software image version requirements are:

- 1700, 2600, or 3600 IOS Router—12.2(4)T or later
- 7100 or 7200 IOS Router—12.1(5a)E or later
- VPN Concentrator 3000 Series—2.5.2f or later

Which services do I need to enable? (Application protocol requirements)

Much like CiscoView, VPN Monitor requires SNMP (UDP port 161) to function. The VPN Monitor server periodically polls the devices to retrieve the IPSec MIB information. Since this is purely a monitoring tool, it is only necessary to consider SNMP get operations on these two classes of devices. This corresponds to configuring the SNMP read community string on the network devices that need to be managed with VPN Monitor. Figure 9 illustrates how VPN Monitor is applied to our reference topology.

Figure 9
VPN Monitor Applied



All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Fls. Nº 487
Doc 3702

Note: Given these requirements, it IS possible to use VPN Monitor on a remote VPN device. However, this is n entirely practical for two reasons: First, this type of monitoring does not scale as well. Second, in most cases it is sufficient to view the VPN metrics from one end of the tunnel (and not both).

Cisco IDS Host Sensor

What is the management function?

The Cisco IDS Host Sensor (Cisco HIDS) application is a product that complements the network-based IDS management provided in IDS MC and Security Monitor, and gives CiscoWorks VMS a truly comprehensive solutio to manage intrusion detection. The basic premise of Cisco HIDS is to protect individual host systems from intrusio detection. The software (agent) sits on the host itself and examines system calls to the OS kernel, comparing these t a database of well-known signatures. Events are reported back to a central Cisco HIDS Console system, which consolidates the information from the agents it is managing. If a signature match is found, Cisco HIDS will preven the operation and shoot off a real-time notification.

This protection model is proven to mitigate well-known threats such as the NIMDA and Code-Red worms withou any user configuration. This means the Cisco HIDS agent software is especially important to use on important network hosts, at the user's discretion. In our reference topology, the Cisco HIDS agent code is installed on all the network management servers that comprise the VMS solution, thus protecting the important network management systems. These servers report IDS events back to the HIDS Console system, which are then forwarded to Security Monitor, provided the integrator software is installed on the HIDS Console. Users are asked to provide the IP address and syslog listening port of Security Monitor during the installation of the integrator.

What devices does it manage?

The Cisco HIDS application does not directly interact with Cisco network devices. It interacts with network hosts with the Cisco HIDS Agent code installed. At present, the following server OS versions are protected:

- Windows NT 4.x Server
- Windows NT Enterprise Server (SP 3 or later)
- Windows 2000 Server
- Windows 2000 Advanced Server
- Solaris 2.6, 2.7, and 2.8

The following Web servers are protected:

- Windows IIS Web Server
- Solaris Apache
- Solaris Netscape Enterprise
- Solaris iPlanet

Consult product documentation to verify the current available option of the Cisco HIDS Agent software.

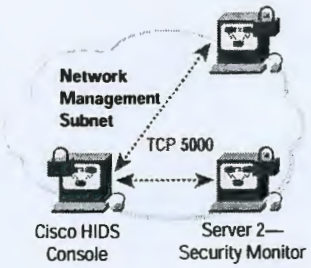
All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

POS nº 03/2003 - CPMI - CORREIOS
488
3702
Doc

Which services do I need to enable? (Application protocol requirements)

For Cisco HIDS to work properly, the agents must be able to communicate with the console. This is necessary so that the agents can report IDS events to the console, and just as importantly, the console can push configuration changes out to the agents. This communication is accomplished through a proprietary protocol that travels on TCP port 5000. This port number is actually a configurable option upon install, but TCP port is the default value. Figure 10 illustrates how the Cisco HIDS application is applied to our reference topology.

Figure 10
Cisco HIDS Console and Agents Applied



Cisco Secure Policy Manager

What is the management function?

Cisco Secure Policy Manager (CSPM) is an end-to-end security policy tool. Network administrators use CSPM to define and deploy security policies for their networks. This can be something as simple as what hosts or networks are allowed to access their network, or it can be something much more complex involving encryption, access methods, and other variables. The point is that, using CSPM, network administrators can implement policy management across their mixed network infrastructures.

From the perspective of our reference topology, the role of CSPM is twofold: 1. It manages traffic encryption policy by handling the VPN configuration that allows the user to configure the hub and spoke VPN tunnels between the 7X00 Series Router on the corporate network to the endpoints on the branch sites (both IOS and PIX devices). 2. It allows the user to configure security policies on the PIX Firewall(s) and also the firewall feature set on the IOS enterprise gateway, defining basic firewall policy distribution.

What devices does it manage?

As can be inferred from the previous paragraph, CSPM is able to manage the Cisco IOS routers and PIX Firewalls. The software image version requirements are:

- Cisco IOS Router—12.0(5) or later with the FW-DES feature set
- PIX Firewall—4.2.4 or later with the Data Encryption Standard (DES) feature set

Other versions can be added and managed as well, using the version management utility in CSPM.

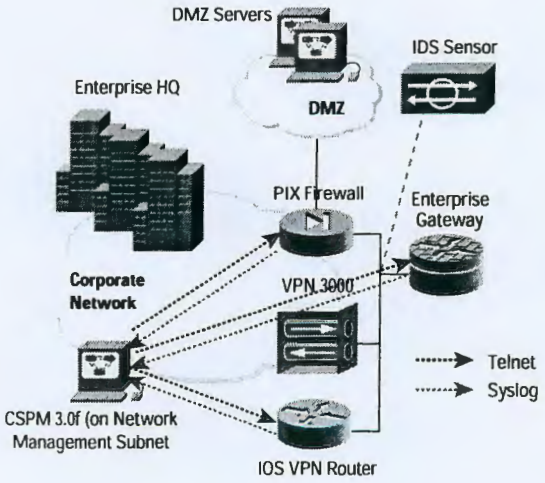
All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

ROS nº 050207 - CP
CPMI - CORREIOS
Fls. Nº 489
Nº 3702 Doc

Which services do I need to enable? (Application protocol requirements)

CSPM requires several protocols in order to function. First, when applying a security policy across the network, CSPM will use Telnet (TCP port 23) to connect to the device(s) and make configuration changes. The second protocol is syslog (UDP port 514). The CSPM has the ability to receive and consolidate syslog messages from the Cisco devices that it is managing. The application keeps an archive of these syslog messages and can use them to generate reports based upon the information they provide. Based on these requirements, the devices must then be configured to support these services. For both Cisco IOS Software and PIX, the telnet service along with a login password must be enabled. These devices also need to be configured to point their syslog messages to the CSPM server. Note that those devices managed by both RME and CSPM will now be sending their syslog messages to two different hosts. Figure 11 illustrates how CSPM is applied in our reference topology.

Figure 11
CSPM Applied



All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Putting It All Together

Clearly, it is important to distinguish which components to use, determine where to deploy the various components of VMS, and identify what elements of the network infrastructure each piece manages. Table 12 summarizes the information presented in this section along with the associated management protocols that must be enabled in order for the applications to function properly.

Table 12 Summary of CiscoWorks VMS Components Applied

Application	Traffic Flow	Service(s)	TCP/UDP Port Number
CiscoView		SNMP	UDP 161
Inventory Manager		SNMP	UDP 161
Configuration Manager		Telnet TFTP SNMP	TCP 23 UDP 69 UDP 161
Software Image Manager		Telnet TFTP SNMP	TCP 23 UDP 69 UDP 161
Change Audit Services		Syslog	UDP 514
Availability Manager		Telnet SNMP ICMP	TCP 23 UDP 161 N/A
Syslog Analyzer		Syslog	UDP 514

Caveats

When deploying VMS, it is important to realize the specific services required by each individual application, as outlined in the previous section. In certain instances, two different applications may require the same type of access to a particular device (for example, CiscoView and VPN Monitor both use SNMP to retrieve the management information). However, because some of the applications within VMS have a security focus, sharing access to a device can be a potentially contentious situation. This section discusses some of the things that need to be considered should you deviate from the deployment guidelines provided in this document.

Considerations with Network Address Translation

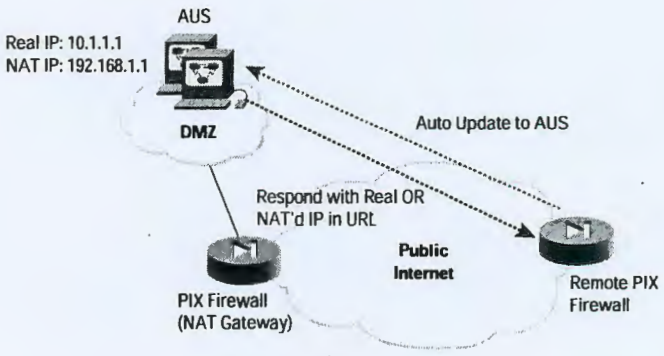
In many topologies, Network Address Translation (NAT) is used. This is an excellent feature for security and address space conservation, but it can create some problems with management tools. This section points out some of the caveats and issues that may occur if CiscoWorks VMS is deployed into a network environment with NAT.

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

NAT and AUS

If the AUS application is used and the server is sitting behind a NAT gateway, pay special attention to the PIX Firewalls you are managing. Consider a remote PIX that contacts the AUS server. It will actually contact the NAT address (not the real address). When the AUS responds with the proper URL to download the updated configuration or software image, it will use the NAT address. Conversely, if the AUS is NOT behind a NAT gateway, you could also configure it to provide it's real address (Figure 12). The bottom line is that you have to decide to use the NAT address or the real address for ALL the PIX Firewalls you are managing—NAT and non-NAT addresses cannot be mixed within a single installation of AUS.

Figure 12
NAT and AUS



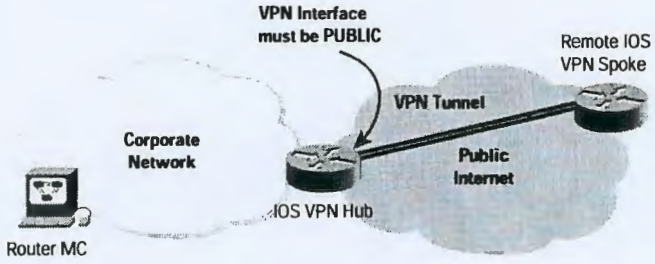
When it is necessary to manage PIX Firewalls (both internal and external), we recommend installing two copies of AUS—one for the external firewalls that will use the NAT address and one for the internal firewalls that will use the real IP address.

NAT and Router MC (Hub Side)

When using Router MC to set up a hub-and-spoke VPN environment, be careful about the hub router VPN interface. Because of the way the product is designed, this interface cannot be behind a NAT gateway. The VPN termination interface must be a publicly addressable IP subnet. If it was behind a NAT gateway, then from the perspective of the peer it would be necessary to assign it the NAT'd address. The Router MC application, however, only allows you to assign by interface and not IP address—so the peer statements will be incorrect. Refer to Figure 13 to see how the VPN topology must be built for compatibility with Router MC.

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Figure 13
NAT and Router MC



NAT and Router MC (Spoke Side)

There is also a deployment caveat with NAT and VPN spoke devices. Router MC needs to manage the spoke devices (VPN peers) with their real IP address. The current version of Router MC does not support the situation where the spoke is behind a NAT gateway.

Managing a Device with CSPM and a MC

With the number of different applications within the VMS bundle, it is possible to have some functional overlap between tools. For example, if you want to change a PIX Firewall access rule, you can use either CSPM or PIX MC. This section describes some caveats and issues that exist when using overlapping applications.

CSPM and PIX MC

The first area of functional overlap is between CSPM and PIX MC. Both applications can be used to manage firewall device settings and access rules. So what happens when somebody tries to use both tools? Will this configuration even work?

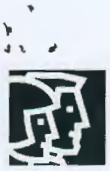
The short answer is that this will NOT work. What will happen is when a configuration change is made using one of the applications, it will overwrite that change with the other application. This can be avoided by doing a re-import of the existing configuration before every deployment, but this is not practical. Also, you would need to make sure that you had an access rule set up to allow SSL traffic to the PIX. The recommendation here is to either use CSPM or PIX MC to manage a device, but not both.

CSPM and Router MC

The second area of functional overlap involves CSPM and Router MC. Both applications can be used to configure site-to-site VPNs on IOS VPN routers. CSPM can also be used to configure the firewall features set on those routers. Here, the consideration when each application would be used and how the two can work together.

As with PIX MC, avoid managing a single router's VPN settings with multiple applications. Even though Router MC does not push out a whole configuration file to the device (it sends out individual commands), it is possible that something will get overwritten in the original configuration. Looking at the reverse, it is definitely a problem if CSPM tries to configure a router that has already been configured with Router MC. The device will need to be re-imported into the CSPM database every time, just to make sure your configuration is current. This is also not a very practical solution. Either use CSPM or Router MC to manage a device, but not both.

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.



When To Use What

Based on some of the overlap in product functionality, it can be confusing to decide which product should be used in what situations. CSPM is currently the only product that can help manage a mixed environment, so you need to use CSPM to set up a VPN tunnel between a PIX device and an IOS device. Otherwise, since they are designed for better scalability, it is ALWAYS recommended to use the MC applications instead, based on the network environment and management needs.

Multiple Syslog Daemons

Several applications within the VMS bundle can receive syslog messages from multiple sources. Now, with Cisco modified OS support, all of these applications can also be installed on a single server. In this case, it is necessary to determine how to make all of these syslog daemons compatible.

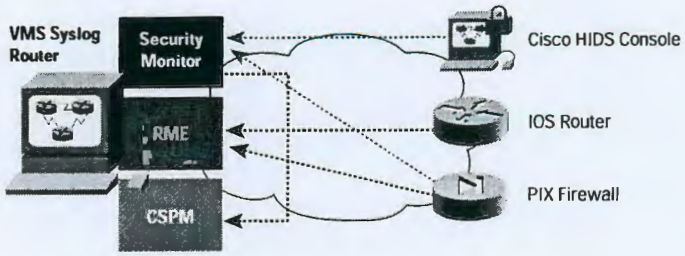
First, look at which applications can receive syslog messages, and from which devices (Table 13):

Table 13 Summary of Syslog Server Applications in VMS

CiscoWorks VMS Module	Syslog Source
RME	IOS, PIX, VPN3K
CSPM	IOS, PIX
Security Monitor	IOS, PIX, Host IDS Console

By default, all of these application listen on UDP port 514. This is not a problem if these applications are split across different servers—simply send syslog messages to multiple sources. However, what happens when all of these applications are installed on a single system AND the customer wants to try and take advantage of all three syslog daemons? (Figure 14.)

Figure 14
Syslog Consolidation in VMS



There are two ways that Security Monitor can alleviate this problem. The first is to configure what port number it should listen for syslog messages. By default it is UDP 514, but it can be changed. Also, Security Monitor can be set up to forward the syslog messages to another port on that same system. This is important because CSPM can change the port numbers they listen to for syslog messages. The other important factor is that PIX Firewalls can send syslog messages to the same host, but different port numbers. In this situation, here is the solution to maximize the syslog functionality:

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

- From IOS, send syslog to RME at UDP 514
- From PIX, send syslog to RME at UDP 514
- From PIX, send syslog to Security Monitor at port x
- From Cisco HIDS Console, send syslog to Security Monitor at port x
- From Security Monitor, forward syslog to CSPM at port y

The only caveat here is that CSPM will not be able to receive IOS syslog messages.

Ideally, at least two servers would be used in this scenario to take advantage of all three tools. The first box would run Security Monitor and CSPM, and the second system would run RME. This way, no syslog functionality within VMS is lost.

Running the Cisco HIDS Software with other Applications

A major component of the CiscoWorks VMS bundle is the ability to manage IDS on a host level—or rather, to provide intrusion protection to critical servers. The management servers for VMS should definitely be considered critical and as such, we also recommend installing the Cisco HIDS agent software on these systems.

When installing another CiscoWorks VMS module on a server with Cisco HIDS, make sure the agent is in "Full Warning" mode during the install process. Running in "Full Protect" mode, it is possible that the normal operations of the software may trigger a HIDS event and, as such, may actually be prevented. In this case, a false positive would have an adverse effect on your management system by not allowing it to perform a legitimate task. In most cases, you should first install the Cisco HIDS agent and run it in "Full Warning" mode. Do this for the first several weeks of regular use to develop a baseline. This allows the user to first see events—but they will NOT be prevented. Based on this activity you can then identify any false positives and create appropriate exceptions. When the exceptions are configured, then you can change the status of your management server agents to "Full Protect" to ensure that the server is properly shielded.

Even using this deployment method, note that even in "Full Protect" mode out of the box, the HIDS agent software does not prevent any normal operations by any of the applications in the VMS bundle.

Compatibility Issues with IDS Event Viewer

Cisco IDS Event Viewer (IEV) is a Java-based application that lets users view and manage alarms from up to three IDS sensors. At the time of this writing, when IEV is installed on a PC, that PC can NOT be used as a client for the CiscoWorks VMS Web-based modules. While this compatibility limitation will be addressed in future releases, the current workarounds for this limitation are:

- Uninstall IEV from that client system
- Use a different PC as your client system

This will not be an issue for most users. Those using IDS MC and Security Monitor will most likely not need IEV as well.

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Fls Nº 495
Doc 3702

Out-of-Band Management

In many networks, it is desirable to design a separate management subnet. This is commonly referred to as out-of-band management and describes a situation where the management stations reside on an isolated subnet separate from the network elements they are trying to manage. This is attractive to many network administrators due to the inherent higher level of security and clear functional division within their network.

As is the case with all network management tools, however, CiscoWorks VMS requires network access to the devices it is trying to manage. So when making this decision, consider that, while it might be nice to have a completely isolated management subnet, it will do no good unless there is IP connectivity to the rest of the network. This must be carefully planned out when deploying VMS in such an environment.

Conclusions

Evolution of VPNs and Security

In the recent past, we have seen huge growth in the need for network security, specifically in two areas: perimeter network security and secured transactions over public infrastructure. This growth has made it necessary to evolve how a management scheme handles this environment, which has resulted in the introduction of the CiscoWorks VPN/Security Management Solution (VMS).

The CiscoWorks VMS provides customers with applications to assist in the management of their security-specific hardware such as the Cisco VPN 3000 Concentrator series, Cisco IOS VPN routers, Cisco PIX Firewalls, and Cisco IDS products. VMS addresses the challenges of VPN deployment, monitoring, development of perimeter security policies, and management of intrusion detection. This paper provides some basic deployment guidelines for VMS by outlining the different components of the solution, what they do, and how they can be configured to work together. After reading this document, the user should clearly understand how VMS fits into the network management scheme and the values it adds.

As with any dynamic environment, the needs and technologies around network security are constantly evolving. From a network management perspective, CiscoWorks VMS will continue to evolve to provide a comprehensive set of tools to manage the unique aspects of this environment.

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 317 7777
Fax: +65 317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the **Cisco Web site at www.cisco.com/go/offices**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

All contents are Copyright © 1992–2002, Cisco Systems, Inc. All rights reserved. Cisco, Cisco IOS, Cisco Systems, the Cisco Systems logo, and Cisco Unity are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0208R)

202881/ETMG 10/02

16132
Fls. Nº 496
Nº 3702
Doc

16.173
L

Segurança Tipo 2 doc 10

RQS nº 03/2006 - CN
CPMI - CORREIOS
Fls. Nº 497
Nº 3702
Doc

16.173

Cisco – Using and Configuring PIX Object Groups

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 498
3702
Doc

Table of Contents

Using and Configuring PIX Object Groups 1
Introduction 1
Before You Begin 1
Conventions 1
Prerequisites 1
Components Used 1
Network Diagram 2
Using Object Groups 2
Configuring Object Groups 2
ICMP–Type Configuration 2
Network Configuration 3
Protocol Configuration 3
Service Configuration 4
Object–Group Nesting Configuration 4
Verify 4
Related Information 5

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 499
Nº 3702
Doc

Using and Configuring PIX Object Groups

Introduction
Before You Begin
Conventions
Prerequisites
Components Used
Network Diagram
Using Object Groups
Configuring Object Groups
ICMP–Type Configuration
Network Configuration
Protocol Configuration
Service Configuration
Object–Group Nesting Configuration
Verify
Related Information

Introduction

This document discusses object groups, a feature introduced in PIX code version 6.2. Object grouping allows objects such as IP hosts or networks, protocols, ports, and Internet Control Message Protocol (ICMP) types to be collected into object groups. Once configured, an object group can then be used with the standard **conduit** or **access–list** PIX commands to reference all objects within that group. This will reduce the configuration size.

Before You Begin

Conventions

For more information on document conventions, see the Cisco Technical Tips Conventions.

Prerequisites

There are no specific prerequisites for this document.

Components Used

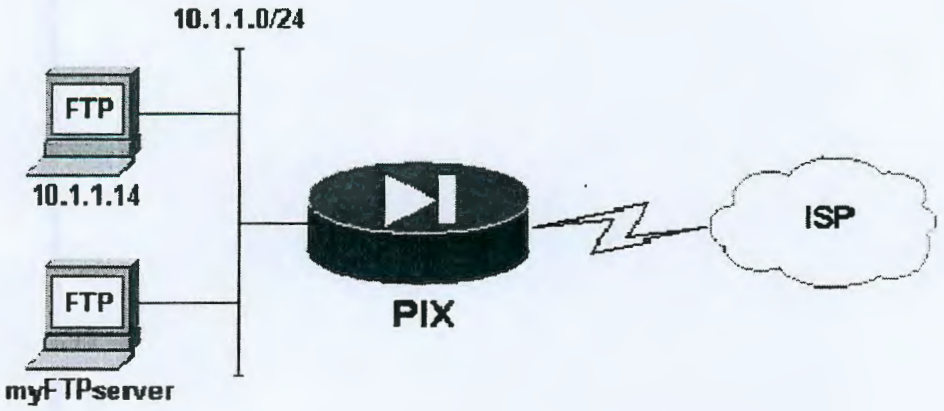
The information in this document is based on the software and hardware versions below.

- Cisco PIX Software Release 6.2(2)
- Cisco 515 PIX Firewall (any PIX model will work with these configurations)

The information presented in this document was created from devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If you are working in a live network, ensure that you understand the potential impact of any command before using it.

RQS nº 03/2005 - CPMI - CORREIOS
Fls. Nº 500
Nº 3702 Doc

Network Diagram



Using Object Groups

When using an object group within a command, the keyword **object–group** must be used before the group name, as shown in the following example.

```
access-list 100 permit object-group protocols object-group
   remotes object-group locals object-group services
```

In this example, protocols, remotes, locals, and services are previously defined object group names. Object groups can also be nested, where one object group can be included as a subset of another object group.

The command set is shown below.

```
object-group grp_id
object-group description description_text
group-object object_grp_name

object-group icmp-type grp_id
icmp-object icmp_type

object-group network grp_id
network-object host host_addr
network-object net_addr netmask

object-group protocol grp_id
protocol-object protocol

object-group service grp_id {tcp|udp|tcp-udp}
port-object eq service
port-object range begin_service end_service
```

Configuring Object Groups

ICMP–Type Configuration

The ICMP–type object group is used to specify specific ICMP types for use only with ICMP access control lists (ACLs) and conduits. A full listing of ICMP types can be found in the PIX command reference for the

RCS nº 03/2005 - CPMI - CORREIOS
Fls. Nº 501
Nº 3702 Doc

object-group command.

```
(config)# object-group icmp-type icmp-allowed
(config-icmp-type)# icmp-object echo
(config-icmp-type)# icmp-object time-exceeded
(config-icmp-type)# exit

(config)# access-list 100 permit icmp any any object-group icmp-allowed
```

Network Configuration

The network object group is used to specify host IP addresses or subnet ranges to be defined in an ACL or conduit. Host IP addresses are prefixed with the keyword **host**, and can be either an IP address or a hostname already defined with the **name** command. This object group can be used as either the source or destination in the associated ACL/conduit.

```
(config)# names
(config)# name 10.1.1.10 myFTPserver

(config)# object-group network ftp_servers

(config-network)# network-object host 10.1.1.14
(config-network)# network-object host myFTPserver

(config-network)# network-object 10.1.1.32 255.255.255.224
(config-network)# exit

(config)# access-list 101 permit ip any object-group ftp_servers
```

If this list consists only of FTP servers, the following specific example applies.

```
(config)# access-list 101 permit tcp any object-group ftp_servers eq ftp
```

Protocol Configuration

The protocol object group is used to specify a protocol(s) to be defined in an ACL or conduit. This object group can be used as the protocol type only in the associated ACL or conduit. Note that the allowed protocols for this object group are only the standard PIX protocol names allowed in an **access-list** or **conduit** command, such as Transmission Control Protocol (TCP), User Datagram Protocol (UDP), Generic Routing Encapsulation (GRE), Enhanced Interior Gateway Routing Protocol (EIGRP), Encapsulating Security Payload (ESP), Authentication Header (AH), and so on. Protocols that sit on top of TCP or UDP cannot be specified with a protocol object group. Instead, these protocols will use an object group, as shown in the following example.

```
(config)# object-group protocol proto_grp_1

(config-protocol)# protocol-object udp
(config-protocol)# protocol-object tcp
(config-protocol)# protocol-object esp
(config-protocol)# exit

(config)# access-list 102 permit object-group proto_grp_1 any any
```


ROS nº 03/2005 - Cx
CPMI - CORREIOS
Fls. Nº 502
Nº Doc. 3702

Service Configuration

The service object group is used to specify specific or ranges of TCP and/or UDP ports to be defined in an ACL or conduit. This object group can be used as either the source port(s) or destination port(s) in the associated ACL/conduit, as shown in the following example.

```
(config)# object-group service allowed_prots tcp
(config-service)# port-object eq ftp
(config-service)# port-object range 2020 2021
(config-service)# exit

(config)# object-group service high_ports tcp-udp
(config-service)# port-object range 1024 65535
(config-service)# exit

(config)# access-list 103 permit tcp any object-group
          high_ports any object-group allowed_prots
```

Object–Group Nesting Configuration

Only object groups of the same type can be nested within another. For example, you cannot nest a protocol–type object group within a network–type object–group.

To nest a group within a group, issue the **group–object** subcommand. In the following example, you could use the all_hosts group in an ACL or conduit to specify all four hosts. Or, you could use either host_grp_1 or host_grp_2 to specify only the two hosts within each group.

```
(config)# object-group network host_grp_1

(config-network)# network-object host 10.1.1.10
(config-network)# network-object host 10.1.1.14
(config-network)# exit

(config)# object-group network host_grp_2

(config-network)# network-object host 172.16.10.1
(config-network)# network-object host 172.16.10.2
(config-network)# exit


(config)# object-group network all_hosts

(config-network)# group-object host_grp_1

(config-network)# group-object host_grp_2

(config-network)# exit
```

Verify

This section provides information you can use to confirm your configuration is working properly.

Certain **show** commands are supported by the Output Interpreter Tool (registered customers only) , which allows you to view an analysis of **show** command output.

- **show object–group** – Shows the currently defined ACLs.

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 503
Nº 3702
Doc

- **show access-list** *<acl>* – Shows the ACL and the associated hit counter for each line. This command shows the expanded ACL entries for each object group defined.

Related Information

- **Documentation for PIX Firewall**
- **PIX Command Reference**
- **PIX Support Page**
- **Requests for Comments (RFCs)**
- **Technical Support – Cisco Systems**

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

ROS nº 03/2005 CPMI – CORREIOS
Fls Nº 504
3702
Doc

Segurança Tipo 2 doc 9

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 505
Doc 3702

A through B Commands

aaa accounting

Enable, disable, or view LOCAL, TACACS+, or RADIUS user accounting (on a server designated by the **aaa-server** command). (Configuration mode.)

Configure with the command...	Remove with the command...
aaa accounting include | exclude *acctg_service* **inbound | outbound |** *if_name local_ip local_mask foreign_ip foreign_mask group_tag*	**no aaa accounting include | exclude** *authen_service* **inbound | outbound |** *if_name group_tag* **clear aaa [accounting include | exclude** *authen_service* **inbound | outbound |** *if_name group_tag*]
aaa accounting match *acl_name* **inbound | outbound |** *if_name group_tag*	**no aaa accounting match** *acl_name* **inbound | outbound |** *if_name group_tag*

Show command options	Show command output
show aaa	Displays the AAA authentication configuration.

Syntax Description

accounting	Enable or disable accounting services with authentication server. Use of this command requires that you previously used the **aaa-server** command to designate an authentication server.
acctg_service	The accounting service. Accounting is provided for all services or you can limit it to one or more services. Possible values are **any**, **ftp**, **http**, **telnet**, or *protocol/port*. Use **any** to provide accounting for all TCP services. To provide accounting for UDP services, use the *protocol/port* form. For *protocol/port*, the TCP *protocol* appears as 6, the UDP protocol appears as 17, and so on, and port is the TCP or UDP destination port. A port value of 0 (zero) means all ports. For protocols other than TCP and UDP, the *port* is not applicable and should not be used.
foreign_ip	The IP address of the hosts you want to access the *local_ip* address. Use 0 to mean all hosts.

File No 506
Doc 3702

foreign_mask	Network mask of *foreign_ip*. Always specify a specific mask value. Use 0 if the IP address is 0. Use 255.255.255.255 for a host.
exclude	Create an exception to a previously stated rule by excluding the specified service from authentication, authorization, or accounting to the specified host. The **exclude** parameter improves the former **except** option by allowing the user to specify a port to exclude to a specific host or hosts.
group_tag	The AAA server group tag defined by the **aaa-server** command. To use the local PIX Firewall user authentication database, enter **LOCAL** for this parameter.
if_name	Interface name from which users require authentication. Use *if_name* in combination with the *local_ip* address and the *foreign_ip* address to determine where access is sought and from whom. The *local_ip* address is always on the highest security level interface and *foreign_ip* is always on the lowest.
include	Create a new rule with the specified service to include.
inbound	Authenticate or authorize inbound connections. Inbound means the connection originates on the outside interface and is being directed to the inside interface.
local_ip	The IP address of the host or network of hosts that you want to be authenticated or authorized. You can set this address to **0** to mean all hosts and to let the authentication server decide which hosts are authenticated.
local_mask	Network mask of *local_ip*. Always specify a specific mask value. Use 0 if the IP address is 0. Use 255.255.255.255 for a host.
match *acl_name*	Specify an **access-list** command statement name.
outbound	Authenticate or authorize outbound connections. Outbound means the connection originates on the inside and is being directed to the outside interface.

Usage Guidelines

User accounting services keep a record of which network services a user has accessed. These records are also kept on the designated AAA server. Accounting information is only sent to the active server in a server group.

Use the **aaa accounting** command with the **aaa authentication** and **aaa authorization** commands.

The **include** and **exclude** options are not backward compatible with previous PIX Firewall versions. If you downgrade to an earlier version, the **aaa** command statements will be removed from your configuration.

Note Traffic that is not specified by an **include** statement is not processed.

For outbound connections, first use the **nat** command to determine which IP addresses can access the PIX Firewall. For inbound connections, first use the **static** and **access-list** command statements to determine which inside IP addresses can be accessed through the PIX Firewall from the outside network.

If you want to allow connections to come from any host, code the local IP address and netmask as **0.0.0.0 0.0.0.0**, or **0 0**. The same convention applies to the foreign host IP address and netmask; **0.0.0.0 0.0.0.0** means any foreign host.

Tip The **help aaa** command displays the syntax and usage for the **aaa authentication**, **aaa authorization**, **aaa accounting**, and **aaa proxy-limit** commands in summary form.

ROS nº 03/2005 - CPMI - CORREIOS
Fls. Nº 507
3702
Doc

Examples

The default PIX Firewall configuration provides the following **aaa-server** protocols:

```
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server LOCAL protocol local
```

The following example uses the default protocol TACACS+ with the **aaa** commands:

```
aaa-server TACACS+ (inside) host 10.1.1.10 thekey timeout 20
aaa authentication include any outbound 0 0 0 0 TACACS+
aaa authorization include any outbound 0 0 0 0
aaa accounting include any outbound 0 0 0 0 TACACS+
aaa authentication serial console TACACS+
```

This example specifies that the authentication server with the IP address 10.1.1.10 resides on the inside interface and is in the default TACACS+ server group. The next three command statements specify that any users starting outbound connections to any foreign host will be authenticated using TACACS+, that the users who are successfully authenticated are authorized to use any service, and that all outbound connection information will be logged in the accounting database. The last command statement specifies that access to the PIX Firewall unit's serial console requires authentication from the TACACS+ server.

Related Commands

- **aaa authorization**
- **auth-prompt**
- **service**
- **ssh**
- **telnet**
- **virtual**

aaa authentication

Enable, disable, or view LOCAL, TACACS+, or RADIUS user authentication (on a server designated by the **aaa-server** command). Additionally, the **aaa authentication** command has been modified to support PDM authentication. (Configuration mode.)

Configure with the command...	Remove with the command...
aaa authentication include | exclude *authen_service* **inbound | outbound |** *if_name local_ip local_mask foreign_ip foreign_mask group_tag*	**no aaa authentication [include | exclude** *authen_service* **inbound | outbound |** *if_name local_ip local_mask foreign_ip foreign_mask group_tag*] **clear aaa [authentication include | exclude** *authen_service* **inbound | outbound |** *if_name local_ip local_mask foreign_ip foreign_mask group_tag*]
aaa authentication match *acl_name* **inbound | outbound |** *if_name group_tag*	**no aaa authentication match** *acl_name* **inbound | outbound |** *if_name group_tag*
aaa authentication [serial | enable | telnet | ssh | http] console *group_tag*	**no aaa authentication [serial | enable | telnet | ssh | http] console** *group_tag*

ROS nº 03/2005 - CPMI - CORREIOS
Fls Nº 508
Doc 3702

Show command options	Show command output
show aaa	Displays the AAA authentication configuration.

Syntax Description

authen_service	The application with which a user is accessing a network. Use **any**, **ftp**, **http**, or **telnet**. The **any** value enables accounting or authentication for all TCP services. To have users prompted for authentication credentials, they must use FTP, HTTP, or Telnet. (HTTP is the Web and only applies to web browsers that can prompt for a username and password.) If the authentication or authorization server is authenticating services other than FTP, HTTP, or Telnet, using **any** will not permit those services to authenticate in the firewall. The firewall only knows how to communicate with FTP, HTTP, and Telnet for authentication and authorization. Only set this parameter to a service other than **any** if the authentication or authorization server is set the same way. Unless you want to temporarily restrict access to a specific service, setting a service in this command can increase system administration work and may cause all connections to fail if the authentication or authorization server is authenticating one service and you set this command to another.
authentication	Enable or disable user authentication, prompt user for username and password, and verify information with authentication server. When used with the **console** option, enables or disables authentication service for access to the PIX Firewall console over Telnet or from the Console connector on the PIX Firewall unit. Use of the **aaa authentication** command requires that you previously used the **aaa-server** command to designate an authentication server. The **aaa authentication** command supports HTTP authentication. The PIX Firewall requires authentication verification of the HTTP server through the **aaa authentication http console** command before PDM can access the PIX Firewall.
console	Specify that access to the PIX Firewall console require authentication and optionally, log configuration changes to a syslog server. The maximum password length for accessing the console is 16 characters.
enable	Access verification for the PIX Firewall unit's privilege mode.
exclude	Create an exception to a previously stated rule by excluding the specified service from authentication, authorization, or accounting to the specified host. The **exclude** parameter improves the former **except** option by allowing the user to specify a port to exclude to a specific host or hosts.
foreign_ip	The IP address of the hosts you want to access the *local_ip* address. Use 0 to mean all hosts.
foreign_mask	Network mask of *foreign_ip*. Always specify a specific mask value. Use 0 if the IP address is 0. Use 255.255.255.255 for a host.
group_tag	The AAA server group tag defined by the **aaa-server** command. To use the local PIX Firewall user authentication database, enter **LOCAL** for this parameter.

NCS nº 03/2005 - DA
CPMI - CORREIOS
Fls. Nº 509
Doc 3702

http	Access verification for the HTTP (Hypertext Transfer Protocol) access to the PIX Firewall (via PDM). The maximum username prompt for HTTP authentication is 30 characters. The maximum password length is 15 characters.
if_name	The interface name from which to authenticate users.
inbound	Authenticate or authorize inbound connections. Inbound means the connection originates on the outside interface and is being directed to the inside interface.
include	Create a new rule with the specified service to include.
local_ip	The IP address of the host or network of hosts that you want to be authenticated or authorized. You can set this address to **0** to mean all hosts and to let the authentication server decide which hosts are authenticated.
local_mask	Network mask of *local_ip*. Always specify a specific mask value. Use 0 if the IP address is 0. Use 255.255.255.255 for a host.
match *acl_name*	Specify an **access-list** command statement name.
outbound	Authenticate or authorize outbound connections. Outbound means the connection originates on the inside and is being directed to the outside interface.
serial	Access verification for the PIX Firewall unit's serial console.
ssh	Access verification for the SSH access to the PIX Firewall console.
telnet	Access verification for the Telnet access to the PIX Firewall console.

Defaults

If an **aaa authentication http console** *group_tag* command statement is not defined, you can gain access to the PIX Firewall (via PDM) with no username and the PIX Firewall enable password (set with the **password** command). If the **aaa** commands are defined but the HTTP authentication requests a time out, which implies the AAA servers may be down or not available, you can gain access to the PIX Firewall using the username **pix** and the enable password. By default, the enable password is not set.

PIX Firewall supports authentication usernames up to 127 characters and passwords of up to 63 characters. A password or username may not contain an "@" character as part of the password or username string, with a few exceptions.

Tip The **help aaa** command displays the syntax and usage for the **aaa authentication**, **aaa authorization**, **aaa accounting**, and **aaa proxy-limit** commands in summary form.

Usage Guidelines

To use the **aaa authentication** command, you must first designate an authentication server with the **aaa-server** command. Also, for each IP address, one **aaa authentication** command is permitted for inbound connections and one for outbound connections.

Use the *if_name*, *local_ip*, and *foreign_ip* variables to define where access is sought and from whom. The address for *local_ip* is always on the highest security level interface and *foreign_ip* is always on the lowest.

The **aaa authentication** command is not intended to mandate your security policy. The authentication servers determine whether a user can or cannot access the system, what services can be accessed, and what IP addresses the user can access. The PIX Firewall interacts with FTP, HTTP (Web access), and

16.206

Telnet to display the credentials prompts for logging in to the network or logging in to exit the network. You can specify that only a single service be authenticated, but this must agree with the authentication server to ensure that both the firewall and server agree.

The **include** and **exclude** options are not backward compatible with previous PIX Firewall versions. If you downgrade to an earlier version, these **aaa authentication** command statements will be removed from your configuration.

The aaa authentication console Command

The **aaa authentication serial console** command allows you to require authentication verification to access the PIX Firewall unit's serial console. The **serial console** options also logs to a syslog server changes made to the configuration from the serial console.

Authenticated access to the PIX Firewall console has different types of prompts depending on the option you choose with the **aaa authentication** [**serial** | **enable** | **telnet** | **ssh**] **console** command. While the **enable** and **ssh** options allow three tries before stopping with an access denied message, both the **serial** and **telnet** options cause the user to be prompted continually until successfully logging in. The **serial** option requests a username and password before the first command line prompt on the serial console connection. The **telnet** option forces you to specify a username and password before the first command line prompt of a Telnet console connection. The **enable** option requests a username and password before accessing privileged mode for serial, Telnet, or SSH connections. The **ssh** option requests a username and password before the first command line prompt on the SSH console connection. The **ssh** option allows a maximum of three authentication attempts.

Telnet access to the PIX Firewall console is available from any internal interface, and from the outside interface with IPSec configured, and requires previous use of the **telnet** command. SSH access to the PIX Firewall console is also available from any interface without IPSec configured, and requires previous use of the **ssh** command.

The new **ssh** option specifies the group of AAA servers to be used for SSH user authentication. The authentication protocol and AAA server IP addresses are defined with the **aaa-server** command statement.

Similar to the Telnet model, if an **aaa authentication ssh console** *group_tag* command statement is not defined, you can gain access to the PIX Firewall console with the username **pix** and with the PIX Firewall Telnet password (set with the **passwd** command). If the **aaa** command is defined but the SSH authentication requests timeouts, which implies the AAA servers may be down or not available, you can gain access to the PIX Firewall using username **pix** and the enable password (set with the **enable password** command). By default, the Telnet password is **cisco** and the enable password is not set.

If the console login request times out, you can gain access to the PIX Firewall from the serial console by entering the **pix** username and the enable password.

Enabling Authentication

The **aaa authentication** command enables or disables the following AAA (authentication, authorization, and accounting) features:

- User authentication services provided by a TACACS+ or RADIUS server are first designated with the **aaa authorization** command. A user starting a connection via FTP, Telnet, or over the World Wide Web is prompted for their username and password. If the username and password are verified by the designated TACACS+ or RADIUS authentication server, the PIX Firewall unit will allow further traffic between the authentication server and the connection to interact independently through the PIX Firewall unit's "cut-through proxy" feature.
- Administrative authentication services providing access to the PIX Firewall unit's console via Telnet, SSH, or the serial console. Telnet access requires previous use of the **telnet** command. SSH access requires previous use of the **ssh** command.

ROS nº 03/2005 - 0
CPMI - CORREIOS
Fls. Nº 511
3702
Doc

The prompts users see requesting AAA credentials differ between the three services that can access the PIX Firewall for authentication: Telnet, FTP, and HTTP (Web):

- Telnet users see a prompt generated by the PIX Firewall that you can change with the **auth-prompt** command. The PIX Firewall permits a user up to four chances to log in and then if the username or password still fails, the PIX Firewall drops the connection.
- FTP users receive a prompt from the FTP program. If a user enters an incorrect password, the connection is dropped immediately. If the username or password on the authentication database differs from the username or password on the remote host to which you are using FTP to access, enter the username and password in these formats:

  authentication_user_name@*remote_system_user_name*
  authentication_password@*remote_system_password*

  If you daisy-chain PIX Firewall units, Telnet authentication works in the same way as a single unit, but FTP and HTTP authentication have additional complexity for users because they have to enter each password and username with an additional at (@) character and password or username for each daisy-chained system. Users can exceed the 63-character password limit depending on how many units are daisy-chained and password length.

  Some FTP graphical user interfaces (GUIs) do not display challenge values.
- HTTP users see a pop-up window generated by the browser itself. If a user enters an incorrect password, the user is reprompted. When the web server and the authentication server are on different hosts, use the **virtual** command to get the correct authentication behavior.

Authenticated access to the PIX Firewall console has different types of prompts depending on the option you choose with the **aaa authentication console** command:

- **enable** option—Allows three tries before stopping with "Access denied." The **enable** option requests a username and password before accessing privileged mode for serial or Telnet connections.
- **serial** option—Causes the user to be prompted continually until successfully logging in. The **serial** option requests a username and password before the first command line prompt on the serial console connection.
- **ssh** option—Allows three tries before stopping with "Rejected by Server." The **ssh** option requests a username and password before the first command line prompt appears.
- **telnet** option—Causes the user to be prompted continually until successfully logging in. The **telnet** option forces you to specify a username and password before the first command line prompt of a Telnet console connection.

You can specify an interface name with the **aaa authentication** command. In previous versions, if you specified **aaa authentication include any outbound 0 0** *server*, PIX Firewall only authenticated outbound connections and not those to the perimeter interface. PIX Firewall now authenticates any outbound connection to the outside as well as to hosts on the perimeter interface. To preserve the behavior of previous versions, use these commands to enable authentication and to disable authentication from the inside to the perimeter interface:

```
aaa authentication include any outbound 0 0 server
aaa authentication exclude outbound perim_net perim_mask server
```

When a host is configured for authentication, all users on the host must use a web browser or Telnet first before performing any other networking activity, such as accessing mail or a news reader. The reason for this is that users must first establish their authentication credentials and programs such as mail agents and newsreaders do not have authentication challenge prompts.

The PIX Firewall only accepts 7-bit characters during authentication. After authentication, the client and server can negotiate for 8 bits if required. During authentication, the PIX Firewall only negotiates Go-Ahead, Echo, and NVT (network virtual terminal).

HTTP Authentication

When using HTTP authentication to a site running Microsoft IIS that has "Basic text authentication" or "NT Challenge" enabled, users may be denied access from the Microsoft IIS server. This occurs because the browser appends the string: "Authorization: Basic=Uuhjksdkfhk==" to the HTTP GET commands. This string contains the PIX Firewall authentication credentials.

Windows NT Microsoft IIS servers respond to the credentials and assume that a Windows NT user is trying to access privileged pages on the server. Unless the PIX Firewall username password combination is exactly the same as a valid Windows NT username and password combination on the Microsoft IIS server, the HTTP GET command is denied.

To solve this problem, PIX Firewall provides the **virtual http** command, which redirects the browser's initial connection to another IP address, authenticates the user, then redirects the browser back to the URL which the user originally requested.

Once authenticated, a user never has to reauthenticate no matter how low the PIX Firewall uauth timeout is set. This is because the browser caches the "Authorization: Basic=Uuhjksdkfhk==" string in every subsequent connection to that particular site. This can *only* be cleared when the user exits *all* instances of Netscape Navigator or Internet Explorer and restarts. Flushing the cache is of no use.

As long as the user repeatedly browses the Internet, the browser resends the "Authorization: Basic=Uuhjksdkfhk==" string to transparently reauthenticate the user.

Multimedia applications such as CU-SeeMe, Intel Internet Phone, MeetingPoint, and MS Netmeeting silently start the HTTP service before an H.323 session is established from the inside to the outside.

Network browsers such as Netscape Navigator do not present a challenge value during authentication; therefore, only password authentication can be used from a network browser.

Note To avoid interfering with these applications, do not enter blanket outgoing **aaa** command statements for all challenged ports such as using the **any** option. Be selective with which ports and addresses you use to challenge HTTP, and when to set user authentication timeouts to a higher timeout value. If interfered with, the multimedia programs may fail on the PC and may even crash the PC after establishing outgoing sessions from the inside.

TACACS+ and RADIUS servers

Up to 196 TACACS+ or RADIUS servers are permitted (up to 14 servers in each of the up to 14 server groups—set with the **aaa-server** command). When a user logs in, the servers are accessed one at a time starting with the first server you specify in the configuration, until a server responds.

The PIX Firewall permits only one authentication type per network. For example, if one network connects through the PIX Firewall using TACACS+ for authentication, another network connecting through the PIX Firewall can authenticate with RADIUS, but one network cannot authenticate with both TACACS+ and RADIUS.

For the TACACS+ server, if you do not specify a key to the **aaa-server** command, no encryption occurs.

The PIX Firewall displays the same timeout message for both RADIUS and TACACS+. The message "aaa server host machine not responding" displays when either of the following occurs:

- The AAA server system is down.
- The AAA server system is up, but the service is not running.

ROS nº 03/2005 - Fls
CPMI - CORREIOS
Fls Nº 513
Nº 3702
Doc

Previously, TACACS+ differentiated between the two preceding states and provided two different timeout messages, while RADIUS did not differentiate between the two states and provided one timeout message.

match *acl_name* Option Usage

The syntax for this command is as follows:

aaa authentication | authorization | accounting match *acl_name* **inbound | outbound |** *interface_name group_tag*

An example follows:

```
show access-list
access-list mylist permit tcp 10.0.0.0 255.255.255.0 172.23.2.0 255.255.255.0 (hitcnt=0)
access-list yourlist permit tcp any any (hitcnt=0)
show aaa
aaa authentication match mylist outbound TACACS+
```

Similar to IPSec, the keyword **permit** means "yes" and **deny** means "no." Therefore, the following command,

```
aaa authentication match yourlist outbound tacacs
```

is equal to this command:

```
aaa authentication include any outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 tacacs
```

The **aaa** command statement list is order dependent between **access-list** command statements. If the following command is entered:

```
aaa authentication match yourlist outbound tacacs
```

after this command:

```
aaa authentication match mylist outbound TACACS+
```

PIX Firewall tries to find a match in the mylist **access-list** command statement group before it tries to find a match in the yourlist **access-list** command statement group.

Old **aaa** command configuration and functionality stays the same and is not converted to the **access-list** format. Hybrid configurations; that is, old configurations combined with the new **access-list** configuration are not recommended.

Examples

The following example shows use of the **aaa authentication** command:

```
pixfirewall(config) aaa authentication telnet console radius
```


Fls № 514
№ Doc. 3702

The following example lists the new include and exclude options:

```
aaa authentication include any outbound 172.31.0.0 255.255.0.0 0.0.0.0 0.0.0.0 tacacs+
aaa authentication exclude telnet outbound 172.31.38.0 255.255.255.0 0.0.0.0 0.0.0.0
tacacs+
```

The following examples demonstrate ways to use the *if_name* parameter. The PIX Firewall has an inside network of 192.168.1.0, an outside network of 209.165.201.0 (subnet mask 255.255.255.224), and a perimeter network of 209.165.202.128 (subnet mask 255.255.255.224).

This example enables authentication for connections originated from the inside network to the outside network:

```
aaa authentication include any outbound 192.168.1.0 255.255.255.0 209.165.201.0
255.255.255.224 tacacs+
```

This example enables authentication for connections originated from the inside network to the perimeter network:

```
aaa authentication include any outbound 192.168.1.0 255.255.255.0 209.165.202.128
255.255.255.224 tacacs+
```

This example enables authentication for connections originated from the outside network to the inside network:

```
aaa authentication include any inbound 192.168.1.0 255.255.255.0 209.165.201.0
255.255.255.224 tacacs+
```

This example enables authentication for connections originated from the outside network to the perimeter network:

```
aaa authentication include any inbound 209.165.201.0 255.255.255.224 209.165.202.128
255.255.255.224 tacacs+
```

This example enables authentication for connections originated from the perimeter network to the outside network:

```
aaa authentication include any outbound 209.165.202.128 255.255.255.224 209.165.201.0
255.255.255.224 tacacs+
```

This example specifies that IP addresses 10.0.0.1 through 10.0.0.254 can originate outbound connections and then enables user authentication so that those addresses must enter user credentials to exit the PIX Firewall. In this example, the first **aaa authentication** command permits authentication on FTP, HTTP, or Telnet depending on what the authentication server handles. The second **aaa authentication** command lets host 10.0.0.42 start outbound connections without being authenticated. This example uses the default authentication group **tacacs+**.

```
nat (inside) 1 10.0.0.0 255.255.255.0
aaa authentication include any outbound 0 0 tacacs+
aaa authentication exclude outbound 10.0.0.42 255.255.255.255 tacacs+ any
```

This example permits inbound access to any IP address in the range of 209.165.201.1 through 209.165.201.30 indicated by the 209.165.201.0 network address (subnet mask 255.255.255.224). All services are permitted by the **access-list** command, and the **aaa authentication** command permits authentication on FTP, HTTP, or Telnet depending on what the authentication server handles. The authentication server is at IP address 10.16.1.20 on the inside interface.

```
aaa-server AuthIn protocol tacacs+
aaa-server AuthIn (inside) host 10.16.1.20 thisisakey timeout 20
static (inside,outside) 209.165.201.0 10.16.1.0 netmask 255.255.255.224
access-list acl_out permit tcp 10.16.1.0 255.255.255.0 209.165.201.0 255.255.255.224
access-group acl_out in interface outside
aaa authentication include any inbound 0 0 AuthIn
```


FOS nº 03/2008 Fls.
CPMI CORREIOS
Fls. Nº 515
Nº 3702
Doc

Related Commands

- **aaa authorization**
- **auth-prompt**
- **service**
- **ssh**
- **telnet**
- **virtual**

aaa authorization

Enable or disable LOCAL or TACACS+ user authorization services. (Configuration mode.)

Configure with the command...	Remove with the command...
aaa authorization command {**LOCAL** | *tacacs_server_tag*}	**no aaa authorization command** {**LOCAL** | *tacacs_server_tag*}
aaa authorization include | **exclude** *author_service* **inbound** | **outbound** | *if_name local_ip local_mask foreign_ip foreign_mask*	**no aaa authorization** [**include** | **exclude** *author_service* **inbound** | **outbound** | *if_name local_ip local_mask foreign_ip foreign_mask*] **clear aaa** [**authorization** [**include** | **exclude** *author_service* **inbound** | **outbound** | *if_name local_ip local_mask foreign_ip foreign_mask*]]
aaa authorization match *acl_name* **inbound** | **outbound** | *if_name group_tag*	**no aaa authorization match** *acl_name* **inbound** | **outbound** | *if_name group_tag*

Show command options	Show command output
show aaa	Displays the AAA authentication configuration.

File N° 516
Doc 3702

Syntax Description

authorization	Enable or disable TACACS+ user authorization for services (PIX Firewall does not support RADIUS authorization). The authentication server determines what services the user is authorized to access.
author_service	The services which require authorization. Use **any**, **ftp**, **http**, **telnet**, or *protocol/port*. Use **any** to provide authorization for all TCP services. To provide authorization for UDP services, use the *protocol/port* form. Services not specified are authorized implicitly. Services specified in the **aaa authentication** command do not affect the services which require authorization. For *protocol/port*: • *protocol*—the protocol (6 for TCP, 17 for UDP, 1 for ICMP, and so on). • *port*—the TCP or UDP destination port, or port range. The *port* can also be the ICMP type; that is, 8 for ICMP echo or ping. A port value of 0 (zero) means all ports. Port ranges only applies to the TCP and UDP protocols, not to ICMP. For protocols other than TCP, UDP, and ICMP the *port* is not applicable and should not be used. An example port specification follows. `aaa authorization include udp/53-1024 inside 0 0 0 0` This example enables authorization for DNS lookups to the inside interface for all clients, and authorizes access to any other services that have ports in the range of 53 to 1024. **Note** Specifying a port range may produce unexpected results at the authorization server. PIX Firewall sends the port range to the server as a string with the expectation that the server will parse it out into specific ports. Not all servers do this. In addition, you may want users to be authorized on specific services, which will not occur if a range is accepted.
foreign_ip	The IP address of the hosts you want to access the *local_ip* address. Use 0 to mean all hosts.
foreign_mask	Network mask of *foreign_ip*. Always specify a specific mask value. Use 0 if the IP address is 0. Use 255.255.255.255 for a host.
exclude	Create an exception to a previously stated rule by excluding the specified service from authentication, authorization, or accounting to the specified host. The **exclude** parameter improves the former **except** option by allowing the user to specify a port to exclude to a specific host or hosts.
group_tag	Specifies the AAA server. Enter **LOCAL** for the group tag value for local AAA services such as local command authorization using privilege levels, or use the AAA server group tag as defined by the **aaa-server** command.
if_name	Interface name from which users require authentication. Use *if_name* in combination with the *local_ip* address and the *foreign_ip* address to determine where access is sought and from whom. The *local_ip* address is always on the highest security level interface and *foreign_ip* is always on the lowest.
include	Create a new rule with the specified service to include.

Fls Nº 517
Nº 3702
Doc

inbound	Authenticate or authorize inbound connections. Inbound means the connection originates on the outside interface and is being directed to the inside interface.
LOCAL	Specifies to use the PIX Firewall local user database for local command authorization (using privilege levels).
local_ip	The IP address of the host or network of hosts that you want to be authenticated or authorized. You can set this address to **0** to mean all hosts and to let the authentication server decide which hosts are authenticated.
local_mask	Network mask of *local_ip*. Always specify a specific mask value. Use 0 if the IP address is 0. Use 255.255.255.255 for a host.
match *acl_name*	Specify an **access-list** command statement name.
outbound	Authenticate or authorize outbound connections. Outbound means the connection originates on the inside and is being directed to the outside interface.
tacacs_server_tag	Specifies to use a TACACS user authentication server.

Usage Guidelines

Except for its use with command authorization, the **aaa authorization** command requires previous configuration with the **aaa authentication** command; however, use of the **aaa authentication** command does not require use of an **aaa authorization** command.

Currently, the **aaa authorization** command is supported for use with LOCAL and TACACS+ servers but not with RADIUS servers.

Tip The **help aaa** command displays the syntax and usage for the **aaa authentication**, **aaa authorization**, **aaa accounting**, and **aaa proxy-limit** commands in summary form.

For each IP address, one **aaa authorization** command is permitted. If you want to authorize more than one service with **aaa authorization**, use the **any** parameter for the service type.

If the first attempt at authorization fails and a second attempt causes a timeout, use the **service resetinbound** command to reset the client that failed the authorization so that it will not retransmit any connections. An example authorization timeout message in Telnet follows.

```
Unable to connect to remote host: Connection timed out
```

User authorization services control which network services a user can access. After a user is authenticated, attempts to access restricted services cause the PIX Firewall unit to verify the access permissions of the user with the designated AAA server.

The **include** and **exclude** options are not backward compatible with previous PIX Firewall versions. If you downgrade to an earlier version, the **aaa** command statements will be removed from your configuration.

Note RADIUS authorization is supported for use with **access-list** command statements and for use in configuring a RADIUS server with an **acl=***acl_name* vendor-specific identifier. Refer to the **access-list** command page for more information. Also see the **aaa-server radius-authport** commands.

If the AAA console login request times out, you can gain access to the PIX Firewall from the serial console by entering the **pix** username and the enable password.

Examples

The default PIX Firewall configuration provides the following **aaa-server** protocols:

```
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server LOCAL protocol local
```

The following example uses the default protocol TACACS+ with the **aaa** commands:

```
aaa-server TACACS+ (inside) host 10.1.1.10 thekey timeout 20
aaa authentication include any outbound 0 0 0 0 TACACS+
aaa authorization include any outbound 0 0 0 0
aaa accounting include any outbound 0 0 0 0 TACACS+
aaa authentication serial console TACACS+
```

This example specifies that the authentication server with the IP address 10.1.1.10 resides on the inside interface and is in the default TACACS+ server group. The next three command statements specify that any users starting outbound connections to any foreign host will be authenticated using TACACS+, that the users who are successfully authenticated are authorized to use any service, and that all outbound connection information will be logged in the accounting database. The last command statement specifies that access to the PIX Firewall unit's serial console requires authentication from the TACACS+ server.

The following example enables authorization for DNS lookups from the outside interface:

```
aaa authorization include udp/53 inbound 0.0.0.0 0.0.0.0
```

The following example enables authorization of ICMP echo-reply packets arriving at the inside interface from inside hosts:

```
aaa authorization include 1/0 outbound 0.0.0.0 0.0.0.0
```

This means that users will not be able to ping external hosts if they have not been authenticated using Telnet, HTTP, or FTP.

The following example enables authorization for ICMP echoes (pings) only that arrive at the inside interface from an inside host:

```
aaa authorization include 1/8 outbound 0.0.0.0 0.0.0.0
```

Related Commands

- **aaa authorization**
- **auth-prompt**
- **service**
- **ssh**
- **telnet**
- **virtual**

ROS nº 03/200
CPMI - CORREIOS
Fls Nº 519
3702
Doc

aaa proxy-limit

Specifies the number of concurrent proxy connections allowed per user. (Configuration mode.)

Configure with the command...	Remove with the command...
aaa proxy-limit *proxy_limit* | **disable**	**no aaa-server** *group_tag* (*if_name*) **host** *server_ip key* **timeout** *seconds* **clear aaa-server** [*group_tag*]

Show command options	Show command output
show aaa proxy-limit	Displays the number of outstanding authentication requests allowed, or indicates that the proxy limit is disabled if disabled.

Syntax Description

disable	Disables the proxy limit.
group_tag	Specifies the AAA server. Enter **LOCAL** for the group tag value for local AAA services such as local command authorization using privilege levels, or use the AAA server group tag as defined by the **aaa-server** command.
proxy_limit	Specifies the number of concurrent proxy connections allowed per user, from 1 to 128. (The default value is 3.)

Usage Guidelines

The **aaa proxy-limit** command enables you to manually configure the uauth session limit by setting the maximum number of concurrent proxy connections allowed per user. By default, this value is set to 3. If a source address is a proxy server, consider excluding this IP address from authentication or increasing the number of allowable outstanding AAA requests.

Examples

The following example shows how to set and display the maximum number of outstanding authentication requests allowed:

```
pixdoc515(config)# aaa proxy-limit 6
pixdoc515(config)# show aaa proxy-limit
aaa proxy-limit 6
```


RQS nº 03/2005 - CN
CPMI CORREIOS
Fls. Nº 520
3702
Doc

aaa-server

Specify an AAA server. (Configuration mode.)

Configure with the command...	Remove with the command...
aaa-server *group_tag* (*if_name*) **host** *server_ip key* **timeout** *seconds*	**no aaa-server** *group_tag* (*if_name*) **host** *server_ip key* **timeout** *seconds* **clear aaa-server** [*group_tag*]
aaa-server *group_tag* **protocol** *auth_protocol*	**N/A**
aaa-server radius-acctport *port*	**N/A**
aaa-server radius-authport *port*	**N/A**
debug radius session	**N/A**
show aaa-server	**N/A**

Show command options	Show command output
show aaa-server	Displays AAA server configuration.

Syntax Description

aaa-server	Specifies an AAA server or up to 14 groups of servers with a maximum of 14 servers each. Certain types of AAA services can be directed to different servers. Services can also be set up to fail over to multiple servers.
aaa-server radius-acctport	Sets the port number of the RADIUS server which the PIX Firewall unit will use for accounting functions. The default port number used for RADIUS accounting is **1646**.
aaa-server radius-authport	Sets the port number of the RADIUS server which the PIX Firewall will use for authentication functions. The default port number used for RADIUS authentication is **1645**.
debug radius session	Captures RADIUS session information and attributes for sent and received RADIUS packets.
group_tag	An alphanumeric string which is the name of the server group. Use the *group_tag* in the **aaa** command to associate **aaa authentication** and **aaa accounting** command statements to an AAA server. Up to 14 server groups are permitted. However, **LOCAL** cannot used with **aaa-server** command because **LOCAL** is predefined by the PIX Firewall.
host *server_ip*	The IP address of the TACACS+ or RADIUS server.
if_name	The interface name on which the server resides.
key	A case-sensitive, alphanumeric keyword of up to 127 characters that is the same value as the key on the TACACS+ server. Any characters entered past 127 are ignored. The key is used between the client and server for encrypting data between them. The *key* must be the same on both the client and server systems. Spaces are not permitted in the key, but other special characters are.
no aaa-server	Unbinds an AAA server from and interface or host.

CPM
File N° 521
Doc 3702

port	Specifies the destination TCP/UDP port number of the remote RADIUS server host to which you wish to assign authentication or accounting functions for the PIX Firewall. These port pairs are listed as assigned to authentication and accounting services on RADIUS servers: • 1645 (authentication), 1646 (accounting) - default for PIX Firewall • 1812 (authentication), 1813 (accounting) - alternate You can view these and other commonly used port number assignments online at the following website: http://www.iana.org/assignments/port-numbers See "Ports" in Chapter 2, "Using PIX Firewall Commands" for additional information.
protocol *auth_protocol*	The type of AAA server, either **tacacs+** or **radius**.
timeout *seconds*	The timeout interval for the request. This is the time after which the PIX Firewall gives up on the request to the primary AAA server. If there is a standby AAA server, the PIX Firewall will send the request to the backup server. The retransmit timeout is currently set to 10 seconds and is not user configurable.

Usage Guidelines

The **aaa-server** command lets you specify AAA server groups. PIX Firewall lets you define separate groups of TACACS+ or RADIUS servers for specifying different types of traffic; such as, a TACACS+ server for inbound traffic and another for outbound traffic. Another use is where all outbound HTTP traffic will be authenticated by a TACACS+ server, and all inbound traffic will use RADIUS.

AAA server groups are defined by a tag name that directs different types of traffic to each authentication server. If the first authentication server in the list fails, the AAA subsystem fails over to the next server in the tag group. You can have up to 14 tag groups and each group can have up to 14 AAA servers for a total of up to 196 AAA servers.

If your RADIUS server uses ports 1812 for authentication and 1813 for accounting, you are required to reconfigure the PIX Firewall to use ports 1812 and 1813.

If accounting is in effect, the accounting information goes only to the active server.

If you are upgrading from a previous version of PIX Firewall and have **aaa** command statements in your configuration, using the default server groups lets you maintain backward compatibility with the **aaa** command statements in your configuration.

Usage Notes

1. The **aaa** command references the tag group. This is a global setting that takes effect when the RADIUS service is started.
2. The previous server type option at the end of the **aaa authentication** and **aaa accounting** commands has been replaced with the **aaa-server** group tag. Backward compatibility with previous versions is maintained by the inclusion of two default protocols for TACACS+ and RADIUS.
3. Changing authorization and accounting port settings is possible. By default, PIX Firewall listens for RADIUS on ports 1645 and 1646. If your RADIUS server uses ports 1812 and 1813, you may also reconfigure it to use ports 1812 and 1813 with the **aaa-server radius-authport** and **aaa-server radius-acctport** commands.

4. Newer RADIUS servers may use the port numbers 1812 and 1813 as defined in RFC 2138 and RFC 2139. If your server uses ports other than 1645 and 1646, then you should define ports using the **aaa-server radius-authport** and **aaa-server radius-acctport** commands prior to starting the RADIUS service with the **aaa-server** command.

Defaults

By default, the PIX Firewall listens for RADIUS on ports **1645** for authentication and **1646** for accounting. (The default ports are 1645 for authentication and 1646 for accounting as defined in RFC 2058.)

The default configuration provides the following **aaa-server** protocols:

```
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server LOCAL protocol local
```

Examples

The following example uses the default protocol TACACS+ with the **aaa** commands:

```
aaa-server TACACS+ (inside) host 10.1.1.10 thekey timeout 20
aaa authentication include any outbound 0 0 0 0 TACACS+
aaa authorization include any outbound 0 0 0 0
aaa accounting include any outbound 0 0 0 0 TACACS+
aaa authentication serial console TACACS+
```

This example specifies that the authentication server with the IP address 10.1.1.10 resides on the inside interface and is in the default TACACS+ server group. The next three command statements specify that any users starting outbound connections to any foreign host will be authenticated using TACACS+, that the users who are successfully authenticated are authorized to use any service, and that all outbound connection information will be logged in the accounting database. The last command statement specifies that access to the PIX Firewall unit's serial console requires authentication from the TACACS+ server.

This example creates the AuthOut and AuthIn server groups for RADIUS authentication and specifies that servers 10.0.1.40, 10.0.1.41, and 10.1.1.2 on the inside interface provide authentication. The servers in the AuthIn group authenticate inbound connections, the AuthOut group authenticates outbound connections.

```
aaa-server AuthIn protocol radius
aaa-server AuthIn (inside) host 10.0.1.40 ab timeout 20
aaa-server AuthIn (inside) host 10.0.1.41 abc timeout 4
aaa-server AuthOut protocol radius
aaa-server AuthOut (inside) host 10.1.1.2 abc123 timeout 15
aaa authentication include any inbound 0 0 0 0 AuthIn
aaa authentication include any outbound 0 0 0 0 AuthOut
```

The following example lists the commands that can be used to establish an Xauth crypto map:

```
ip address inside 10.0.0.1 255.255.255.0
ip address outside 168.20.1.5 255.255.255.0
ip local pool dealer 10.1.2.1-10.1.2.254
nat (inside) 0 access-list 80
aaa-server TACACS+ host 10.0.0.2 secret123
crypto ipsec transform-set pc esp-des esp-md5-hmac
crypto dynamic-map cisco 4 set transform-set pc
crypto map partner-map 20 ipsec-isakmp dynamic cisco
crypto map partner-map client configuration address initiate
crypto map partner-map client authentication TACACS+
crypto map partner-map interface outside
isakmp key cisco1234 address 0.0.0.0 netmask 0.0.0.0
isakmp client configuration address-pool local dealer outside
isakmp policy 8 authentication pre-share
```

```
isakmp policy 8 encryption des
isakmp policy 8 hash md5
isakmp policy 8 group 1
isakmp policy 8 lifetime 86400
```

The **aaa-server** command is used with the **crypto map** command to establish an authentication association so that VPN clients are authenticated when they access the PIX Firewall.

Related Commands

- **crypto ipsec**
- **isakmp**

access-group

Binds the access list to an interface. (Configuration mode.)

Configure with the command...	Remove with the command...
access-group *acl_ID* **in interface** *interface_name*	**no access-group** *acl_ID* **in interface** *interface_name* **clear access-group** [*acl_ID*]

Show command options	Show command output
show access-group [*acl_ID*]	Displays the current access list bound to the interfaces.

Syntax Description

acl_ID	The name associated with a given access list.
in interface	Filter inbound packets at the given interface.
interface_name	The name of the network interface.

Usage Guidelines

The access-group command binds an access list to an interface. The access list is applied to traffic inbound to an interface. If you enter the **permit** option in an **access-list** command statement, the PIX Firewall continues to process the packet. If you enter the **deny** option in an **access-list** command statement, PIX Firewall discards the packet and generates the following syslog message.

```
%PIX-4-106019: IP packet from source_addr to destination_addr, protocol protocol received
from interface interface_name deny by access-group acl_ID
```

Always use the **access-list** command with the **access-group** command.

Note The use of **access-group** command overrides the **conduit** and **outbound** command statements for the specified *interface_name*.

The **no access-group** command unbinds the *acl_ID* from the interface *interface_name*.

The **show access-group** command displays the current access list bound to the interfaces.

CPMI
Fls. Nº 524
Doc 3702

The **clear access-group** command removes all entries from an access list indexed by *acl_ID*. If *acl_ID* is not specified, all **access-list** command statements are removed from the configuration.

Examples

The following example shows use of the **access-group** command:

```
static (inside,outside) 209.165.201.3 10.1.1.3
access-list acl_out permit tcp any host 209.165.201.3 eq 80
access-group acl_out in interface outside
```

The **static** command statement provides a global address of 209.165.201.3 for the web server at 10.1.1.3. The **access-list** command statement lets any host access the global address using port 80. The **access-group** command specifies that the **access-list** command statement applies to traffic entering the outside interface.

access-list

Create an access list, or use downloadable access lists. (Downloadable access lists are supported for RADIUS servers only). (Configuration mode.)

Configure with the command...	Remove with the command...
access-list [*acl_ID*] **compiled**	**no access-list** [*acl_ID*] **compiled**
access-list *acl_ID* {**deny** | **permit**} **icmp** {*source_addr* | *local_addr*} {*source_mask* | *local_mask*} {*destination_addr* | *remote_addr*} {*destination_mask* | *remote_mask*} *icmp_type*	**no access-list** [*acl_ID* {**deny** | **permit**} **icmp** {*source_addr* | *local_addr*} {*source_mask* | *local_mask*} {*destination_addr* | *remote_addr*} {*destination_mask* | *remote_mask*} *icmp_type*]
access-list *id* {**deny** | **permit**} **icmp** {*source_addr* | *local_addr*} {*source_mask* | *local_mask*} | **object-group** *network_obj_grp_id* {*destination_addr* | *remote_addr*} {*destination_mask* | *remote_mask*} | **object-group** *network_obj_grp_id* [*icmp_type* | **object-group** *icmp_type_obj_grp_id*]	**no access-list** *id* {**deny** | **permit**} {**icmp** {*source_addr* | *local_addr*} {*source_mask* | *local_mask*} | **object-group** *network_obj_grp_id* {*destination_addr* | *remote_addr*} {*destination_mask* | *remote_mask*} | **object-group** *network_obj_grp_id* [*icmp_type* | **object-group** *icmp_type_obj_grp_id*]}
access-list *acl_ID* {**deny** | **permit**} *protocol* {*source_addr* | *local_addr*} {*source_mask* | *local_mask*}[*operator port* [*port*] {*destination_addr* | *remote_addr*} {*destination_mask* | *remote_mask*} [*operator port* [*port*]	**no access-list** *acl_ID* [{**deny** | **permit**} *protocol* {*source_addr* | *local_addr*} {*source_mask* | *local_mask*} [*operator port* [*port*] {*destination_addr* | *remote_addr*} {*destination_mask* | *remote_mask*} [*operator port* [*port*]]

Configure with the command...	Remove with the command...
access-list *id* {**deny** | **permit**} {*protocol* | **object-group** *protocol_obj_grp_id* {*source_addr* | *local_addr*} {*source_mask* | *local_mask*} | **object-group** *network_obj_grp_id* [*operator port* [*port*] | **object-group** *service_obj_grp_id*] {*destination_addr* | *remote_addr*} {*destination_mask* | *remote_mask*} | **object-group** *network_obj_grp_id* [*operator port* [*port*] | **object-group** *service_obj_grp_id*]}	**no access-list** *id* {**deny** | **permit**} {*protocol* | **object-group** *protocol_obj_grp_id* {*source_addr* | *local_addr*} {*source_mask* | *local_mask*} | **object-group** *network_obj_grp_id* [*operator port* [*port*] | **object-group** *service_obj_grp_id*] {*destination_addr* | *remote_addr*} {*destination_mask* | *remote_mask*} | **object-group** *network_obj_grp_id* [*operator port* [*port*] | **object-group** *service_obj_grp_id*]}
debug access-list all | **standard** | **turbo**	**no debug access-list all** | **standard** | **turbo**
N/A	**clear access-list** [*acl_ID*]
N/A	**clear access-list** *acl_ID* **counters**

Show command options	Show command output
show access-list [[*acl_ID*] *source_addr*]	Displays the **access-list** command statements in the configuration, the hit count of the number of times each element has been matched during an **access-list** command search, and whether or not the list is configured for TurboACL. The *source_addr* option filters the show output so that only those access-list elements that match the source IP address (or with **any** as source IP address) are displayed.

Syntax Description

acl_ID	Name of an access list. You can use either a name or number.
compiled	When used in conjunction with the **access-list** command, this turns on TurboACL unless the **no** qualifier is used, in which case the command **no access-list** *acl_ID* **compiled** turns off TurboACL for that access list. To use TurboACL globally, enter the **access-list compiled** command and to globally turn off TurboACL, enter the **no access-list compiled** command. After TurboACL has been globally configured, individual access lists or groups can have TurboACL enabled or disabled using individual **[no] access-list** *acl_ID* **compiled** commands. TurboACL is compiled only if the number of access list elements is greater than or equal to 19.
debug	Outputs access list debugging information to the console.

ROS nº 03/00
CPMI CORREIOS
Fls Nº 526
3702
Doc

deny	When used with the **access-group** command, the **deny** option does not allow a packet to traverse the PIX Firewall. By default, PIX Firewall denies all inbound or outbound packets unless you specifically permit access. When used with a **crypto map** command statement, **deny** does not select a packet for IPSec protection. The **deny** option prevents traffic from being protected by IPSec in the context of that particular crypto map entry. In other words, it does not allow the policy as specified in the **crypto map** command statements to be applied to this traffic.
destination_addr	IP address of the network or host to which the packet is being sent. Specify a *destination_addr* when the **access-list** command statement is used in conjunction with an **access-group** command statement, or with the **aaa match access-list** command and the **aaa authorization** command. For inbound and outbound connections, *destination_addr* is the address before NAT has been performed.
destination_mask	Netmask bits (mask) to be applied to *destination_addr*, if the destination address is a network mask.
icmp_type	For non-IPSec use only, permit or deny access to ICMP message types. Refer to Table 3-1 for a list of message types. Omit this option to mean all ICMP types. ICMP message types are not supported for use with IPSec; that is when the **access-list** command is used in conjunction with the **crypto map** command, the *icmp_type* is ignored.
local_addr	Address of the network or host local to the PIX Firewall. Specify a *local_addr* when the **access-list** command statement is used in conjunction with a **crypto access-list** command statement, a **nat 0 access-list** command statement, or a **vpngroup split-tunnel** command statement. The *local_addr* is the address after NAT has been performed.
local_mask	Netmask bits (mask) to be applied to *local_addr*, if the local address is a network mask.
object-group	Specifies an object group. Refer to the object-group command for information on how to configure object groups.
obj_grp_id	An existing object group.

RQS nº 03/2005 - CPMI - CORREIOS
Fls Nº 527
3702
Doc

operator	The *operator* compares the source IP address (*sip*) or destination IP address (*dip*) ports. Possible operands include **lt** for less than, **gt** for greater than, **eq** for equal, **neq** for not equal, and **range** for an inclusive range. Use the **access-list** command the without an operator and port to indicate all ports by default.
	
	For example,
	
	`access-list acl_out permit tcp any host 209.165.201.1`
	
	Use **eq** and a port to permit or deny access to just that port. For example, use **eq ftp** to permit or deny access only to FTP.
	
	`access-list acl_out deny tcp any host 209.165.201.1 eq ftp`
	
	Use **lt** and a port to permit or deny access to all ports less than the port you specify. For example, use **lt 2025** to permit or deny access to the well known ports (1 to 1024).
	
	`access-list acl_dmz1 permit tcp any host 192.168.1.1 lt 1025`
	
	Use **gt** and a port to permit or deny access to all ports greater than the port you specify. For example, use **gt 42** to permit or deny ports 43 to 65535.
	
	`access-list acl_dmz1 deny udp any host 192.168.1.2 gt 42`
	
	Use **neq** and a port to permit or deny access to every port except the ports that you specify. For example, use **neq 10** to permit or deny ports 1-9 and 11 to 65535.
	
	`access-list acl_dmz1 deny tcp any host 192.168.1.3 neq 10`
	
	Use **range** and a port range to permit or deny access to only those ports named in the range. For example, use **range 10 1024** to permit or deny access only to ports 10 through 1024. All other ports are unaffected. The use of port ranges can dramatically increase the number of IPSec tunnels. For example, if a port range of 5000 to 65535 is specified for a highly dynamic protocol, up to 60,535 tunnels can be created.

permit	When used with the **access-group** command, the **permit** option selects a packet to traverse the PIX Firewall. By default, PIX Firewall denies all inbound or outbound packets unless you specifically permit access. When used with a **crypto map** command statement, **permit** selects a packet for IPSec protection. The **permit** option causes all IP traffic that matches the specified conditions to be protected by IPSec using the policy described by the corresponding **crypto map** command statements.
port	Services you permit or deny access to. Specify services by the port that handles it, such as **smtp for port 25**, **www** for port 80, and so on. You can specify ports by either a literal name or a number in the range of 0 to 65535. You can view valid port numbers online at the following website: http://www.iana.org/assignments/port-numbers See "Ports" in Chapter 2, "Using PIX Firewall Commands" for a list of valid port literal names in port ranges; for example, **ftp h323**. You can also specify numbers.
protocol	Name or number of an IP protocol. It can be one of the keywords **icmp**, **ip**, **tcp**, or **udp**, or an integer in the range 1 to 254 representing an IP protocol number. To match any Internet protocol, including ICMP, TCP, and UDP, use the keyword **ip**.

RQS nº 03/2005 - CPMI - CORREIOS
Fls Nº 528
Nº 3702
Doc

source_addr	Address of the network or host from which the packet is being sent. Use this field when an **access-list** command statement is used in conjunction with an **access-group** command statement, or with the **aaa match access-list** command and the **aaa authorization** command.
source_mask	Netmask bits (mask) to be applied to *source_addr*, if the source address is for a network mask.
remote_addr	IP address of the network or host remote to the PIX Firewall. Specify a *remote_addr* when the **access-list** command statement is used in conjunction with a **crypto access-list** command statement, a **nat 0 access-list** command statement, or a **vpdn group split-tunnel** command statement.
remote_mask	Netmask bits (mask) to be applied to *remote_addr*, if the remote address is a network mask.

Usage Guidelines

The **access-list** command lets you specify if an IP address is permitted or denied access to a port or protocol. In this document, one or more **access-list** command statements with the same access list name are referred to as an "access list." Access lists associated with IPSec are known as "crypto access lists."

By default, all **access-list** commands have an implicit **deny** unless you explicitly specify **permit**. In other words, by default, all access in an access list is denied unless you explicitly grant access using a **permit** statement.

Note Do not use the string "multicastACL" following the name of a PIX Firewall interface in an access-list name because this is a reserved keyword used by PIX Device Manager (PDM).

Additionally, you can use the **object-group** command to group access lists like any other network object.

Use the following guidelines for specifying a source, local, or destination address:

- Use a 32-bit quantity in four-part, dotted-decimal format.
- Use the keyword **any** as an abbreviation for an address and mask of 0.0.0.0 0.0.0.0. This keyword is normally not recommended for use with IPSec.
- Use **host** *address* as an abbreviation for a mask of 255.255.255.255.

Use the following guidelines for specifying a network mask:

- Do not specify a mask if the address is for a host; if the destination address is for a host, use the **host** parameter before the address.

  For example:

  ```
  access-list acl_grp permit tcp any host 192.168.1.1
  ```

- If the address is a network address, specify the mask as a 32-bit quantity in four-part, dotted-decimal format. Place zeros in the bit positions you want to ignore.
- Remember that you specify a network mask differently than with the Cisco IOS software **access-list** command. With PIX Firewall, use 255.0.0.0 for a Class A address, 255.255.0.0 for a Class B address, and 255.255.255.0 for a Class C address. If you are using a subnetted network address, use the appropriate network mask.

  For example:

  ```
  access-list acl_grp permit tcp any 209.165.201.0 255.255.255.224
  ```


RQS nº 03/2005 - CPMI - CORREIOS
Fls Nº 529
3702
Doc.

If appropriate, after you have defined an access list, bind it to an interface using the **access-group** command. For IPSec use, bind it with a **crypto ipsec** command statement. In addition, you can bind an access list with the RADIUS authorization feature (described in the next section).

The **access-list** command supports the **sunrpc** service.

The **show access-list** command lists the **access-list** command statements in the configuration and the hit count of the number of times each element has been matched during an **access-list** command search. Additionally, it displays the number of access list statements in the access list and indicates whether or not the list is configured for TurboACL. (If the list has less than eighteeen access control entries then it is marked to be turbo-configured but is not actually configured for TurboACL until there are 19 or more entries.)

The **clear access-list** command removes all **access-list** command statements from the configuration or, if specified, access lists by their *acl_ID*. The **clear access-list** *acl_ID* **counters** command clears the hit count for the specified access list.

The **no access-list** command removes an **access-list** command from the configuration. If you remove all the **access-list** command statements in an access list, the **no access-list** command also removes the corresponding **access-group** command from the configuration.

Note The **aaa**, **crypto map**, and **icmp** commands make use of the **access-list** command statements.

RADIUS Authorization

PIX Firewall allows a RADIUS server to send user group attributes to the PIX Firewall in the RADIUS authentication response message. Additionally, the PIX Firewall allows downloadable access lists from the RADIUS server. For example, you can configure an access list on a Cisco Secure ACS server and download it to the PIX Firewall during RADIUS authorization.

After the PIX Firewall authenticates a user, it can then use the CiscoSecure **acl** attribute returned by the authentication server to identify an access list for a given user group. To maintain consistency, PIX Firewall also provides the same functionality for TACACS+.

To restrict users in a department to three servers and deny everything else, the **access-list** command statements are as follows:

```
access-list eng permit ip any server1 255.255.255.255
access-list eng permit ip any server2 255.255.255.255
access-list eng permit ip any server3 255.255.255.255
access-list eng deny ip any any
```

In this example, the vendor specific attribute string in the CiscoSecure configuration has been set to **acl=eng**. Use this field in the CiscoSecure configuration to identify the **access-list** identification name. The PIX Firewall gets the **acl=***acl_ID* from CiscoSecure and extracts the ACL number from the attribute string, which it places in a user's uauth entry. When a user tries to open a connection, PIX Firewall checks the access list in the user's uauth entry, and depending on the permit or deny status of the access list match, permits or denies the connection. When a connection is denied, PIX Firewall generates a corresponding syslog message. If there is no match, then the implicit rule is to deny.

Because the source IP of a given user can vary depending on where they are logging in from, set the source address in the **access-list** command statement to **any**, and the destination address to identify which network services the user is permitted or denied access to. If you want to specify that only users logging in from a given subnet may use the specified services, specify the subnet instead of using **any**.

CPM
File N° 530
N° 3702
Doc

16 j 86
2.

Note An access list used for RADIUS authorization does not require an **access-group** command to bind the statements to an interface.

There is *not* a **radius** option to the **aaa authorization** command.

Configure the access list specified in Attribute 11 to specify a per-user access list name. Otherwise, remove Attribute 11 from the aaa RADIUS server configuration if no access list is intended for user authentication. If the access list is not configured on the PIX Firewall when the user attempts to login, the login will fail.

For more information on how to use RADIUS server authorization, refer to the *Cisco PIX Firewall and VPN Configuration Guide*, version 6.2 or higher.

TurboACL

On the PIX Firewall, TurboACL is turned on globally with the command **access-list compiled** (and turned off globally by the command **no access-list compiled**).

The PIX Firewall default mode is TurboACL off (**no access-list compiled**), and TurboACL is active only on access lists with 19 or more entries.

The minimum amount of Flash memory required to run TurboACL is 2.1 MB. If memory allocation fails, the TurboACL lookup tables will not be generated.

Note Use TurboACL only on PIX Firewall platforms that have 16MB or more of Flash memory. Consequently, TurboACL is not supported on PIX 501 because it has 8MB of Flash memory.

If TurboACL is configured, some access control list or access control list group modifications can trigger regeneration of the TurboACL internal configuration. Depending on the extent of TurboACL configuration(s), this could noticeably consume CPU resources. Consequently, we recommend modifying turbo-complied access lists during non-peak system usage hours.

For more information on how to use TurboACL, refer to the *Cisco PIX Firewall and VPN Configuration Guide*, version 6.2 or higher.

Usage Notes

1. The **clear access-list** command automatically unbinds an access list from a **crypto map** command or interface. The unbinding of an access list from a **crypto map** command can lead to a condition that discards all packets because the **crypto map** command statements referencing the access list are incomplete. To correct the condition, either define other **access-list** command statements to complete the **crypto map** command statements or remove the **crypto map** command statements that pertain to the **access-list** command statement. Refer to the **crypto map** command for more information.
2. Access control lists that are dynamically updated on the PIX Firewall by an AAA server can only be shown using the **show access-list** command. The **write** command does not save or display these updated lists.
3. The **access-list** command operates on a first match basis.
4. If you specify an **access-list** command statement and bind it to an interface with the **access-group** command statement, by default, all traffic inbound to that interface is denied. You must explicitly permit traffic. Note that "inbound" in this context means traffic passing through the interface, rather than the more typical PIX Firewall usage of inbound meaning traffic passing from a lower security level interface to a higher security level interface.

ROS nº 03/2005 - CPMI - CORREIOS
Fls Nº 531
Doc 3702

5. Always permit access first and then deny access afterward. If the host entries match, then use a **permit** statement, otherwise use the default **deny** statement. You only need to specify additional **deny** statements if you need to deny specific hosts and permit everyone else.
6. You can view security levels for interfaces with the **show nameif** command.
7. The ICMP message type (*icmp_type*) option is ignored in IPSec applications because the message type cannot be negotiated with ISAKMP.
8. Only one access list can be bound to an interface using the **access-group** command.
9. If you specify the **permit** option in the access list, the PIX Firewall continues to process the packet. If you specify the **deny** option in the access list, PIX Firewall discards the packet and generates the following syslog message.

   ```
   %PIX-4-106019: IP packet from source_addr to destination_addr, protocol protocol
   received from interface interface_name deny by access-group acl_ID
   ```

   The **access-list** command uses the same syntax as the Cisco IOS software **access-list** command *except* that PIX Firewall uses a subnet mask, whereas Cisco IOS software uses a wildcard mask. (In Cisco IOS software, the mask in this example would be specified with the 0.0.0.255 value.) For example, in the Cisco IOS software **access-list** command, a subnet mask of 0.0.0.255 would be specified as 255.255.255.0 in the PIX Firewall **access-list** command.
10. We recommend that you do not use the **access-list** command with the **conduit** and **outbound** commands. While using these commands together will work, the way in which these commands operate may cause debugging issues because the **conduit** and **outbound** commands operate from one interface to another whereas the **access-list** command used with the **access-group** command applies only to a single interface. If these commands must be used together, PIX Firewall evaluates the **access-list** command before checking the **conduit** and **outbound** commands.
11. Refer to the Chapter 3, "Managing Network Access and Use" in the *Cisco PIX Firewall and VPN Configuration Guide* for a detailed description about using the **access-list** command to provide server access and to restrict outbound user access.
12. Refer to the **aaa-server radius-acctport** and **aaa-server radius-authport** commands to verify or change port settings.

ICMP Message Types

For non-IPSec use only, if you prefer more selective ICMP access, you can specify a single ICMP message type as the last option in this command. Table 3-1 lists possible ICMP types values.

Table 3-1 ICMP Type Literals

ICMP Type	Literal
0	echo-reply
3	unreachable
4	source-quench
5	redirect
6	alternate-address
8	echo
9	router-advertisement
10	router-solicitation
11	time-exceeded

RQS nº 03/2005 CPMI
Fls Nº 532
Doc 3702

Table 3-1 ICMP Type Literals (continued)

ICMP Type	Literal
12	parameter-problem
13	timestamp-reply
14	timestamp-request
15	information-request
16	information-reply
17	mask-request
18	mask-reply
31	conversion-error
32	mobile-redirect

If you specify an ICMP message type for use with IPSec, PIX Firewall ignores it.

For example:

```
access-list 10 permit icmp any any echo-reply
```

IPSec is enabled such that a **crypto map** command references the *acl_ID* for this **access-list** command, then the **echo-repy** ICMP message type is ignored.

Using the access-list Command with IPSec

If an access list is bound to an interface with the **access-group** command, the access list selects which traffic can traverse the PIX Firewall. When bound to a **crypto map** command statement, the access list selects which IP traffic IPSec protects and which traffic IPSec does not protect. For example, access lists can be created to protect all IP traffic between Subnet X and Subnet Y or traffic between Host A and Host B. More information is available in the **crypto map** command section of this guide.

The access lists themselves are not specific to IPSec. It is the **crypto map** command statement referring to the specific access list that defines whether IPSec processing is applied to the traffic matching a permit in the access list.

Crypto access lists associated with the IPSec **crypto map** command statement have these primary functions:

- Select outbound traffic to be protected by IPSec (permit = protect).
- Indicate the data flow to be protected by the new security associations (specified by a single permit entry) when initiating negotiations for IPSec security associations.
- Process inbound traffic to filter out and discard traffic that IPSec protects.
- Determine whether or not to accept requests for IPSec security associations on behalf of the requested data flows when processing IKE negotiation from the IPSec peer. (Negotiation is only done for **crypto map** command statements with the **ipsec-isakmp** option.) For a peer's initiated IPSec negotiation to be accepted, it must specify a data flow that is permitted by a crypto access list associated with an **ipsec-isakmp** crypto map entry.

You can associate a crypto access list with an interface by defining the corresponding **crypto map** command statement and applying the crypto map set to an interface. Different access lists must be used in different entries of the same crypto map set. However, both inbound and outbound traffic will be

evaluated against the same "outbound" IPSec access list. Therefore, the access list's criteria are applied in the forward direction to traffic exiting your PIX Firewall and the reverse direction to traffic entering your PIX Firewall.

If you want certain traffic to receive one combination of IPSec protection (for example, authentication only) and other traffic to receive a different combination of IPSec protection (for example, both authentication and encryption), you need to create two different crypto access lists to define the two different types of traffic. These different access lists are then used in different crypto map entries that specify different IPSec policies.

We recommend that you configure "mirror image" crypto access lists for use by IPSec and that you avoid using the **any** keyword. See the *Cisco PIX Firewall and VPN Configuration Guide* for more information.

If you configure multiple statements for a given crypto access list, in general, the first **permit** statement matched, will be the statement used to determine the scope of the IPSec security association. That is, the IPSec security association will be set up to protect traffic that meets the criteria of the matched statement only. Later, if traffic matches a different **permit** statement of the crypto access list, a new, separate IPSec security association will be negotiated to protect traffic matching the newly matched **access list** command statement.

Some services such as FTP require two **access-list** command statements, one for port 10 and another for port 21, to properly encrypt FTP traffic.

Examples

The following example creates a numbered access list that specifies a Class C subnet for the source and a Class C subnet for the destination of IP packets. Because the **access-list** command is referenced in the **crypto map** command statement, PIX Firewall encrypts all IP traffic that is exchanged between the source and destination subnets.

```
access-list 101 permit ip 172.21.3.0 255.255.0.0 172.22.2.0 255.255.0.0
access-group 101 in interface outside
crypto map mymap 10 match address 101
```

The next example only lets an ICMP message type of echo-reply be permitted into the outside interface:

```
access-list acl_out permit icmp any any echo-reply
access-group acl_out interface outside
```

activation-key

Updates the activation key on your PIX Firewall and checks the activation key running on your PIX Firewall against the activation key stored in the Flash memory of the PIX Firewall. (Configuration mode.)

Configure with the command...	Remove with the command...
activation-key *activation-key-four-tuple*	N/A

Show command options	Show command output
show activation-key	Displays the results of checking the activation key running on the PIX Firewall against the activation key stored in the Flash memory of the PIX Firewall.

Syntax Description

activation-key	Updates the PIX Firewall activation key unless there is a mismatch between the Flash memory and running PIX Firewall software versions.
activation-key-four-tuple	A four-element hexidecimal string with one space between each element. For example: `0xe02888da 0x4ba7bed6 0xf1c123ae 0xffd8624e` (The leading 0x specfier is optional; all values are assumed to be hexadecimal.)

Usage Guidelines

Use the **activation-key** *activation-key-four-tuple* command to change the activation key on your PIX Firewall.

Caution Use only an activation key valid for your PIX Firewall software version and platform or your system may not reload after rebooting.

The **activation-key** *activation-key-four-tuple* command output indicates the status of the activation key as follows:

- If the PIX Firewall Flash memory software image version is the same as the running PIX Firewall software version, and the PIX Firewall Flash memory activation key is the same as the running PIX Firewall software activation key, then the **activation-key** command output reads as follows:

```
The flash activation key has been modified.
The flash activation key is now the SAME as the running key.
```

- If the PIX Firewall Flash memory image version is the same as the running PIX Firewall software, and the PIX Firewall Flash memory activation key is different from the running PIX Firewall activation key, then the **activation-key** command output reads as follows:

```
The flash activation key has been modified.
The flash activation key is now DIFFERENT from the running key.
The flash activation key will be used when the unit is reloaded.
```

- If the PIX Firewall Flash memory image version is not the same as the running PIX Firewall software, then the **activation-key** command output reads as follows:

```
The flash image is DIFFERENT from the running image.
The two images must be the same in order to modify the flash activation key.
```

- If the PIX Firewall Flash memory image version is the same as the running PIX Firewall software, and the entered activation key is not valid, then the **activation-key** command output reads as follows:

```
ERROR: The requested key was not saved because it is not valid for this system.
```

- If the PIX Firewall Flash memory activation key is the same as the entered activation key, then the **activation-key** command output reads as follows:

```
The flash activation key has not been modified.
The requested key is the SAME as the flash activation key.
```


ROS N° 03/2005 - CPMI - CORREIOS
Fls N° 535
3702
Doc

The **show activation-key** command output indicates the status of the activation key as follows:

- If the activation key in the PIX Firewall Flash memory is the same as the activation key running on the PIX Firewall, then the **show activation-key** output reads as follows:

```
The flash activation key is the SAME as the running key.
```

- If the activation key in the PIX Firewall Flash memory is the different from the activation key running on the PIX Firewall, then the **show activation-key** output reads as follows:

```
The flash activation key is DIFFERENT from the running key.
The flash activation key takes effect after the next reload.
```

- If the PIX Firewall Flash memory software image version is not the same as the running PIX Firewall software image, then the **show activation-key** output reads as follows:

```
The flash image is DIFFERENT from the running image.
The two images must be the same in order to examine the flash activation key.
```

Usage Notes

1. The PIX Firewall must be rebooted for a new activation key to be enabled.
2. If the PIX Firewall software image is being upgraded to a higher version and the activation key is being updated at the same time, we recommend that you first install the software image upgrade and reboot the PIX Firewall unit, and then update the activation key in the new image and reboot the unit again.
3. If you are downgrading to a lower PIX Firewall software version, we recommend that you ensure that the activation key running on your system is not intended for a higher version before installing the lower version software image. If this is the case, you must first change the activation key to one that is compatible with the the lower version before installing and rebooting. Otherwise, your system may refuse to reload after installation of the new software image.

Examples

The following example shows sample out from the **show activation-key** command:

```
pixfirewalll(config)# show activation-key
Serial Number: 480221353 (0x1c9f98a9)

Running Activation Key: 0x36df4255 0x246dc5fc 0x39d2ec4d 0x09f6288f
Licensed Features:
Failover:           Enabled
VPN-DES:            Enabled
VPN-3DES:           Enabled
Maximum Interfaces: 6
Cut-through Proxy:  Enabled
Guards:             Enabled
URL-filtering:      Enabled
Inside Hosts:       Unlimited
Throughput:         Unlimited
IKE peers:          Unlimited

The flash activation key is the SAME as the running key.
pixfirewall(config)#
```


Fls Nº 536
Doc 3702

alias

Administer overlapping addresses with dual NAT. (Configuration mode.)

Configure with the command...	Remove with the command...
alias [(*if_name*)] *dnat_ip foreign_ip* [*netmask*]	**no alias** [[(*if_name*)] *dnat_ip foreign_ip* [*netmask*]] **clear alias**

Show command options	Show command output
show alias	Displays the **alias** command statements in the configuration.

Syntax Description

dnat_ip	An IP address on the internal network that provides an alternate IP address for the external address that is the same as an address on the internal network.
foreign_ip	IP address on the external network that has the same address as a host on the internal network.
if_name	The internal network interface name in which the *foreign_ip* overlaps.
netmask	Network mask applied to both IP addresses. Use 255.255.255.255 for host masks.

Usage Guidelines

The **alias** command translates one address into another. Use this command to prevent conflicts when you have IP addresses on a network that are the same as those on the Internet or another intranet. You can also use this command to do address translation on a destination address. For example, if a host sends a packet to 209.165.201.1, you can use the **alias** command to redirect traffic to another address, such as, 209.165.201.30.

Note For DNS **fixup** to work properly, **proxy-arp** has to be disabled. If you are using the **alias** command for DNS **fixup**, disable **proxy-arp** with the following command after the **alias** command has been executed:

```
sysopt noproxyarp internal_interface
```

If the **alias** command is used with the **sysopt ipsec pl-compatible** command, a static **route** command statement must be added for each IP address specified in the **alias** command statement. There must be an A (address) record in the DNS zone file for the "dnat" address in the **alias** command.

Use the **no alias** command to disable a previous **set alias** command statement. Use the **show alias** command to display **alias** command statements in the configuration. Use the **clear alias** command to remove all **alias** commands from the configuration. After changing or removing an **alias** command statement, use the **clear xlate** command.

The **alias** command changes the default behavior of the PIX Firewall in three ways:

- When receiving a packet coming in through the interface identified by *if_name*, destined for the address identified by *dnat_ip*, PIX Firewall sends it to the address identified by *foreign_ip*.

CPMI
Fls Nº 537
Doc 3702

- When receiving a DNS A response, containing the address identified by *foreign_ip*, coming from a lower security interface, and destined for the host behind the inteface identified by *if_name*, PIX Firewall changes *foreign_ip* in the reply to *dnat_ip*. This can be turned off by using the command **sysopt nodnsalias inbound**.
- When receiving a DNS A response, containing the address identified by *dnat_ip*, coming from a DNS server behind the interface, *if_name*, and destined for a host behind the lower security interface, PIX Firewall changes *dnat_ip* address to *foreign_ip*. This can be turned off using the command **sysopt nodnsalias outbound**.

The **alias** command is applied on a per-interface basis, while the **sysopt nodnsalias** changes the behaviour for all interfaces. Also, note that addresses in the zone transfers made across the PIX Firewall, are not changed.

You can specify a net alias by using network addresses for the *foreign_ip* and *dnat_ip* IP addresses. For example, the **alias 192.168.201.0 209.165.201.0 255.255.255.224** command creates aliases for each IP address between 209.165.201.1 and 209.165.201.30.

Note ActiveX blocking does not occur when users access an IP address referenced by the **alias** command. ActiveX blocking is set with the **filter activex** command.

Usage Notes

- To access an **alias** *dnat_ip* address with **static** and **access-list** command statements, specify the *dnat_ip* address in the **access-list** command statement as the address from which traffic is permitted from. The following example illustrates this note.

```
alias (inside) 192.168.201.1 209.165.201.1 255.255.255.255
static (inside,outside) 209.165.201.1 192.168.201.1 netmask 255.255.255.255
access-list acl_out permit tcp host 192.168.201.1 host 209.165.201.1 eq ftp-data
access-group acl_out in interface outside
```

  An alias is specified with the inside address 192.168.201.1 mapping to the foreign address 209.165.201.1.

- You can use the **sysopt nodnsalias** command to disable inbound embedded DNS A record fixups according to aliases that apply to the A record address and outbound replies.

Examples

In the following example, the inside network contains the IP address 209.165.201.29, which on the Internet belongs to example.com. When inside clients try to access example.com, the packets do not go to the PIX Firewall because the client assumes 209.165.201.29 is on the local inside network.

To correct this, use the **alias** command as follows:

```
alias (inside) 192.168.201.0 209.165.201.0 255.255.255.224

show alias
alias 192.168.201.0 209.165.201.0 255.255.255.224
```

When the inside network client 209.165.201.2 connects to example.com, the DNS response from an external DNS server to the internal client's query would be altered by the PIX Firewall to be 192.168.201.29. If the PIX Firewall uses 209.165.200.225 through 209.165.200.254 as the global pool IP addresses, the packet goes to the PIX Firewall with SRC=209.165.201.2 and DST=192.168.201.29. The PIX Firewall translates the address to SRC=209.165.200.254 and DST=209.165.201.29 on the outside.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 538
Doc 3702

In the next example, a web server is on the inside at 10.1.1.11 and a **static** command statement was created for it at 209.165.201.11. The source host is on the outside with address 209.165.201.7. A DNS server on the outside has a record for www.example.com as follows:

```
www.example.com. IN A 209.165.201.11
```

The period at the end of the www.example.com. domain name must be included.

The **alias** command follows:

```
alias 10.1.1.11 209.165.201.11 255.255.255.255
```

PIX Firewall doctors the nameserver replies to 10.1.1.11 for inside clients to directly connect to the web server.

The **static** command statement is as follows:

```
static (inside,outside) 209.165.201.11 10.1.1.11
```

The **access-list** command statement you would expect to use follows:

```
access-list acl_grp permit tcp host 209.165.201.7 host 209.165.201.11 eq telnet
```

But with the **alias** command, use this command:

```
access-list acl_grp permit tcp host 209.165.201.11 eq telnet host 209.165.201.7
```

You can test the DNS entry for the host with the following UNIX **nslookup** command:

```
nslookup -type=any www.example.com
```

arp

Change or view the ARP cache, and set the timeout value. (Configuration mode.)

Configure with the command...	Remove with the command...
arp *if_name ip_address mac_address* [**alias**]	**no arp** *if_name ip_address* **clear arp**
arp timeout *seconds*	**no arp timeout**

Show command options	Show command output
show arp [*if_name*] [*ip_address mac_address* **alias**]	Displays the entries in the ARP table.
show arp timeout	Displays the current timeout value.

Syntax Description

alias	Make this entry permanent. Alias entries do not time out and are automatically stored in the configuration when you use the **write** command to store the configuration.
if_name	The internal or external interface name specified by the **nameif** command.
ip_address	Host IP address for the ARP table entry.
mac_address	Hardware MAC address for the ARP table entry; for example, 00e0.1e4e.3d8b.
seconds	Duration that an ARP entry can exist in the ARP table before being cleared.

ROS nº 03/2005 - CPMI - CORREIOS
Fls. Nº 539
3702
Doc

16.177
L

Usage Guidelines

The **arp** command adds an entry to the PIX Firewall ARP cache. ARP is a low-level TCP/IP protocol that resolves a node's physical address from its IP address through an ARP request asking the node with a particular IP address to send back its physical address. The presence of entries in the ARP cache indicates that the PIX Firewall has network connectivity. The **clear arp** command clears the ARP table but not the **alias** (permanent) entries. Use the **no arp** command to remove these entries. The **show arp** command lists the entries in the ARP table.

Note You can use the **sysopt noproxyarp** command to disable proxy-arps on an interface.

Use the **arp** command to add an entry for new hosts you add on your network or when you swap an existing host for another. Alternatively, you can wait for the duration specified with the **arp timeout** command to expire and the ARP table rebuilds itself automatically with the new host information.

The **no arp timeout** command sets the timer to its default value. The **show arp timeout** command displays the current timeout value.

Defaults

The **arp timeout** command sets the duration that an ARP entry can stay in the PIX Firewall ARP table before expiring. The timer is known as the ARP persistence timer. The default value is 14,400 seconds (4 hours).

Examples

The following examples illustrate use of the **arp** and **arp timeout** commands:

```
arp inside 192.168.0.42 00e0.1e4e.2a7c
arp outside 192.168.0.43 00e0.1e4e.3d8b alias
show arp
    outside 192.168.0.43 00e0.1e4e.3d8b alias
    inside 192.168.0.42 00e0.1e4e.2a7c

clear arp inside 192.168.0.42

arp timeout 42
show arp timeout
arp timeout 42 seconds

no arp timeout
show arp timeout
arp timeout 14400 seconds
```

auth-prompt

Change the AAA challenge text for through the firewall user sessions. (Configuration mode.)

Configure with the command...	Remove with the command...
auth-prompt [**accept** | **reject** | **prompt**] *string*	**no auth-prompt** [**accept** | **reject** | **prompt**] *string* **clear auth-prompt**

CPM CORP 540

№ Doc 3702

Show command options	Show command output
show auth-prompt	Displays the AAA challenge text.

Syntax Description

accept	If a user authentication via Telnet is accepted, display the prompt *string*.
prompt	The AAA challenge prompt string follows this keyword. This keyword is optional for backward compatibility.
reject	If a user authentication via Telnet is rejected, display the prompt *string*.
string	A string of up to 235 alphanumeric characters or 31 words, limited by whichever maximum is first reached. Special characters should not be used; however, spaces and punctuation characters are permitted. Entering a question mark or pressing the **Enter** key ends the string. (The question mark appears in the string.)

Usage Guidelines

The **auth-prompt** command lets you change the AAA challenge text for HTTP, FTP, and Telnet access through the firewall requiring user authentication from TACACS or RADIUS servers. This text is primarily for cosmetic purposes and displays above the username and password prompts that users view when logging in. If the user authentication occurs from Telnet, you can use the **accept** and **reject** options to display different status prompts to indicate that the authentication attempt is accepted or rejected by the AAA server.

Following is the authentication sequence showing when each **auth-prompt** string is displayed:

1. A user initiates a telnet session from the **inside** interface through the firewall to the **outside** interface.
2. The user receives the **auth-prompt** challenge text, followed by the **username** prompt.
3. The user enters the AAA username/password username and password, or in the formats **aaa_user@outside_user** and **aaa_pass@outside_pass**.
4. The firewall sends the **aaa_user/aaa_pass** to the TACACS or RADIUS AAA server.
5. If the AAA server authenticates the user, the firewall displays the **auth-prompt accept** text to the user, otherwise the **reject** challenge text is displayed. Authentication of http and ftp sessions displays only the challenge text at the prompt. The **accept** and **reject** text are not displayed.

If you do not use this command, FTP users view `FTP authentication`, HTTP users view `HTTP Authentication`, and challenge text does not appear for Telnet access.

Note Microsoft Internet Explorer only displays up to 37 characters in an authentication prompt. Netscape Navigator displays up to 120 characters, and Telnet and FTP display up to 235 characters in an authentication prompt.

Examples

The following example shows how to set the authentication prompt and how users view the prompt:

```
auth-prompt XYZ Company Firewall Access
```

After this string is added to the configuration, users view the following:

```
Example.com Company Firewall Access
User Name:
Password:
```


ROS nº 03/2005
CPMI - CORREIOS
Fls. Nº 541
3702
Doc

The **prompt** keyword can be included or omitted.

For example:

```
auth-prompt prompt Hello There!
```

This command statement is the same as the following:

```
auth-prompt Hello There!
```

auto-update

Specifies how often to poll an Auto Update Server. (Configuration mode.)

Configure with the command...	Remove with the command...
auto-update device-id hardware-serial | hostname | ipaddress [*if_name*] | **mac-address** [*if_name*] | **string** *text*	**no auto-update device-id hardware-serial | hostname | ipaddress** [*if_name*] | **mac-address** [*if_name*] | **string** *text*
auto-update poll-period *poll_period* [*retry_count* [*retry_period*]]	**no auto-update** *poll_period* **poll-period** [*retry_count* [*retry_period*]] **clear auto-update**
auto-update server *url* [*verify_certificate*]	**no auto-update server** *url* [*verify_certificate*] **clear auto-update**
auto-update timeout *period*	**no auto-update timeout** *period* **clear auto-update**

Show command options	Show command output
show auto-update	Displays the Auto Update Server, poll time, and timeout period.

Syntax Description

device-id	The device ID of the PIX Firewall.
hardware-serial	Specifies to use the hardware serial number of the PIX Firewall to uniquely identify the firewall.
hostname	Specifies to use the host name of the PIX Firewall to uniquely identify the firewall.
if_name	Specifies the interface to use (with its corresponding IP or MAC address) to uniquely identify the PIX Firewall.
ipaddress	Specifies to use the IP address of the specified PIX Firewall interface to uniquely identify the firewall.
mac-address	Specifies to use the MAC address of the specified PIX Firewall interface to uniquely identify the firewall.
period	Specifies how long to attempt to contact the Auto Update Server, after the last successful contact, before stopping all traffic passing through the PIX Firewall.

poll_period	Specifies how often, in minutes, to poll an Auto Update Server. The default is 720 minutes (12 hours).
retry_count	Specifies how many times to try reconnecting to the Auto Update Server if the first attempt fails. The default is 0.
retry_period	Specifies how long to wait, in minutes, between connection attempts. The default is 5 minutes and the valid range of values is from 1 to 35791.
text	Specifies the text string to uniquely identify the PIX Firewall to the Auto Update Server.
url	Specifies the location of the Auto Update Server using the following syntax: **http**[**s**]:[[*user:password@*] *location* [:*port*]] / *pathname* See the **copy** command for variable descriptions.
verify_certificate	Specifies to verify the certificate returned by the Auto Update Server.

Usage Guidelines

The **clear auto-update** command removes the entire auto-update configuration.

The **auto-update poll-period** command specifies how often to poll the Auto Update Server for configuration or software image updates. The **no auto-update poll-period** command resets the poll period to the default.

The **auto-update server** command specifies the URL of the Auto Update Server. Only one server can be configured. The **no auto-update server** command disables polling for auto-update updates (by terminating the auto-update daemon).

The **auto-update timeout** command is used to stop all new connections to the PIX Firewall if the Auto Update Server has not been contacted for *period* minutes. This can be used to ensure that the PIX Firewall has the most recent image and configuration.

Examples

The **show auto-update** command displays the Auto Update Server, poll time, and timeout period. The following is sample output from the command:

```
Server: https:pix:********@172.23.58.115:1742/management.cgi?1276 (verify)
Poll period: 720, retry count: 2, retry period: 5
Timeout: none
```

Commands

There are no commands that start with the letter B in PIX Firewall software version 6.2.

ROS nº 03/2005
CPMI - CORR
Fls Nº 543
Doc 3702

Doc.
000233

CPL/AC

PREGÃO
050/2003

LOCAÇÃO DE EQUIPAMENTOS DE INFORMÁTICA INCLUINDO ASSISTÊNCIA TÉCNICA E TREINAMENTO

COBRA TECNOLOGIA – PROPOSTA ECONÔMICA

2003
PASTA 28

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 544
Nº 3702
Doc

COBRA TECNOLOGIA
Integradora de Soluções em TI e Serviços

17.224

ANEXO 3

(MODELO IV)

PROPOSTA ECONÔMICA

PREGÃO N°050/2003 – CPL/AC

1. **Razão Social da Empresa: COBRA TECNOLOGIA S/A .**
2. **CNPJ:** 42.318.949/0001-84
3. **Inscrição Estadual:** 82.131.515
4. **Inscrição Municipal:** 00.554.855
5. **Endereço Completo:** Estrada dos Bandeirantes, 7966, Jacarepaguá, Rio de Janeiro, RJ, CEP:22.783-110
6. **Telefone:** 21-2442-8800 **Fax:** 21-2441-2066 Home-Page: www.cobra.com.br
7. **Validade da Proposta:** 60 (sessenta) dias
8. **Prazo de Pagamento:** Conforme Edital
9. **Banco:** Banco do Brasil **Agência:** 0493-6 **C/Corrente:** 5826-2
10. **Representante da Empresa:** Eduardo Galdeano François
11. **Cargo:** Diretor Comercial **RG:** 2.813.754 IFP **CPF:** 511.410.517-53

Apresentamos nossa Proposta para locação de equipamentos de informática – novos de fábrica –incluindo instalação, configuração, treinamento e operação assistida do pessoal encarregado, assistência técnica, garantia e instalação dos PRODUTOS locados, do objeto do Pregão nº 050/2003, acatando todas as estipulações consignadas no Edital, conforme abaixo:

1. ASPECTOS FINANCEIROS

1.1. O **VALOR MENSAL DA LOCAÇÃO** para cada produto constante das condições específicas da contratação – **ANEXOS 1, 1-A e 1-B** – para o período de **48 (quarenta e oito) meses**, conforme tabela abaixo:

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 545
Doc 3702

COBRA TECNOLOGIA
Integradora de Soluções em TI e Serviços

17.223
L

PREÇO UNITÁRIO MENSAL DA LOCAÇÃO DOS PRODUTOS

TIPO DE PRODUTO	PREÇO UNITÁRIO DE LOCAÇÃO (R$)	DISTRIBUIÇÃO		TOTAL
		CCD AC (DF)	CD SPM (SP)	
SERVIDOR INTEL TIPO 01	37.719,62	14	7	21 792.112,02
SERVIDOR INTEL TIPO 02	9.403,94	29	6	35 329.137,90
SERVIDOR INTEL TIPO 03	3.800,71	27	24	51 193.836,21
SERVIDOR RISC TIPO 01	136.006,10	8	3	11 1.496.067,10
SWITCH TIPO 01	130.189,25	2	2	4 520.757,00
SWITCH TIPO 02	3.517,50	4	2	6 21.105,00
SWITCH TIPO 03	45.107,38	4	2	6 270.644,28
SWITCH TIPO 04	49.726,75	8	4	12 596.721,00
SWITCH TIPO 05	4.387,50	1	1	2 8.775,00
ROTEADOR TIPO 01	22.684,50	1	1	2 45.369,00
ROTEADOR TIPO 02	4.768,00	2	0	2 9.536,00
UNIDADE DE BACKUP ROBOTIZADO	96.057,50	1	1	2 192.115,00
SERVIDOR DE SEGURANÇA LÓGICA TIPO 01	28.485,25	2	2	4 113.941,00
SERVIDOR DE SEGURANÇA LÓGICA TIPO 02	14.600,50	1	1	2 29.201,00
SERVIDOR PARA DETECÇÃO DE INTRUSÃO	15.664,00	1	1	2 31.329,00
TOTAL		105	57	162

1.1.1. Nestes valores deverão estar inclusos: a instalação dos **PRODUTOS**, a assistência técnica, o treinamento, as despesas decorrentes dos deslocamentos de técnicos para atendimento dos chamados, frete, seguros (contra incêndio, roubo, danos elétricos ou provenientes de fenômenos da natureza), impostos/taxas e demais despesas com peças e acessórios, bem como todas as despesas decorrentes do cumprimento integral do objeto do Edital. 4.650 645,51

1.2. O VALOR TOTAL DA LOCAÇÃO será o resultado do **VALOR MENSAL DA LOCAÇÃO** multiplicado por **48 (quarenta e oito)**, que representa o número de meses de locação.

1.3. A apresentação do Cronograma de Trabalho (ANEXO 1-A, item 1.2.) estipulado em 1% (um por cento) do **VALOR TOTAL DA LOCAÇÃO, subitem 1.2.** desta proposta.

1.4. O VALOR GLOBAL DA PROPOSTA será o resultado do somatório dos itens: **VALOR TOTAL DA LOCAÇÃO (1.2.) e do Cronograma de Trabalho (1.3.)**

Discriminação dos Valores:

VALOR TOTAL DA LOCAÇÃO (somatório dos 48 meses de aluguel)	**R$220.998.669,41**	R$223.230.984,40
APRESENTAÇÃO DO CRONOGRAMA DE TRABALHO (1% do Valor Total da Locacao)	**R$2.232.309,79**	R$2.232.309,80
VALOR GLOBAL DA PROPOSTA (VALOR TOTAL DA LOCAÇÃO + Cronograma de Trabalho)	**R$223.230.979,20**	R$225.463.294,20

Duzentos e vinte e três milhões, duzentos e trinta mil, novecentos e setenta e nove reais e vinte centavos.

COBRA Tecnologia S.A.
Estrada dos Bandeirantes 7965
CEP 22783-110 Rio de Janeiro RJ
Tel 21 442 8800
www.cobra.com.br

RQS nº 03/2005 - CN - CPMI - CORREIOS
546
2/4
Doc. 3702

17.222

18 → 223.230.984,40

1% — 2.232.309,84

TOTAL = 225.463.294,20

ROS nº 03/2006 - CPMI - CORREIOS
Fls. Nº 547
Doc 3702

17.221
L

1.5. A **LICITANTE** deverá apresentar planilha detalhada de custo de formação do preço mensal da locação, em atendimento a exigência constante no subitem 5.8. do edital conforme modelo abaixo:

ITEM (especificar o percentual de cada um)	PERCENTUAL
1. EQUIPAMENTOS:	
Subtotal	25,95%
2. SOFTWARE	
Subtotal	29,12%
3. TREINAMENTOS	
Subtotal	6,72%
4. ASSISTÊNCIA TÉCNICA/GARANTIA	
Subtotal	13,44%
5. INSTALAÇÃO	
Subtotal	2,24%
6. TRIBUTOS	
Subtotal	9,86%
7. TRANSPORTE/FRETE/SEGURO	
Subtotal	0,13%
8. DESPESAS ADMINISTRATIVAS	
Subtotal	1,34%
9. LUCRO	
Subtotal	2,24%
10. OUTROS	
Subtotal	8,96%
TOTAL	**100,00%**

2. DECLARAÇÕES QUE DEVERÃO ACOMPANHAR A PROPOSTA ECONÔMICA:

2.1. Declaração de que dispõe ou disporá, no prazo máximo de **20 (vinte) dias** da assinatura do contrato, de central de atendimento telefônico com discagem gratuita e/ou via internet, para processo de recepção, qualificação, controle e solução dos chamados de manutenção corretiva, conforme modelo no **ANEXO 3 (MODELO VII)**.

2.2. Declaração do fabricante, em papel timbrado e com firma (s) reconhecida (s), mencionando o número e o objeto deste Edital, assegurando que os equipamentos cotados (citar marca e modelo) são de linha de produção continuada e que se compromete a fornecer peças de reposição pelo período mínimo de 60 (sessenta) meses.

2.3. Certificado de distribuidor ou revenda autorizada, em papel timbrado do emissor e com firma (s) reconhecida (s), caso o proponente não seja fabricante dos equipamentos, conforme abaixo:

a) certificado de distribuidor autorizado e sediado no Brasil, emitido pelo fabricante dos equipamentos;

b) certificado de revenda autorizada, emitido pelo fabricante ou distribuidor dos equipamentos, devendo também, para este último, ser apresentado certificado conforme alínea anterior.

2.4. Carta de solidariedade emitida pelo fabricante, em papel timbrado e com firma reconhecida, caso por oponente não seja o fabricante dos equipamentos, especificados no **ANEXO 1-B** (Servidores, Switches, Roteadores e Unidade de Backup Robotizado), mencionando o número e o objeto deste edital, atestando:

Fls. Nº 548
3/4
Nº 3792
Doc

17.220
L

a) sua solidariedade para com o licitante no âmbito dos produtos de sua fabricação quanto aos compromissos que o licitante venha a assumir perante a ECT, no escopo desta licitação;

b) que o proponente está apto a prestar assistência técnica, com o uso de peças e componentes originais, bem como suporte aos produtos cotados;

c) sua responsabilidade solidária para com o proponente pelo perfeito cumprimento das exigências de garantia dos produtos, durante todo o prazo de vigência do contrato.

2.5. Declaração de responsabilidade nos componentes de terceiros, utilizados na solução da proponente, conforme modelo no **ANEXO 3** (**MODELO VII**).

2.6. Certificado PMP (Project Management Professional) emitido em favor do gestor do projeto alocado pelo PMI (Project Management Institute), conforme letra "k", do subitem 1.1, do Anexo 1-A.

2.7. Atestados de Vistoria conforme **MODELO VI** constante do **ANEXO 3** deste Edital, nas instalações dos Centros Corporativos de Dados localizados em Brasília-DF e São Paulo-SP.

Garantia do objeto: 48 (quarenta e oito) meses (período de locação)

Declaramos disponibilizar os **PRODUTOS** no prazo de **60 (sessenta)** dias após o término da vigência do Contrato, conforme descrito no **subitem 2.18. da cláusula segunda do ANEXO 2** do Edital.

Declaramos, ainda, que tomamos conhecimento de todas as informações e condições para o cumprimento das obrigações objeto desta licitação e que atendemos todas as condições do Edital.

Rio de Janeiro, 24 de julho de 2003.

COBRA TECNOLOGIA S.A.
CNPJ 42.318.949/0001-84

Eduardo Galdeano François

EDUARDO GALDEANO FRANÇOIS

ROS nº 03/2003 - CN
CPMI - CORREIOS
Fls. Nº 549
Doc. 3702

COBRA TECNOLOGIA
Integradora de Soluções em TI e Serviços

17.219
2

ANEXO 3

(MODELO VII)

DECLARAÇÃO DE RESPONSABILIDADE DOS COMPONENTES DE TERCEIROS E DISPONIBILIDADE DE CENTRAL DE ATENDIMENTO

À EMPRESA BRASILEIRA DE CORREIOS E TELÉGRAFOS – ECT
SBN – Quadra 01, Bloco "A" – Sobreloja – Ed. Sede ECT
Fax: (61) 426-2759

Ref.: Pregão n.º 050/2003 - CPL/AC

Empresa **COBRA TECNOLOGIA S.A**, inscrita no CNPJ nº **42.318.949/0001-84**, por intermédio de seu representante legal o Sr. **Eduardo Galdeano François**, portador(a) da Carteira de Identidade nº 2.813.754 do IFP e do CPF nº 511.410.517-53, declara que o fornecimento de equipamentos/ softwares ou prestação de serviços por terceiros, constantes da nossa proposta, não diminui, em hipótese alguma, a nossa total responsabilidade pelo perfeito e completo funcionamento do objeto do Edital do Pregão n.º 050/2003- CPL/AC. Declaramos, ainda, de que dispomos (vamos dispor, no prazo máximo de **20 (vinte) dias** da assinatura do contrato), de central de atendimento telefônico com discagem gratuita e/ou via internet, para processo de recepção, qualificação, controle e solução dos chamados de manutenção corretiva.

Atenciosamente,

22 de Julho de 2003.

COBRA TECNOLOGIA S.A
42.318.949/0001-84

Eduardo Galdeano François

EDUARDO GALDEANO FRANÇOIS

RCE/ECT CPMI - CORREIOS
Fls. Nº 550
Doc 3702

17.218
L

BLACK BOX®
NETWORK SERVICES

DECLARAÇÃO

São Paulo, 17 de Julho de 2.003

Á
EMPRESA BRASILEIRA DE CORREIOS E TELÉGRAFOS - ECT
Administração Central
SBN – Quadra 01, Bloco "A" – Sobreloja – Ed. Sede ECT
Brasília – D.F.

Ref.: EDITAL DO PREGÃO N.º 050/2003 – CPL/AC

Prezados Senhores,

Declaramos para fins de comprovação junto ao Edital em epigrafe que os equipamentos cotados abaixo pela Cobra Computadores e Sistemas Brasileiro S/A, inscrita no CNPJ sob o nº 42.318.949/0001-84, sediada na Estrada dos Bandeirantes, 7966 – Jacarepaguá – Rio de Janeiro – RJ, são de linha de produção continuada e que nos comprometemos a fornecer peças de reposição pelo período mínimo de 60 (sessenta) meses.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 551
Doc 3702

17.217
L

Os equipamentos cotados são:

✓ **KV138A**	**CHASSIS AFFINITY ARQUITETURA 8 USUARIOS**
✓ **KV1301C-R2**	**AFFINITY USER/CPU C 1 X 4 CARD**
✓ **KV1300C**	**SERVSWITCH AFFINITY - PLACA 0 USER X 4 CPUS**
✓ **KV1306C**	**SERVSWITCH AFFINITY HI-DENSITY EXPANS**
✓ **RMK19A-BB**	**SERVSWITCH AFFINITY KIT PARA RACK 19"**
✓ **KV180035**	**SERVSWITCH AFFINITY HI-DENS EXP CABLE**
✓ **EHN515-0035**	**CABO SERVSWITCH CPU SUN/HD15 COM 10,6M**
✓ **EHN382-0035**	**CABO SERVSWITCH CPU COAX PC COM 10,6M**
✓ **EHN382-0100**	**CABO SERVSWITCH CONSOLE COAX PC/PS2 COM 30,0M**
✓ **EHN383-0100**	**CABO SERVSWITCH CONSOLE COAX PC/PS2 COM 30,0M**
✓ **EHN225-0100**	**CABO SERVSWITCH CONSOLE SUN/HD15 COM 30,0M**
✓ **KV134A-R2**	**SERVSWITCH AFFINITY - 4 CONSOLES X 16 CPUïS**
✓ **KV131A-R2**	**SERVSWITCH AFFINITY W/EXPANSION MODUL**
✓ **KV1305C**	**SERVSWITCH AFFINITY - PLACA DE EMPILHAMENTO**
✓ **KV140050**	**CABO DE EMPILHAMENTO PARA SERVSWITCH 15,2M**

Atenciosamente

5º Tabelionato de Notas FRIANÇA

São Paulo, 17 de julho de 2003

Wilson D. Batistela
Gerente Geral
Black Box do Brasil Ltda.

5º Tabelionato de Notas - Jose Roberto Fagnoni Franco - Tabeliao
Av. Joao Dias, 2224-Santo Amaro - Fone/Fax 5181-0472 - CEP 04753-050
Reconheco por semelhanca a(s) firma(s) de:
(01)-WILSON BONIZETE BATISTELA
VALIDO SOMENTE COM SELO DE AUTENTICIDADE - Dou fe em virtude de ser verdade.
Carimbo:135996 Sao Paulo, 17 de julho de 2003.
Total...R$ 4,20 Em testemunho
Simone Bifulco
Escrevente

5º TABELIONATO DE NOTAS - SÃO PAULO - SP
AA046526

552

3802

17210

BLACK BOX®
NETWORK SERVICES

DECLARAÇÃO

São Paulo, 17 de julho de 2.003

Á
EMPRESA BRASILEIRA DE CORREIOS E TELÉGRAFOS - ECT
SBN – Quadra 01, Bloco "A" – Sobreloja – Ed. Sede ECT
Brasília – D.F.

Ref.: EDITAL DO PREGÃO N.º 050/2003 – CPL/AC

Prezados Senhores,

Declaramos para fins de comprovação junto ao edital em epigrafe que a Cobra Computadores e Sistemas Brasileiro S/A, inscrita no CNPJ sob o n.º 42.318.949/000184, sediada na Estrada dos Bandeirantes, 7966 – Jacarepaguá – Rio de Janeiro – RJ, está autorizada a comercializar, instalar, prestar serviços de manutenção nos produtos abaixo descritos

✓ **KV138A**	**CHASSIS AFFINITY ARQUITETURA 8 USUARIOS**
✓ **KV1301C-R2**	**AFFINITY USER/CPU C 1 X 4 CARD**
✓ **KV1300C**	**SERVSWITCH AFFINITY - PLACA 0 USER X 4 CPUS**
✓ **KV1306C**	**SERVSWITCH AFFINITY HI-DENSITY EXPANS**
✓ **RMK19A-BB**	**SERVSWITCH AFFINITY KIT PARA RACK 19"**
✓ **KV180035**	**SERVSWITCH AFFINITY HI-DENS EXP CABLE**
✓ **EHN515-0035**	**CABO SERVSWITCH CPU SUN/HD15 COM 10,6M**
✓ **EHN382-0035**	**CABO SERVSWITCH CPU COAX PC COM 10,6M**
✓ **EHN382-0100**	**CABO SERVSWITCH CONSOLE COAX PC/PS2 COM 30,0M**
✓ **EHN383-0100**	**CABO SERVSWITCH CONSOLE COAX PC/PS2 COM 30,0M**

Fls. nº 553
Nº 3702

17.215
L

✓	**EHN225-0100**	**CABO SERVSWITCH CONSOLE SUN/HD15 COM 30,0M**
✓	**KV134A-R2**	**SERVSWITCH AFFINITY - 4 CONSOLES X 16 CPUïS**
✓	**KV131A-R2**	**SERVSWITCH AFFINITY W/EXPANSION MODUL**
✓	**KV1305C**	**SERVSWITCH AFFINITY - PLACA DE EMPILHAMENTO**
✓	**KV140050**	**CABO DE EMPILHAMENTO PARA SERVSWITCH 15,2M**

Atenciosamente

São Paulo, 17 de julho de 2003

Wilson D. Batistela
Gerente Geral
Black Box do Brasil Ltda.

5º Tabelionato de Notas FRANÇA

5º Tabelionato de Notas - Jose Roberto [illegible] - Tabelião
Av. João Dias, [illegible]-Santo Amaro - Fone: [illegible] No. [illegible]
Reconheco por semelhança [illegible] firma(s) de:
001-WILSON DONIZETE BATISTELA
VALIDO SOMENTE COM SELO DE AUTENTICIDADE - DOU FÉ. [illegible]
Tarimbo:139999 | 18 DE JUNHO DE 2003.
Total...:XXXXXX,07 | Em testemunho [illegible] verdade.
Conf...:FJNR: | TABELIÃO CARLOS BASTOS - ESCREVENTE

Simone Bifulco
Escrevente
AA045

Cartório Notarial do Brasil SP

554

3702

17.214

BLACK BOX®
NETWORK SERVICES

Black Box do Brasil
Av. Guido Caloi, 1935 – Bl. B Térreo
CNPJ 00.017.332/0001-89

Carta de Solidariedade

Ref: Edital do Pregão ECT No. 050/2003

Vimos, por meio desta, apresentar nossa solidariedade com a Cobra Computadores e Sistemas Brasileiro S/A. CNPJ: 42.318.949/0001-84, localizada na Estrada dos Bandeirantes, 7966, CEP 22783-110, Cidade do Rio de Janeiro, Estado do Rio de Janeiro, Brasil, no Edital supracitado, que estamos solidários a esta, garantindo o fornecimento dos seguintes produtos:

✓ **KV138A**	**CHASSIS AFFINITY ARQUITETURA 8 USUARIOS**
✓ **KV1301C-R2**	**AFFINITY USER/CPU C 1 X 4 CARD**
✓ **KV1300C**	**SERVSWITCH AFFINITY - PLACA 0 USER X 4 CPUS**
✓ **KV1306C**	**SERVSWITCH AFFINITY HI-DENSITY EXPANS**
✓ **RMK19A-BB**	**SERVSWITCH AFFINITY KIT PARA RACK 19"**
✓ **KV180035**	**SERVSWITCH AFFINITY HI-DENS EXP CABLE**
✓ **EHN515-0050**	**CABO SERVSWITCH CPU SUN/HD15 COM 15,2 M**
✓ **EHN382-0050**	**CABO SERVSWITCH CPU COAX PC COM 15,2 M**
✓ **EHN382-0100**	**CABO SERVSWITCH CONSOLE COAX PC/PS2 COM 30,0M**
✓ **EHN383-0100**	**CABO SERVSWITCH CONSOLE COAX PC/PS2 COM 30,0M**
✓ **EHN225-0100**	**CABO SERVSWITCH CONSOLE SUN/HD15 COM 30,0M**
✓ **KV134A-R2**	**SERVSWITCH AFFINITY - 4 CONSOLES X 16 CPUïS**

Doc 555

Nº 3702

17-213

✓	**KV131A-R2**	**SERVSWITCH AFFINITY W/EXPANSION MODUL**
✓	**KV1305C**	**SERVSWITCH AFFINITY - PLACA DE EMPILHAMENTO**
✓	**KV140050**	**CABO DE EMPILHAMENTO PARA SERVSWITCH 15,2M**

Asseguramos ainda que tais equipamentos cotados são de linha de produção continuada e nos comprometemos a fornecer peças de reposição pelo período mínimo de 60 (sessenta) meses.

Adicionalmente atestamos:

a) nossa solidariedade com a Cobra Computadores e Sistemas Brasileiro no âmbito dos produtos acima listados, quanto aos compromissos por ela assumidos na licitação supra-citada;
b) Que a Cobra Computadores e Sistemas Brasileiro está apta a prestar assistência técnica, com o uso de peças e componentes originais, bem como suporte aos produtos cotados.
c) Nossa responsabilidade solidária com a Cobra Computadores e Sistemas Brasileiro pelo perfeito cumprimento das exigências de garantia dos produtos, durante o todo o prazo de vigência do Contrato.

São Paulo, 23 de Julho de 2003.

Carlos Cezar Fagan.
Gerente Comercial
Black Box do Brasil

5o.Tabelionato de Notas - Jose Roberto Pacheco Franca - Tabeliao
Av. Joao Dias, 2320-Santo Amaro - Fone:5041607?2 No.011161?5/5885
Reconheco por semelhanca ********000******** (firma) de:
001-CARLOS CEZAR FAGAN
VALIDO SOMENTE COM SELO DE AUTENTICIDADE - Doc. sem valor econo.
Carimbo:139252 | 23 DE JULHO DE 2003
Total..:******2,07 | Em testemunho _____ da verdade.
Conf...:FIRMA | SIMONE BIFULCO - ESCREVENTE

Colegio Notarial do Brasil - SP
FIRMA
1036AA038902

5º TABELIONATO DE NOTAS
FRANÇA
www.quintotabelionatofranca.com.br
SÃO PAULO - SP

556

702

17.212

declaração

Hewlett Packard Computadores Ltda.
Rua Hum, Nº 1000 - Centro Industrial
13820-000 - Campinas - SP
CNPJ: 00.379.771/0001-31
Fone: (11) 4197 8000
Fax: (11) 4197 8432
www.hp.com.br

670394-BR

Barueri, 22 de julho de 2003.

A
EMPRESA BRASILEIRA DE CORREIOS E TELEGRAFOS
BRASILIA/DF

Ref.: PREGÃO Nº050/2003 – CPL/AC

Objeto.: Locação e instalação de 162(cento e sessenta e dois) equipamentos de informática – novos de fábrica – incluindo: a configuração, o treinamento, a assistência técnica e a garantia, destinados aos Centros Corporativos de Dados da ECT, localizados nas cidades de Brasília e São Paulo, conforme condições gerais e pauta de distribuição e especificações constantes dos ANEXOS 1-a e 1-B deste EDITAL.

DECLARAÇÃO DE SOLIDARIEDADE

Declaramos, na qualidade de fabricante, que a COBRA TECNOLOGIA S/A, CNPJ nº 42.318.949/0001-84, é nosso revendedor autorizado e está apto a comercializar os equipamentos ofertados por nós produzidos.

Declaramos ainda :

a) nossa solidariedade para com a COBRA TECNOLOGIA S/A quanto aos compromissos que esta venha a assumir perante a EMPRESA BRASILEIRA DE CORREIOS E TELEGRAFOS;
b) que a COBRA TECNOLOGIA S/A está apta a prestar assistência técnica, com uso de peças e componentes originais, bem como suporte aos produtos e equipamentos cotados;
c) que somos responsáveis solidários com a COBRA TECNOLOGIA S/A, pelo perfeito cumprimento das exigências de garantia dos equipamentos, durante todo o seu prazo de vigência do contrato.

CARTÓRIO DE ALDEIA

Atenciosamente,

Jose Roberto Giani Garcia
Hewlett-Packard Computadores Ltda
CNPJ 00.379.771/0001-31

Fls. 557
Nº 3702
Doc.

17211

Hewlett Packard Company
Palo Alto - California - EUA
www.hp.com

22/07/2003

A
EMPRESA BRASILEIRA DE CORREIOS E TELEGRAFOS
BRASILIA/DF

Ref.: PREGÃO Nº050/2003 - CPL/AC

Objeto.: Locação e instalação de 162(cento e sessenta e dois) equipamentos de informática - novos de fábrica - incluindo: a configuração, o treinamento, a assistência técnica e a garantia, destinados aos Centros Corporativos de Dados da ECT, localizados nas cidades de Brasília e São Paulo, conforme condições gerais e pauta de distribuição e especificações constantes dos ANEXOS 1-a e 1-B deste EDITAL.

DECLARAÇÃO DE SOLIDARIEDADE

Declaramos, na qualidade de fabricante, que a COBRA TECNOLOGIA S/A, CNPJ nº 42.318.949/0001-84, é nosso revendedor autorizado e está apto a comercializar os equipamentos por nós produzidos, descritos abaixo:

Declaramos ainda :

a) nossa solidariedade para com a COBRA TECNOLOGIA S/A quanto aos compromissos que esta venha a assumir perante a EMPRESA BRASILEIRA DE CORREIOS E TELEGRAFOS;
b) que a COBRA TECNOLOGIA S/A está apta a prestar assistência técnica, com uso de peças e componentes originais, bem como suporte aos produtos e equipamentos cotados;
c) que somos responsáveis solidários com a COBRA TECNOLOGIA S/A, pelo perfeito cumprimento das exigências de garantia dos equipamentos, durante todo o seu prazo de vigência do contrato.

Hewlett-Packard Company
Carlos Rocha Ribeiro da Silva
Procurador

Fls. Nº 558
Nº 3702

declaração

Hewlett Packard Computadores Ltda.
Rua Hum, Nº 1000 - Centro Industrial
13820-000 - Campinas - SP
CNPJ: 00.379.771/0001-31
Fone: (11) 4197 8000
Fax: (11) 4197 8432
www.hp.com.br

17.210

670394-BR

Barueri, 22 de julho de 2003.

A
EMPRESA BRASILEIRA DE CORREIOS E TELEGRAFOS
BRASILIA/DF

Ref.: PREGÃO Nº050/2003 - CPL/AC

Objeto.: Locação e instalação de 162(cento e sessenta e dois) equipamentos de informática - novos de fábrica - incluindo: a configuração, o treinamento, a assistência técnica e a garantia, destinados aos Centros Corporativos de Dados da ECT, localizados nas cidades de Brasília e São Paulo, conforme condições gerais e pauta de distribuição e especificações constantes dos ANEXOS 1-a e 1-B deste EDITAL.

HEWLETT-PACKARD COMPUTADORES LTDA, inscrita no CNPJ/MF sob número 00.379.771/0001-31, certifica que tem como revenda autorizada a Empresa COBRA TECNOLOGIA S/A, sediada na Estrada dos Bandeirantes, 7966 - Jacarepaguá - Rio de Janeiro/RJ, inscrita no CNPJ/MF sob número 42.318.949/0001-84, perante o cliente Correios, referente ao Edital do Pregão No 050/2003.

Atenciosamente,

Jose Roberto Giani Garcia
Hewlett-Packard Computadores Ltda
CNPJ 00.379.771/0001-31

559
Nº 3702

declaração

E C T
17.209
CPL-AC

Hewlett Packard Computadores Ltda.
Rua Hum, N° 1000 - Centro Industrial
13820-000 - Campinas - SP
CNPJ: 00.379.771/0001-31
Fone: (11) 4197 8000
Fax: (11) 4197 8432
www.hp.com.br

670394-BR

Barueri, 22 de julho de 2003.

A
EMPRESA BRASILEIRA DE CORREIOS E TELEGRAFOS
BRASILIA/DF

Ref.: PREGÃO Nº050/2003 – CPL/AC

Objeto.: Locação e instalação de 162(cento e sessenta e dois) equipamentos de informática – novos de fábrica – incluindo: a configuração, o treinamento, a assistência técnica e a garantia, destinados aos Centros Corporativos de Dados da ECT, localizados nas cidades de Brasília e São Paulo, conforme condições gerais e pauta de distribuição e especificações constantes dos ANEXOS 1-a e 1-B deste EDITAL.

Hewlett-Packard Computadores Ltda, CNPJ 00.379.771/0001-31, declara que, para o atendimento ao Pregão em epígrafe, os produtos cotados, conforme relação abaixo mencionada, são de nossa linha de produção continuada e terão o fornecimento garantido de peças de reposição pelo período mínimo de 60 (sessenta) meses.

Marca	**Modelo**
HP -	**Proliant DL760, DL580, DL380, ML350, Racks**

Atenciosamente,

Jose Roberto Giani Garcia
Hewlett-Packard Computadores Ltda
CNPJ 00.379.771/0001-31

560
Nº 3702

declaração

Hewlett Packard Computadores Ltda.
Rua Hum, Nº 1000 - Centro Industrial
13820-000 - Campinas - SP
CNPJ: 00.379.771/0001-31
Fone: (11) 4197 8000
Fax: (11) 4197 8432
www.hp.com.br

670394-BR

Barueri, 22 de julho de 2003.

ECT 17.208 CPL-AC

A
EMPRESA BRASILEIRA DE CORREIOS E TELEGRAFOS
BRASILIA/DF

Ref.: PREGÃO Nº050/2003 – CPL/AC

Objeto.: Locação e instalação de 162(cento e sessenta e dois) equipamentos de informática – novos de fábrica – incluindo: a configuração, o treinamento, a assistência técnica e a garantia, destinados aos Centros Corporativos de Dados da ECT, localizados nas cidades de Brasília e São Paulo, conforme condições gerais e pauta de distribuição e especificações constantes dos ANEXOS 1-a e 1-B deste EDITAL.

Declaramos, na qualidade de fabricante, que teclado ABNT-2 (267145-208) é de nossa fabricação.

Atenciosamente,

Jose Roberto Giani Garcia
Hewlett-Packard Computadores Ltda
CNPJ 00.379.771/0001-31

Nº 561 3702

17.207

Hewlett Packard Company
Palo Alto - California - EUA
www.hp.com

invent

22/07/2003

A
EMPRESA BRASILEIRA DE CORREIOS E TELEGRAFOS
BRASILIA/DF

Ref.: PREGÃO Nº050/2003 – CPL/AC

Objeto.: Locação e instalação de 162(cento e sessenta e dois) equipamentos de informática – novos de fábrica – incluindo: a configuração, o treinamento, a assistência técnica e a garantia, destinados aos Centros Corporativos de Dados da ECT, localizados nas cidades de Brasília e São Paulo, conforme condições gerais e pauta de distribuição e especificações constantes dos ANEXOS 1-a e 1-B deste EDITAL.

Declaramos, na qualidade de fabricante, que a COBRA TECNOLOGIA S/A, CNPJ nº 42.318.949/0001-84, é nosso revendedor autorizado e está apto a comercializar os equipamentos descritos abaixo e asseguramos que os equipamentos estão em nossa linha de produção continuada e comprometemo-nos a fornecer peças de reposição pelo período mínimo de 60 (sessenta) meses.

MARCA	***MODELO***
Hewlett-Packard	HP 9000(RD 2470 e RP 5430), Racks 19"
Hewlett-Packard	HP 9000 SuperDome
Hewlett-Packard	HP SureStore Disk System DS2100
Hewlett-Packard	HP SureStore Tape Array 5300
Hewlett-Packard	Storageworks Core Switch
Hewlett-Packard	OpenView Storage Data Protector
Hewlett-Packard	HP Storageworks ESL 9000/9595 Series-Tape Library
Hewlett-Packard	Software Família OpenView

Hewlett-Packard Company
Carlos Rocha Ribeiro da Silva
Procurador

562

Nº 3702

Hewlett Packard Company
Palo Alto - California - EUA
www.hp.com

invent

22/07/2003

A
EMPRESA BRASILEIRA DE CORREIOS E TELEGRAFOS
BRASILIA/DF

Ref.: PREGÃO Nº050/2003 – CPL/AC

Objeto.: Locação e instalação de 162(cento e sessenta e dois) equipamentos de informática – novos de fábrica – incluindo: a configuração, o treinamento, a assistência técnica e a garantia, destinados aos Centros Corporativos de Dados da ECT, localizados nas cidades de Brasília e São Paulo, conforme condições gerais e pauta de distribuição e especificações constantes dos ANEXOS 1-a e 1-B deste EDITAL.

DECLARAÇÃO DE SOLIDARIEDADE

Declaramos, na qualidade de fabricante, que a COBRA TECNOLOGIA S/A, CNPJ nº 42.318.949/0001-84, é nosso revendedor autorizado e está apto a comercializar os equipamentos por nós produzidos, descritos abaixo:

Declaramos ainda :

a) nossa solidariedade para com a COBRA TECNOLOGIA S/A quanto aos compromissos que esta venha a assumir perante a EMPRESA BRASILEIRA DE CORREIOS E TELEGRAFOS;
b) que a COBRA TECNOLOGIA S/A está apta a prestar assistência técnica, com uso de peças e componentes originais, bem como suporte aos produtos e equipamentos cotados;
c) que somos responsáveis solidários com a COBRA TECNOLOGIA S/A, pelo perfeito cumprimento das exigências de garantia dos equipamentos, durante todo o seu prazo de vigência do contrato.

Hewlett-Packard Company
Carlos Rocha Ribeiro da Silva
Procurador

563
Nº 3702

17.205

PROCURAÇÃO

OUTORGANTE: HEWLETT-PACKARD COMPANY, empresa devidamente incorporada e organizada de acordo com as leis do Estado da Califórnia, Estados Unidos da América, com sede em 3000 Hanover Street, na cidade de Palo Alto, através de seu representante legal o Sr. Charles N. Charnas

OUTORGADA: HEWLETT PACKARD BRASIL LTDA., com sede em Barueri – SP, na Alameda Rio Negro, 750, fundos, 1º andar – sala 4 Alphaville, inscrita no CNPJ sob o nº 61.797.924/0001-55 e HEWLETT-PACKARD COMPUTADORES LTDA, com sede em Campinas-SP, na Rua Um, 1000 – Distrito Industrial – inscrita no CNPJ sob o nº 00.379.771/0001-31, representadas por:

- Carlos Rocha Ribeiro da Silva, cidadão brasileiro, casado, engenheiro, residente na Avenida Professor Rubens Gomes de Souza, 1359, na Cidade de São Paulo, Estado de São Paulo, Brasil, com RG número 17.817.356-9 (SSP-SP) e CPF sob o número 405.086.097-04;

- Ivo Romani, cidadão brasileiro, casado, administrador de empresas, residente na Rua Sergipe, 309, 3o andar, na Cidade de São Paulo, Estado de São Paulo, Brasil, com RG número 7.187.356-9 (SSP-SP) e CPF sob o número 903.621.798-91;

- Décio Alarcon, cidadão brasileiro, solteiro, advogado, residente na Rua Guararapes, 78, apartamento 15, na Cidade de São Paulo, Estado de São Paulo, Brasil, com RG número 7.811.131-6 (SSP-SP) CPF sob o número 012.139,148-50;

PODERES: Pelo presente instrumento e na melhor forma de direito a OUTORGANTE nomeia e constitui a OUTORGADA sua bastante procuradora para o fim especial de, assinar cartas de solidariedade do fabricante referente a garantia dos produtos, em processos licitatórios no Brasil, nos quais participem as Outorgadas acima, perante os Órgãos Federais, Estaduais e Municipais, bem como praticar todos os demais atos necessários ao fiel cumprimento deste mandato, inclusive substabelecer. O presente mandato terá validade de 18 meses a partir desta data.

Data: 10 de fevereiro, 2003

Charles N. Charnas
Vice Presidente, Vice Conselheiro Geral e Secretário Assistente

POWER OF ATTORNEY

PRINCIPAL: HEWLETT-PACKARD COMPANY, a company duly incorporated in accordance with the laws of the State of California, United States of America, headquartered at 3000 Hanover Street, Palo Alto city, through its legal representative Mr. Charles N. Charnas

GRANTEE: HEWLETT PACKARD BRASIL Ltda., headquartered at 750 Alameda Rio Negro, 1st floor, room 4, Alphaville, Barueri, enrolled with CNPJ under number 61.797.924/0001-55, and HEWLETT PACKARD COMPUTADORES LTDA, headquartered at Um Street, 1000 – Distrito Industrial, city of Campinas, São Paulo, enrolled with CNPJ under number 00.379.771/0001-31, represented by:

- Carlos Rocha Ribeiro da Silva, Brazilian Citizen, married, engineer, resident on Professor Rubens Gomes de Souza Avenue, 1359, Sao Paulo City, State of São Paulo, Brazil, ID number 17.817.822 (SSP-SP) and Taxpayer's individual number 405.086.097-04.

- Ivo Romani, Brazilian Citizen, married, business administrator, resident on Sergipe Street, 309 – 3rd floor, São Paulo city, State of São Paulo, Brazil, ID number 7.187.356-9 (SSP-SP) and Individual Taxpayer's number 903.621.798-91.

- Décio Alarcon, Brazilian Citizen, single, attorney, resident on Guararapes Street, 78, apartment 15, São Paulo City, State of São Paulo, Brazil, ID number 7.811.131-6 (SSP-SP) and Individual Taxpayer's number 012.139,148-50.

POWERS: By this power of attorney, and in accordance with the law, the PRINCIPAL, hereby appoints GRANTEE, to sign joint liability agreements regarding product warranties for tenders in Brazil, awarded to the above mentioned parties, appear before all federal, state and municipal government agencies, as well as perform all acts necessary to fully comply with the scope of this power, including the right of delegation. This power is valid for eighteen months from this date.

Date: February 10, 2003

Charles N. Charnas
Vice President, Deputy General Counsel and Assistant Secretary

564

Nº 3702

27 FEB 2003

171551

REGISTRO DE DOCUMENTOS
Títulos e Documentos

Colégio Notarial do Brasil - SP

17.204
2

EM BRANCO

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 565
Doc: 3702

TABELIONATO
REGISTRO CIVIL
ABDEL
BERI - SP

AUTENTICAÇÃO
CONSULADO GERAL DO BRASIL
01 177772

CONSULADO GERAL DO BRASIL SÃO FRANCISCO

Reconheço verdadeira a assinatura, no documento anexo, de VALANNI--- Escrivão da Corte do Condado de Santa Clara Estado Califórnia Estado Unidos da America.

E, para constar onde convier, mandei passar o presente, que assinei a fiz selar com o Selo deste Consulado.
Dispensado reconhecimento de firma de acordo com o Decreto nº 84.451, do 31-01-1980. A legalização deste documento não implica aceitação ou approvação de seu conteúdo.
The legalization of this document does not imply approval or acceptance of its contents.

São Francisco, 12 de fevereiro de 20 03

JAIRO COLLIER
Cônsul-Adjunto

SELO CONSULAR
REPÚBLICA FEDERATIVA DO BRASIL
REAIS OURO

Recebemos R$ 2,00 (ouro) ou US $ 1.00 tab. 1/16

17.203
L

CALIFORNIA ALL-PURPOSE ACKNOWLEDGMENT

State of California

County of SANTA CLARA } ss.

On FEBRUARY 10, 2003 (Date), before me, VALYNN VALANDANI, NOTARY PUBLIC (Name and Title of Officer (e.g., "Jane Doe, Notary Public"))

personally appeared CHARLES N. CHARNAS (Name(s) of Signer(s)),

☑ personally known to me
☐ proved to me on the basis of satisfactory evidence

to be the person~~(s)~~ whose name~~(s)~~ is~~/are~~ subscribed to the within instrument and acknowledged to me that he~~/she/they~~ executed the same in his~~/her/their~~ authorized capacity~~(ies)~~, and that by his~~/her/their~~ signature~~(s)~~ on the instrument the person~~(s)~~, or the entity upon behalf of which the person~~(s)~~ acted, executed the instrument.

WITNESS my hand and official seal.

VALYNN VALANDANI
Commission # 1273761
Notary Public - California
Santa Clara County
My Comm. Expires Aug 13, 2004

Place Notary Seal Above

Signature of Notary Public

OPTIONAL

Though the information below is not required by law, it may prove valuable to persons relying on the document and could prevent fraudulent removal and reattachment of this form to another document.

Description of Attached Document

Title or Type of Document: _____

Document Date: _____ Number of Pages: _____

Signer(s) Other Than Named Above: _____

Capacity(ies) Claimed by Signer

Signer's Name: _____

☐ Individual
☐ Corporate Officer — Title(s): _____
☐ Partner — ☐ Limited ☐ General
☐ Attorney in Fact
☐ Trustee
☐ Guardian or Conservator
☐ Other: _____

RIGHT THUMBPRINT OF SIGNER
Top of thumb here

Signer Is Representing: _____

Colegio Notarial do Brasil - SP
AUTENTICAÇÃO
0109AA17773

27 FEV 2003
17.455-1

REGISTRO DE TITULOS E DOCUMENTOS

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 566
Doc: 3702

© 1999 National Notary Association • 9350 De Soto Ave., P.O. Box 2402 • Chatsworth, CA 91313-2402 • www.nationalnotary.org

HELOISA DO LAGO ALVES PEQUENO
TRADUTORA PÚBLICA E INTÉRPRETE COMERCIAL
Idioma: Inglês

Rua Des. Eliseu Guilherme, 304 - Conj 51 - Paraiso - CEP 04004-030 - São Paulo - SP
Tel:(11) 3887-0822 Fax: (11) 3051-2395
www.heloisapequeno.com.br E-mail: helopeq@heloisapequeno.com.br
Matrícula JUCESP nº 1001 RG nº 4.988.499-2 CPF nº 063.193.638-60 CCM nº 2244147-6

17201

Colégio Notarial do Brasil - SP
TABELIONATO DE NOTAS
ALEXANDRE SIMÕES
AUTENTICAÇÃO
VERSO E ANVERSO
AUTENTICAÇÃO
SELO DE AUTENTICIDADE
AA177769

TRADUÇÃO Nº 360 LIVRO Nº 008 FOLHA Nº 1

Certifico e dou fé, para os devidos fins, que, nesta data, me foi apresentado um documento lavrado no idioma inglês, com a seguinte identificação: PROCURAÇÃO, contendo 1 (uma) página datilografada e apensos, que passo a traduzir para o vernáculo, no seguinte teor:

Este documento está escrito em duas colunas, sendo uma em inglês e a outra, já em português, cujo texto transcrevo a seguir:

PROCURAÇÃO

OUTORGANTE: HEWLETT-PACKARD COMPANY, empresa devidamente constituída de acordo com as leis do Estado de da Califórnia, Estados Unidos da América, com sede em 3000 Hanover Street, na cidade de Palo Alto, através de seu representante legal, o Sr. Charles N. Charnas.

OUTORGADAS: HEWLETT PACKARD BRASIL LTDA., com sede em Barueri-SP, na Alameda Rio Negro, 750, fundos, 1º andar – sala 4 Alphaville, inscrita no CNPJ sob o nº 61.797.924/0001-55 e HEWLETT- PACKARD COMPUTADORES LTDA, com sede em Campinas-SP, NA Rua Um, 1000-Distrito Industrial – inscrita no CNPJ sob o nº 00.379.771/0001-31, representadas por:

- Carlos Rocha Ribeiro da Silva, cidadão brasileiro, casado, engenheiro, .residente na Avenida Professor Rubens Gomes de Souza, 1359,na Cidade de São Paulo, Estado de São Paulo, Brasil, com RG número 17.817.356-9 (SSP-SP) e CPF sob o número 405.086.097-04;

- Ivo Romani, cidadão brasileiro, casado, administrador de empresas, residente na Rua Sergipe,309,3º andar, na Cidade de São Paulo, Estado de São Paulo, Brasil, com RG número 7.187.356-9 (SSP-SP) e CPF sob o número 903.621.798-91;

- Décio Alarcon, cidadão brasileiro, solteiro, advogado, residente na Rua Guararapes, 78, apartamento 15, na Cidade de São Paulo, Estado de São Paulo, Brasil, com RG número 7.811.131-6 (SSP-SP) e CPF sob o número 012.139.148-50;

PODERES: Pelo presente instrumento e na melhor forma de direito, a OUTORGANTE nomeia e constitui a OUTORGADA sua bastante procuradora, para o fim especial de assinar, cartas de solidariedade do fabricante referente a garantia dos produtos, em processos licitatórios no Brasil, nos quais participem as Outorgadas acima, perante os Órgãos Federais, Estaduais e Municipais, bem como praticar todos os demais atos necessários ao fiel cumprimento deste mandato,

27 FEV 2003
1º REGISTRO DE TÍTULOS E DOCUMENTOS
BARUERI - SP
Nº 174551

ROS nº 03/2005 - CN CGMI - CORREIOS
Fls Nº 567
Nº 3702
Doc:

HELOISA DO LAGO ALVES PEQUENO
TRADUTORA PÚBLICA E INTÉRPRETE COMERCIAL
Idioma: Inglês
Rua Des. Eliseu Guilherme, 304 - Conj 51 - Paraiso - CEP 04004-030 - São Paulo - SP
Tel:(11) 3887-0822 Fax: (11) 3051-2395
www.heloisapequeno.com.br E-mail: helopeq@heloisapequeno.com.br
Matrícula JUCESP nº 1001 RG nº 4.988.499-2 CPF nº 063.193.638-60 CCM nº 2244147-6

17200

Colégio Notarial do Brasil - SP
AUTENTICAÇÃO
TABELIÃO ALDEMAR PAIVA
AUTENTICAÇÃO
VERSO E ANVERSO
9AA177770

inclusive substabelecer. O presente mandato terá validade de 18 meses a partir desta data.

Data: 10 de fevereiro de 2003

Assinaturas, nas duas colunas, de Charles N. Charnas, Vice Presidente, Vice Conselheiro Geral e Secretário Assistente

---

Em anexo, consta um formulário de notarização, denominado "Autenticação para todos os fins, da Califómia", nos seguintes termos:

Estado da Califórnia

} ss.

Condado de Santa Clara

Em 10 de fevereiro de 2003, perante mim, Valynn Valandani, Tabeliã Pública, compareceu pessoalmente Charles N. Charnas, que conheço pessoalmente como sendo a pessoa cujo nome está subscrito ao instrumento anexo e que perante mim comprovou ter assinado o mesmo, na qualidade para a qual está autorizada, sendo que mediante a sua assinatura aposta a esse instrumento, a pessoa ou a empresa em nome da qual agiu, também firmou o referido instrumento.
EM TESTEMUNHO DO QUE, aponho minha assinatura e afixo o selo de meu ofício.
Assinatura e carimbo de Valynn Valandani, Tabeliã Pública do Condado de Santa Clara, na Califórnia, habilitação Nº 1273761, que expira em 13 de agosto de 2004.

27 FEV 2003 171551
BARUERI - SP
SOLICITADO E SOLTO!!!
TÍTULOS E DOCUMENTOS
2º REGISTRO

OPCIONAL – Embora as informações abaixo não sejam exigidas por lei, podem ser de valia para pessoas que precisem confiar no documento e podem evitar a retirada e recolocação fraudulenta do presente formulário em outro documento.
(Todos os campos estão em branco)

Em apenso, encontra-se a legalização consular, em vernáculo, transcrita abaixo:
"CONSULADO GERAL DO BRASIL EM SÃO FRANCISCO

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 568
Doc: 3702

17.198

HELOISA DO LAGO ALVES PEQUENO
TRADUTORA PÚBLICA E INTÉRPRETE COMERCIAL

Idioma: Inglês

Rua Des. Eliseu Guilherme, 304 - Conj 51 - Paraiso - CEP 04004-030 - São Paulo - SP
Tel:(11) 3887-0822 Fax: (11) 3051-2395
www.heloisapequeno.com.br E-mail: helopeq@heloisapequeno.com.br
Matrícula JUCESP nº 1001 RG nº 4.988.499-2 CPF nº 063.193.638-60 CCM nº 2244147-6

TRADUÇÃO Nº 360 LIVRO Nº 008 FOLHA Nº 3

Reconheço verdadeira a assinatura, no documento anexo, de Valynn Valandani, Escrivão (sic) da Corte do Condado de Santa Clara, Estado da Califórnia, Estados Unidos da América. E, para constar onde convier, mandei passar o presente, que assinei e fiz selar com o Selo deste Consulado. Dispensado reconhecimento de firma de acordo com o Decreto nº 84.451, do 31-01-1980. A legalização deste documento não implica aceitação ou aprovação de seu conteúdo. São Francisco, 12 de fevereiro de 2003. Assinatura de Jairo Collier, Cônsul Adjunto."

Constam carimbos do Serviço Consular da República Federativa do Brasil em São Francisco, CA, e a estampilha consular, no valor de R$ 20,00 (ouro) ou US$ 20,00, conforme a Tabela 416."

NADA MAIS CONSTAVA DO DOCUMENTO QUE ME FOI ENTREGUE, QUE DEVOLVO JUNTAMENTE COM ESTA TRADUÇÃO, DATILOGRAFADA EM 03 (TRÊS) PÁGINAS DEVIDAMENTE RUBRICADAS, E QUE CONFERI, ACHEI CONFORME E À QUAL APONHO MINHA ASSINATURA E AFIXO O SELO DE MEU OFÍCIO PÚBLICO, NESTE DIA 24 DE FEVEREIRO DE 2003. CERTIFICO E DOU FÉ.

HELOISA DO LAGO ALVES PEQUENO
Tradutora Pública e Intérprete Comercial
Matriculada na JUCESP sob. nº 1001

BARUERI - SP

Emolumentos: R$ 106,40
Talonário nº 005
Recibo nº 0230

27 FEV 2003

1º REGISTRO DE TÍTULOS E DOCUMENTOS

174551

Colegio Notarial do Brasil - SP
AUTENTICAÇÃO
0109AA077777

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 569
Doc: 3702

17.196

São Paulo, 21 de julho de 2003

EMPRESA BRASILEIRA DE CORREIOS E TELÉGRAFOS - ECT

Re.: **PREGÃO N.º 050/2003 - CPL/AC**

Prezados Senhores,

Versão em inglês para referência apenas
English version for reference only

Declaramos para fins do pregão acima que **COBRA COMPUTADORES E SISTEMAS BRASILEIROS S.A.**, CNPJ 42.318.949/0001-84, com endereço na Estrada dos Bandeirantes, 7966, CEP: 22783-110 – Rio de Janeiro - RJ, doravante EMPRESA, é revendedor autorizado Cisco no Brasil.

We hereby inform for the purposes of the above process that **COBRA COMPUTADORES E SISTEMAS BRASILEIROS S.A.**, CNPJ 42.318.949/0001-84, com endereço na Estrada dos Bandeirantes, 7966, CEP: 22783-110 – Rio de Janeiro - RJ, hereinafter COMPANY is an authorized reseller in Brazil.

Asseguramos para fins do certame em referência:

- o fornecimento e a garantia dos produtos Cisco no anexo relacionados; e que
- os equipamentos Cisco cotados pela EMPRESA, relacionados no anexo são de linha de produção continuada e que serão fornecidas peças de reposição pelo período mínimo de 60 (sessenta) meses.

Atestamos ainda, com relação aos equipamentos Cisco relacionados no anexo:

We certify for the purposes of the above process:

- the supply and warranty of the Cisco products listed in the attachment hereto; and that
- the Cisco equipment offered by COMPANY are from a continued line of production and that spare parts will be available for a minimum period of 60 (sixty) months.

We also certify with regards to the Cisco products listed in the attachment hereto:

a) nossa solidariedade para com a EMPRESA no âmbito dos produtos Cisco quanto aos compromissos que a EMPRESA venha a assumir perante a ECT, no escopo desta licitação;

a) our joint liability with COMPANY with regards to Cisco products in relation to the obligations that COMPANY commits before ECT, within this process;

b) que a EMPRESA está apta a prestar assistência técnica, com o uso de peças e componentes originais, bem como suporte aos produtos Cisco cotados;

b) that COMPANY is capable of rendering technical assistance, with the use of original spare parts, as well as support to the Cisco products offered;

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 570
Doc: 3702

17.195

CISCO SYSTEMS

c) nossa responsabilidade solidária para com a EMPRESA pelo perfeito cumprimento das exigências de garantia dos produtos Cisco, durante todo o prazo de vigência do contrato.

c) our joint liability responsibility with COMPANY for the perfect fulfillment of warranty of Cisco products, during the whole term of the agreement.

CONFERIDO POR

Atenciosamente,

Cisco do Brasil Ltda
Sérgio Tsujioka
Representante Legal

30.CARTORIO REGISTRO CIVIL IBIRAPUERA
AV.Nova Independencia,51 Fone: 5506.5744
VALIDO SOMENTE COM SELO DE AUTENTICIDADE
RECONHECO POR SEMELHANCA 0001 FIRMAS (6):
0001-SERGIO FUMIAKI TSUJIOKA
SAO PAULO, 22 DE JULHO DE 2003.
EM TESTEMUNHO DA VERDADE
ALCIDES BATISTA CORREIA-ESC. AUTORIZ.
Total Custas,:*****2,07
Car.:1337029 DOC.S/V.ECONOMICO
Selo:1063AA055807

Selo de Autenticidade Notarial do Brasil - SP
FIRMA 1
1063AA055807
Marcio Roberto Trofino
Escrevente Autorizado

Trofino
Autorizado

RGB nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 571
Doc: 3702

17.194
2

Cisco do Brasil Ltda.
Av. Nações Unidas, 12.901 - 26° and.
04578-000 - São Paulo – SP
Tel.: (011) 5508-9999
Fax: (011) 5508-9998
www.cisco.com

São Paulo, 21 de julho de 2003

A
EMPRESA BRASILEIRA DE CORREIOS E TELÉGRAFOS - ECT

Ref.: **PREGÃO N.º 050/2003 - CPL/AC**

Prezados Senhores,

Declaramos, para fins de comprovação no edital em epígrafe que a empresa **MULTIREDE INFORMÁTICA LTDA.**, inscrita no CNPJ/MF sob o número 66.060.088/0001-45 e localizada na rua Dr. Eduardo de Souza Aranha, 387 – Itaim Bibi – São Paulo - SP é atualmente parceiro certificado pela Cisco Systems, Inc. como **Cisco Learning Solutions Partner**.

Esclarecemos por oportuno que os cursos CWFUN e CWLAW foram descontinuados e substituídos pelo curso CWENT.

CONFERIDO POR

Atenciosamente,

Cisco do Brasil Ltda.
Sergio Tsujioka
Representante Legal

30.CARTORIO REGISTRO CIVIL IBIRAPUERA
AV.Nova Independencia,51 Fone: 5506.5744
VALIDO SOMENTE COM SELO DE AUTENTICIDADE
RECONHECO POR SEMELHANCA 0001 FIRMAS DE:
0001-SERGIO FUMIAKI TSUJIOKA
SAO PAULO, 22 DE JULHO DE 2003.
EM TESTEMUNHO DA VERDADE
NARCIO ROBERTO TROFINO-ESC. AUTORIZ.
Total Custas.:******2,07
Car.:1336963 DOC.S/V.ECONOMICO
Selo:1063AA055783

Colegio Notarial do Brasil - SP
FIRMA 1
1063AA055783

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 572
Doc: 702

Cisco do Brasil Ltda.
Av. Nações Unidas, 12.901 - 26 and
04578-903 - São Paulo – SP
Tel.: (011) 5508-9999
Fax: (011) 5505-9998
www.cisco.com

17.193
2

Procuração

Outorgante: **Cisco do Brasil Ltda.**, com sede na cidade de São Paulo, Estado de São Paulo, na Avenida Nações Unidas, 12.901, 18°. e 26°. andares, CEP 04578-903, inscrita no CNPJ sob o n°. 00.028.666/0001-58, neste ato representada por seu gerente delegado, Sr. Carlos Carnevali, brasileiro, casado, engenheiro, portador da cédula de identidade RG n°. 3.500.054-SSP/SP, inscrito no CPF-MF sob o n°. 205.601.848-91, residente e domiciliado na Cidade de São Paulo-SP, com escritório na Cidade de São Paulo-SP, na Avenida Nações Unidas, 12.901, Torre Oeste, 26°. andar.

Outorgados: **Luis Carlos Araújo Moraes Rego Júnior**, brasileiro, engenheiro elétrico, portador da cédula de identidade RG n°. 6.953.526-7-SSP/SP, inscrito no CPF-MF sob o n°. 082.948.428-00, e **Sérgio Fumiaki Tsujioka**, brasileiro, técnico administrativo, portador da cédula de identidade RG n°. 4.639.759-0-SSP/SP, inscrito no CPF-MF sob o n°. 682.843.908-25, ambos residentes e domiciliados na Cidade de São Paulo-SP, com escritório na Cidade de São Paulo-SP, na Avenida Nações Unidas, 12.901, Torre Oeste,18°. andar.

Poderes: Pelo presente instrumento particular e nos termos do seu Contrato Social atualmente em vigor, a Outorgante nomeia e constitui os Outorgados seus bastante procuradores com poderes para individualmente (i) representar a Outorgante perante as repartições públicas federais, estaduais e municipais, entidades autárquicas e paraestatais, incluindo mas não limitando ao Banco Central do Brasil e às Juntas Comerciais, INSS, neles requerendo, assinado cartas, petições, formulários, documentos de câmbio, arquivar e retirar documentos; (ii) assinar contratos com empresas de utilidade pública e prestadores de serviços, incluindo mas não se limitando a contratos bancários e contratos de câmbio; (iii) representar a Outorgante em licitações, estando autorizado, para esse fim, a assinar documentos em benefício da Outorgante; (iv) interpor e responder recursos administrativos perante qualquer órgão da Administração Pública; (v) movimentar as contas bancárias em nome da Outorgante, assinar cheques e transferências, autorizar ordens de pagamento; e (vi) praticar todos os demais atos necessários ao bom e fiel cumprimento do presente mandato, mas sempre de total conformidade com as disposições e restrições contidas no Contrato Social da Outorgante. É vedado o substabelecimento no todo ou em parte da presente procuração.

Validade: A presente procuração vigorará de 03 de Janeiro de 2003 até **03 de Janeiro de 2004**, a menos que anteriormente revogada.

São Paulo, 19 de dezembro de 2002

Cisco do Brasil Ltda.
Carlos Carnevali
Gerente Delegado

CARTÓRIO REGISTRO CIVIL IBIRAPUERA
... SOMENTE COM SELO DE AUTENTICIDADE ...
... RECONHECIDA 0001 FIRMAS DE:
CARLOS ROBERTO CARNEVALI
... DEZEMBRO DE 2002.
TESTEMUNHO DA VERDADE
... BATISTA CORREIA-ESC. AUTORIZ.
Marcio Roberto Trolino
ESCREVENTE AUT. - SP
RECONHECIMENTO DE FIRMA
1480AA525867

TABELIÃO DE IBIRAPUERA
São Paulo - Capital - Tel: 5505-8570
AUTENTICAÇÃO: ESTA CÓPIA REPROGRÁFICA CONFERE COM O ORIGINAL DA QUAL FOI EXTRAÍDA
Dou FÉ.
21 JUL. 2003
SP,
Cartório Notarial
1º Brasil 30
CAPITAL
5505-8570
AUTENTICAÇÃO
1063

RQS nº 03/2005 - CN - CPMI - CORREIOS
573
Fls Nº
3702
Doc:

17.192
2

CERTIFICADO

A BRTÜV certifica que a Empresa:

CISCO SYSTEMS, INC.
170 West Tasman Drive
San Jose, CA 95134-1706

Implantou e utiliza um Sistema de Qualidade
para a seguinte área de aplicação:

Projeto, desenvolvimento, fabricação, serviço e suporte para solução de rede para internet.

O Sistema auditado está em conformidade com a norma:

NBR ISO 9001: 2000

Este Certificado é válido até: 30 / Novembro / 2003
Nº. de Registro do Certificado: CSQ – Q-1095

A validade deste certificado está sujeita ao atendimento satisfatório e contínuo pela empresa das condições estabelecidas em contrato.
Este certificado dá direito ao registro na Lista de Empresas Certificadas do Sistema Brasileiro de Certificação.

Barueri - SP, 2/6/2003

INMETRO OCS - 0012

BRTÜV Avaliações da Qualidade S/C Ltda.

TABELIÃO DE IBIRAPUERA
São Paulo - Capital - Tel: 5505-8570
AUTENTICAÇÃO: ESTA CÓPIA REPROGRÁFICA CONFERE COM O ORIGINAL DA QUAL FOI EXTRAÍDA
Dou FÉ.
21 MAI 2003
SP
Alcides Batista Correia - Escr. Aut.
Marcio Roberto Trofino - Escr. Aut.
VALIDO SOMENTE COM O SELO DE AUTENTICIDADE
POR AUTENTICAÇÃO R$1,10
Colégio Notarial do Brasil
AUTENTICAÇÃO
106ABD40084
VALIDO SOMENTE COM O SELO DE AUTENTICIDADE

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 574
3702
Doc:

17.191
L

CERTIFICATE

BRTÜV hereby certifies that Company:

CISCO SYSTEMS, INC.
170 West Tasman Drive
San Jose, CA 95134-1706

Has established and applies a Quality Assurance System for:

Design, development, manufacture, service and support of networking solutions for the internet.

The System complies with the standard:

NBR ISO 9001: 2000

This Certificate is valid until: 30 / November / 2003
Certificate registration nr.: CSQ – Q-1095

The validity of this certificate is subject to the continuous and satisfactory compliance of the company to the conditions stated in the contract.
This certificate entitles the company to be registered in the list of certified companies of the Brazilian Certification System.

Barueri - SP, 2/6/2003

INMETRO OCS - 0012

BRTÜV Avaliações da Qualidade S/C Ltda.

TABELIÃO DE IBIRAPUERA
São Paulo - Capital - Tel: 9505-6570
AUTENTICAÇÃO: ESTA CÓPIA REPROGRÁFICA CONFERE COM O ORIGINAL DA QUAL FOI EXTRAÍDA
Dou FÉ.
21 JUL. 2003
SP
Alcides Batista Correia - Escr. Aut.
Márcio Roberto Trofino - Escr. Aut.
POR AUTENTICAÇÃO R$1,10

RQS nº 03/2005 - CN - CPMI - CORREIOS
575
3702

Cobra Equipamentos de rede ECT rev 05

Item 3.1	Switch tipo 1 (layer 3 - GE)	
Produto	**Descrição**	**Qtd.**
WS-C6513	Cat 6513 Chassis, 13slot, 19RU, No Pow Supply, No Fan Tray	1
WS-C6K-13SLT-FAN2	High Speed Fan Tray for Catalyst 6513 / Cisco 7613	1
WS-CAC-2500W	Catalyst 6000 2500W AC Power Supply	1
WS-CAC-2500W/2	Catalyst 6000 Second 2500W AC Power	1
CAB-AC-2500W-INT	Power Cord, 250Vac 16A, INTL	2
S6S22ZK2-12119E	Catalyst 6000 SUP2/MSFC2 IOS SP W/VIP SSH 3DES	1
WS-X6K-S2-MSFC2	Catalyst 6500 Supervisor Engine-2, 2GE, plus MSFC-2 / PFC-2	1
WS-X6500-SFM2	Catalyst 6500 Switch Fabric Module 2	1
WS-X6516A-GBIC	Catalyst 6500 16-port GigE Mod, fabric-enabled (Req. GBICs)	1
WS-F6K-DFC	Dist Fwd Card for 65xx, 6816 Modules used with SUP1A/SUP2	1
MEM-DFC-128MB	128 MB DRAM FOR DFC	1
WS-X6548-GE-TX	Catalyst 6500 48-port fabric-enabled 10/100/1000 Module	1
WS-X6548-GE-TX	Catalyst 6500 48-port fabric-enabled 10/100/1000 Module	1
WS-X6548-GE-TX	Catalyst 6500 48-port fabric-enabled 10/100/1000 Module	1
WS-X6516-GE-TX	Catalyst 6500 16-port Gig/Copper Module, x-bar	1
WS-F6K-DFC	Dist Fwd Card for 65xx, 6816 Modules used with SUP1A/SUP2	1
MEM-DFC-128MB	128 MB DRAM FOR DFC	1
WS-X6066-SLB-APC	Catalyst 6000 Content Switching Module	1
SC6K-3.1.3-CSM	CSM 3.1.3 Software Release	1
WS-SVC-NAM-1	Catalyst 6500 Network Analysis Module-1	1
SC-SVC-NAM-3.1	Catalyst 6500 NAM SW Release 3.1	1
WS-X6516-GE-TX	Catalyst 6500 16-port Gig/Copper Module, x-bar	1
WS-F6K-DFC	Dist Fwd Card for 65xx, 6816 Modules used with SUP1A/SUP2	1
MEM-DFC-128MB	128 MB DRAM FOR DFC	1
WS-X6516-GE-TX	Catalyst 6500 16-port Gig/Copper Module, x-bar	1
WS-F6K-DFC	Dist Fwd Card for 65xx, 6816 Modules used with SUP1A/SUP2	1
MEM-DFC-128MB	128 MB DRAM FOR DFC	1
WS-X6516-GE-TX	Catalyst 6500 16-port Gig/Copper Module, x-bar	1
WS-F6K-DFC	Dist Fwd Card for 65xx, 6816 Modules used with SUP1A/SUP2	1
MEM-DFC-128MB	128 MB DRAM FOR DFC	1
WS-G5484	1000BASE-SX Short Wavelength GBIC (Multimode only)	16

Fls Nº 576
Doc:
03/2005 - CN - CORREIOS

17.190

MEM-S2-128MB	Catalyst 6000 Sup2 Mem, 128MB DRAM Option	1
MEM-MSFC2-128MB	Catalyst 6000 MSFC-2 Mem, 128MB DRAM Option	1
	Equipamento (unitário)	
	Total de equipamentos	**4**

Item 3.2	**Switch tipo 2 (FE)**	
Produto	**Descrição**	**Qtd.**
WS-C2950G-48-EI	Catalyst 2950, 48 10/100 with 2 GBIC slots, Enhanced Image	1
CAB-AC	Power Cord,110V	1
WS-G5484=	1000BASE-SX Short Wavelength GBIC (Multimode only)	1
WS-X3500-XL	GigaStack Stacking GBIC and 50cm cable	1
PWR675-AC-RPS-N1=	675W Redundant Power Supply with 1 connector cable	1
CAB-AC	Power Cord,110V	1
	Equipamento	
	Total de equipamentos	**6**

Item 3.5	**Switch tipo 5 (Concentrador de VPNs)**	
Produto	**Descrição**	**Qtd.**
CVPN3060-NR	VPN 3060 Concentrator (Non-Redun, 1 P/S); 5000users@100Mbps	1
CVPN3060-SW-K9	Software for VPN3060 Concentrator	1
CAB-AC	Power Cord,110V	1
CVPN3000-PWR=	Cisco VPN 3000 Concentrator Power Supply	1
	Equipamento	
	Total de equipamentos	**4**

Item 3.5 (cont.)	**Servidor de Autenticação para o Switch tipo 5**	
Produto	**Descrição**	**Qtd.**
CSACSE-1111-K9	Cisco Secure ACS 3.2 Solution; includes HW and SW	1
CAB-AC	Power Cord,110V	1
CSACSE-3.2-SW-K9	Config. Option; CSACS 3.2 Software loaded on Cisco 1111	1
	Equipamento	
	Total de equipamentos	**2**

Item 3.6	**Router tipo 1**	
Produto	**Descrição**	**Qtd.**

ECT/CN
CORREIOS
03/2005
577
0270
2

7
1781

CISCO3745	3700 Series, 4-Slot, Dual FE, Multiservice Access Router	1
PWR-3745-AC	AC Power Supply for the Cisco 3745	1
PWR-3745-AC/2	Redundant AC System Power Suppy for the Cisco 3745	1
CAB-AC	Power Cord,110V	2
S374AK9-12301	Cisco 3745 Ser IOS ENTERPRISE PLUS IPSEC 3DES	1
NM-1FE2W	1 10/100 Ethernet with 2 WAN Card Slot Network Module	1
WIC-2T	2-Port Serial WAN Interface Card	2
NM-1A-E3	1-Port E3 ATM Network Module	1
NM-1GE	1 Port GE Network Module	1
WIC-2T	2-Port Serial WAN Interface Card	2
CAB-SS-V35MT	V.35 Cable, DTE Male to Smart Serial, 10 Feet	8
ROUTER-SDM	Device manager for routers	1
WS-G5483=	1000BASE-T GBIC	1
	Equipamento	
	Total de equipamentos	**2**

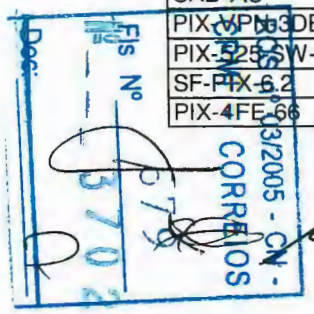
Item 3.7	**Router tipo 2**	
Produto	**Descrição**	**Qtd.**
CISCO1751-V	10/100 Modular Router w/Voice,32F/64D	1
MEM1700-64U96D	Cisco 1751-V 64MB to 96MB DRAM Factory Upgrade	1
S17C7HVK9-12208T	Cisco 1700 IOS IP/ADSL/VOICE/FW/IDS PLUS IPSEC 3DES	1
WIC-2T	2-Port Serial WAN Interface Card	1
VIC-2FXO	Two-port Voice Interface Card - FXO	1
VIC-2FXS	Two-port Voice Interface Card - FXS	1
PVDM-256K-4	4-Channel Packet Voice/Fax DSP Module	2
CAB-AC	Power Cord,110V	1
CAB-SS-V35FC	V.35 Cable, DCE Female to Smart Serial, 10 Feet	1
CAB-SS-V35MT	V.35 Cable, DTE Male to Smart Serial, 10 Feet	1
	Equipamento	
	Total de equipamentos	**2**

Item 6.1	**Servidor Segurança Lógica tipo 1**	
Produto	**Descrição**	**Qtd.**
PIX-535	PIX Firewall 535 Chassis	1
CAB-AC	Power Cord,110V	1
PIX-VPN-3DES	168-bit 3DES VPN feature license for PIX Firewall	1

ECT
Fls Nº 3702
578
Doc.
SRTE/SC Nº 03/2005 - CN - CORREIOS

PIX-535UR-SW	Unrestricted feature license for PIX 535 Firewall	1
SF-PIX-6.2	PIX v6.2 Software for the PIX 515E, 525 and 535 Chassis	1
PIX-1GE-66	66MHz Gigabit Ethernet Interface, Multimode (SX) SC	1
PIX-1GE-66	66MHz Gigabit Ethernet Interface, Multimode (SX) SC	1
PIX-4FE-66	PIX 66-MHz Four-port 10/100 Ethernet Interface, RJ45	1
PIX-535-PWR-AC	Redundant AC power supply for PIX 535	1
PIX-1FE	Single 10/100 Fast Ethernet Inteface for PIX Firewall, RJ45	1
PIX-1FE	Single 10/100 Fast Ethernet Inteface for PIX Firewall, RJ45	1
PIX-VPN-ACCEL	VPN Accelerator Card for PIX 515E/525/535-UR/FO Firewall	1
PIX-535-MEM-512	PIX 535 512MB RAM Upgrade (2-256MB DIMM, UR Only)	1
PIX-535-PWR-BLANK	Blank to fill unused power supply slot on PIX 535	1
PIX-535	PIX Firewall 535 Chassis	1
CAB-AC	Power Cord,110V	1
PIX-VPN-3DES	168-bit 3DES VPN feature license for PIX Firewall	1
PIX-535FO-SW	Failover feature license for PIX 535 Firewall	1
SF-PIX-6.2	PIX v6.2 Software for the PIX 515E, 525 and 535 Chassis	1
PIX-1GE-66	66MHz Gigabit Ethernet Interface, Multimode (SX) SC	1
PIX-1GE-66	66MHz Gigabit Ethernet Interface, Multimode (SX) SC	1
PIX-4FE-66	PIX 66-MHz Four-port 10/100 Ethernet Interface, RJ45	1
PIX-535-PWR-AC	Redundant AC power supply for PIX 535	1
PIX-1FE	Single 10/100 Fast Ethernet Inteface for PIX Firewall, RJ45	1
PIX-1FE	Single 10/100 Fast Ethernet Inteface for PIX Firewall, RJ45	1
PIX-VPN-ACCEL	VPN Accelerator Card for PIX 515E/525/535-UR/FO Firewall	1
PIX-535-MEM-512	PIX 535 512MB RAM Upgrade (2-256MB DIMM, UR Only)	1
PIX-535-PWR-BLANK	Blank to fill unused power supply slot on PIX 535	1
	Equipamento	
	Total de equipamentos	**4**

Item 6.2	**Servidor Segurança Lógica tipo 2**	
Produto	**Descrição**	**Qtd.**
PIX-525	PIX Firewall 525 Chassis	1
CAB-AC	Power Cord,110V	1
PIX-VPN-3DES	168-bit 3DES VPN feature license for PIX Firewall	1
PIX-525-SW-UR	Unrestricted feature license for PIX 525 Firewall	1
SF-PIX-6.2	PIX v6.2 Software for the PIX 515E, 525 and 535 Chassis	1
PIX-4FE-66	PIX 66-MHz Four-port 10/100 Ethernet Interface, RJ45	1



PIX-1GE-66	66MHz Gigabit Ethernet Interface, Multimode (SX) SC	1
PIX-VPN-ACCEL	VPN Accelerator Card for PIX 515E/525/535-UR/FO Firewall	1
PIX-525	PIX Firewall 525 Chassis	1
CAB-AC	Power Cord,110V	1
PIX-VPN-3DES	168-bit 3DES VPN feature license for PIX Firewall	1
PIX-525-SW-FO	Failover feature license for PIX 525 Firewall	1
SF-PIX-6.2	PIX v6.2 Software for the PIX 515E, 525 and 535 Chassis	1
PIX-4FE-66	PIX 66-MHz Four-port 10/100 Ethernet Interface, RJ45	1
PIX-1GE-66	66MHz Gigabit Ethernet Interface, Multimode (SX) SC	1
PIX-VPN-ACCEL	VPN Accelerator Card for PIX 515E/525/535-UR/FO Firewall	1
	Equipamento	
	Total de equipamentos	**2**

Item 6.3	**Servidor para Detecção de Intrusão - IDS**	
Produto	**Descrição**	**Qtd.**
IDS-4250-TX-K9	4250 Sensor (chassis, s/w, SSH, 10/100/1000BaseT w/ RJ-45)	1
CAB-AC	Power Cord,110V	1
IDS-RAIL-2	2 post Rail Kits for the IDS 4235/4250 Sensor Platforms	1
	Equipamento	
	Total de equipamentos	**2**

	CiscoWorks VPN/Security Management Solution (VMS)	
Produto	**Descrição**	**Qtd.**
CWVMS-2.2-UR-K9	VMS 2.2 WIN/SOL Unrestricted	1
CWVMS-MCCSA-4.0	Expanded Part use Only: MC for Cisco Security Agents 4.0	1
	Equipamento	
	Total de equipamentos	**2**

	CiscoWorks LAN Management Solution	
Produto	**Descrição**	**Qtd.**
CWLMS-2.2-K9	LAN Managment 2.2 for WIN/SOL; CM, DFM, RME, RTM, CV	1
	Equipamento	
	Total de equipamentos	**2**

	CiscoWorks2000 Routed WAN Management	
Produto	**Descrição**	**Qtd.**

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 3702
Doc: 580

CWRW-1.3-K9	Routed WAN Mgmt 1.3 for WIN/SOL; ACL, IPM, RME, CV	1
	Equipamento	
	Total de equipamentos	**2**

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 581
Doc: 3702

17185

EMC²
where information lives

17.184
L

DECLARAÇÃO DE SOLIDARIEDADE DO FABRICANTE/REVENDA

A EMC Computer Systems Brasil Ltda, inscrita no CNPJ/MF sob o n.º 01.462.017/0001-12 declara, para fins de prova do **subitem 2.4** do Anexo 3, do Edital de Pregão n.º 050/2003, na condição de fabricante/revenda, que a empresa licitante COBRA Tecnologia S.A., inscrita no CNPJ/MF sob número 42.318.949/0001-84, está autorizada a comercializar o produto Connectrix ED-12000B.

A EMC Computer Systems Brasil Ltda declara sua solidariedade com a empresa licitante COBRA Tecnologia S.A., no âmbito dos produtos de sua fabricação quanto aos compromissos que a referida empresa licitante venha a assumir perante a ECT, no escopo desta licitação.

A EMC Computer Systems Brasil Ltda, informa que a licitante COBRA Tecnologia S.A. esta apta a prestar assistência técnica, com uso de peças e componetes originais, bem como suporte aos produtos cotados.

Adicionalmente a EMC Computer Systems Brasil Ltda, declara sua responsabilidade solidária para com o proponente pelo perfeito cumprimento das exigências de garantia dos produtos, durante todo o prazo de vigência do contrato.

São Paulo, 17 de Julho de 2003.

CONFERIDO POR

Rinaldo Sganzela
Diretor Financeiro

1063AA052444

RGS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 582
Doc. 3702

EMC²
where information lives

17.185

CERTIFICADO

A EMC Computer Systems Brasil Ltda., estabelecida na Rua Verbo Divino, 1.488, 4° andar, São Paulo, SP, inscrita no CNPJ/MF sob número 01.462.107/0001-23, subsidiária da EMC Corporation, certifica que tem como revenda autorizada a Empresa COBRA Tecnologia S.A., sediada na Estrada dos Bandeirantes, 7.966, Jacarepaguá, Rio de Janeiro – RJ, inscrita no CNPJ/MF sob número 42.318.949/0001-84, perante o cliente Correios, referente ao Edital do Pregão Nº 050/2003.

São Paulo, 14 de Julho de 2003

CONFERIDO COM O ORIGINAL

Rinaldo Sganzela
Diretor Financeiro

30.CARTORIO REGISTRO CIVIL TIRADENTES
AV.Nova Independencia,51 Fone: 5506.
VALIDO SOMENTE COM SELO DE AUTENTICIDADE
RECONHECO POR SEMELHANCA 0001 FIRMA(S)
0001-RINALDO SGANZELA
SAO PAULO, 17 DE JULHO DE 2003
EM TESTEMUNHO
JOAO ANGELO
Total Custas:
Car.:
Selo:

FIRMA 1 1063AA052445

ROS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 583
Doc: 3702

EMC²
where information lives

17.182

CERTIFICADO

A EMC Computer Systems Brasil Ltda., estabelecida na Rua Verbo Divino, 1.488, 4° andar, São Paulo, SP, inscrita no CNPJ/MF sob número 01.462.107/0001-23, subsidiária da EMC Corporation, assegura que os equipamentos cotados, EMC Connectrix ED-12000B, são de linha de produção continuada e que se compromete a fornecer peças de reposição pelo período mínimo de 60 (sessenta) meses, perante o cliente Correios, referente ao Edital do Pregão Nº 050/2003.

São Paulo, 22 de Julho de 2003

CONFERIDO POR

Rinaldo Sganzela
Diretor Financeiro

30.CARTORIO REGISTRO CIVIL IBIRAPUERA
AV.Nova Independencia,51 Fone: 5506.5744
VALIDO SOMENTE COM SELO DE AUTENTICIDADE
RECONHECO POR SEMELHANCA 0001 FIRMAS DE:
001-RINALDO SGANZELA
SAO PAULO, 23 DE JULHO DE 2003.
EM TESTEMUNHO DA VERDADE
OLIVIA NEVES D. SIMOES-ESC. AUTORIZ.
Total Custas.:*****2,70
Car.:133704 POD.S/V.RECONHEC
Selo:1063**AA045744

FIRMA 1 1063AA045744

CORREIOS
Fls Nº 584
Nº 3702

Project Management Institute

This is to certify that

Cyrus Daylac

has successfully completed all prescribed requirements and is hereby designated by the Project Management Institute as a

Project Management Professional

26 December 2002 - 31 December 2005

In testimony whereof, we have subscribed our signatures under the seal of the Institute.

Project Management Institute

Certification Number: 58744

Chair, Board of Directors

Executive Director

RGS nº 03/2005 - CN - CEMI - CORREIOS
Fls Nº 585
3702

PROPERTY OF THE PROJECT MANAGEMENT INSTITUTE

4181

CORREIOS **ADMINISTRAÇÃO CENTRAL** 17.180

ATESTADO DE VISTORIA

Atestamos para fins de Licitação, relativamente ao Edital do Pregão n.º 050/2003- CPL/AC, cujo objeto é a locação de equipamentos de informática, que o Sr(a) Ozilia Mª Rodrigues Pereira representante da empresa Cobra Computadores Sist. Brasileiros S.A., esteve visitando nesta data, as instalações físicas do Centro Corporativo de Dados de Brasília - DF., visando obter subsídios para a proposta econômica da licitação em questão.

1. Responsável pelo Termo de Vistoria
   Nome em letra de forma: Ruy Ney Muniz Barbosa
   Matrícula: 1-1339939-2
   Assinatura: _____
   Data: 17 / 7 /2003.

2. Representante da Licitante
   Nome em letra de forma: Ozilia Mª Rodrigues Pereira
   Assinatura: _____
   Data: 017/07/2003.

Brasília-DF, 17 de Julho de 2003.

OBSERVAÇÕES:

- Os interessados em participar desta Licitação deverão realizar, ***obrigatoriamente***, vistoria nos Centros Corporativos de Dados de Brasília e São Paulo, devidamente acompanhada de representante da ECT.
  Os endereços dos CCDs são os seguintes:
  Brasília : SBN - QUADRA 01- BLOCO A - 2º SUBSOLO - ED. SEDE ECT - BRASÍLIA/DF
  São Paulo : RUA MERGENTHALER, Nº 592 – BLOCO 3 – 4° ANDAR – VILA LEOPOLDINA CEP: 05311-900 SÃO PAULO – SP
- As vistorias deverão ocorrer no prazo de até **02 (dois) dias úteis** antes da data de abertura da licitação, objetivando conhecer, principalmente, as características técnicas do ambiente e os locais de instalação dos produtos.
- O agendamento das vistorias deverá ser previamente efetuado junto aos seguintes telefones:
  Brasília: (0xx61) 426-2214/1754/1896
  São Paulo: (0xx11) 3838-7755/7000/7001

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 586
Nº 3702
Doc:

17.179

ANEXO 3

(MODELO VI)

ATESTADO DE VISTORIA

Atestamos para fins de Licitação, relativamente ao Edital do Pregão n.º 050/2003- CPL/AC, cujo objeto é a locação de equipamentos de informática, que o Sr(a) José de Andrade Francisco, representante da empresa Cobra Computadores e Sist. Bras SA, esteve visitando nesta data, as instalações físicas do Centro Corporativo de Dados de São Paulo- SPM, visando obter subsídios para a proposta econômica da licitação em questão.

1. Responsável pelo Termo de Vistoria
   Nome em letra de forma: OCAVO DE BRITO
   Matrícula: BSIB438-6
   Assinatura:
   Data: 17/07/2003.

2. Representante da Licitante
   Nome em letra de forma: JOSÉ DE ANDRADE FRANCISCO
   Assinatura:
   Data: 17/07/2003.

São Paulo
~~Brasília~~-DF, 17 de julho de 2003.

OBSERVAÇÕES:

- Os interessados em participar desta Licitação deverão realizar, ***obrigatoriamente***, vistoria nos Centros Corporativos de Dados de Brasília e São Paulo, devidamente acompanhada de representante da ECT.
  ~~Os endereços dos CCDs são os seguintes:~~
  Brasília : SBN - QUADRA 01- BLOCO A - 2º SUBSOLO - ED. SEDE ECT - BRASÍLIA/DF
  São Paulo : RUA MERGENTHALER, N° 592 – BLOCO 3 – 4° ANDAR – VILA LEOPOLDINA CEP: 05311-900 SÃO PAULO – SP
- As vistorias deverão ocorrer no prazo de até **02 (dois) dias úteis** antes da data de abertura da licitação, objetivando conhecer, principalmente, as características técnicas do ambiente e os locais de instalação dos produtos.
- O agendamento das vistorias deverá ser previamente efetuado junto aos seguintes telefones:
  Brasília: (0xx61) 426-2214/1754/1896
  São Paulo: (0xx11) 3838-7755/7000/7001

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 587
Doc: 3702

17.178

CISCO SYSTEMS

São Paulo, 22 de julho de 2003

EMPRESA BRASILEIRA DE CORREIOS E TELÉGRAFOS - ECT

Re.: **PREGÃO N.º 050/2003 - CPL/AC**

Prezados Senhores,

Informamos abaixo algumas características técnicas dos produtos Cisco abaixo relacionados:

1) As fontes de alimentação do concentrador Cisco VPN 3060 possuem recurso de troca sem interrupção (HOT-SWAPPABLE/HOT-PLUGGABLE).

2) O roteador Cisco 3745 possui capacidade de roteamento de até 225.000 (duzentos e vinte e cinco mil) pacotes por segundo, utilizando pacotes de 64 (sessenta e quatro) bytes, sem perdas de pacotes.

3) O roteador Cisco 3745 possui MTBF (Mean Time Between Failures) superior a 50.000 (cinqüenta mil) horas.

4) O roteador Cisco 3745 permite a configuração de 1024 (mil e vinte e quatro) rotas estáticas.

5) A módulo de rede NM-1A-E3, compatível com o roteador Cisco 3745, possui interface compatível com o padrão ITU-T G.703.

6) O roteador Cisco 1751-V possui fonte de alimentação elétrica de 90 a 240 Volts com comutação automática e freqüencia de 60 (sessenta) Hertz.

7) A Cisco do Brasil recomenda, para o Edital 050/2003 da Empresa de Correios e Telégrafos, o uso o sistema operacional Pix OS versão 6.2 para os firewalls Cisco Pix 535 e Pix 525.

8) O firewall Cisco Pix 525 com a versão do sistema operacional Pix OS 6.2 possui capacidade de processamento superior a 350 Mbps em texto claro.

9) O sistema de detecção de intrusão IDS 4250 permite a detecção de ataques que utilizam recursos de detecção Whisker anti-IDS.

10) O sistema de detecção de intrusão IDS 4250 permite a detecção de Probin Attacks através das assinaturas de ataques do tipo Probe, como por exemplo Finger Probe, Apache/mod_ssl Worm Probe, SATAN Probe e Backdoor Probes em portas TCP ou UDP.

CONFERIDO POR

Atenciosamente,

Cisco do Brasil Ltda.
Sérgio Tsujioka
Representante Legal

30.CARTORIO REGISTRO CIVIL IBIRAPUERA
AV.Nova Independencia,51 Fone: 5506.5744
VALIDO SOMENTE COM SELO DE AUTENTICIDADE
RECONHECO POR SEMELHANCA 0001 FIRMAS (EM)
001-SERGIO FUMIAKI TSUJIOKA
SAO PAULO, 23 DE JULHO DE 2003.
EM TESTEMUNHO DA VERDADE
MARCIO ROBERTO PROPHIRO - ESCREVENTE AUTORIZ.
Total Custas: [illegible]2,07
Car.:[illegible] MOD.5/V.ECONOMICO
Selo:1063AA054801

ROSRAP 03/2005 - CNJ
CPMI - CORREIOS
588
Colégio Notarial do Brasil - SP
Fls. Nº
FIRMA 1
Marcio Roberto Prophiro
Escrevente Autorizado
1063AA054801

PROPOSTA TÉCNICA – Edital do Pregão CORREIOS Nº 050/2003

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

RQS nº 03/2005 - CN - CPMI - CORREIOS
1/25
Fls Nº 589
Nº Doc: 3702

INDICE

1. ASPECTOS GERAIS 4
2. DETALHAMENTO DO CRONOGRAMA DE TRABALHO 5
2.1. CRONOGRAMA DE EXECUÇÃO 5
3. ENTREGA E INSTALAÇÃO 6
3.1. RECURSOS DE SUPORTE AOS EQUIPAMENTOS 6
3.2. RELATÓRIO DE INSTALAÇÃO (RI) 7
4. INSTALAÇÃO E HOMOLOGAÇÃO DO AMBIENTE 7
5. DISPONIBILIDADE 8
6. COMPATIBILIDADE E PORTABILIDADE 9
7. GARANTIA E ASSISTÊNCIA TÉCNICA 9
8. CHAMADOS TÉCNICOS 10
8.1. CHAMADO DE SUPORTE DE HARDWARE 11
8.2. CHAMADO DE SUPORTE DO AMBIENTE OPERACIONAL 11
8.3. HORÁRIO DE ATENDIMENTO DE SUPORTE 12
9. TREINAMENTO OPERACIONAL 12
10. TREINAMENTO ON-SITE 13
10.1. TREINAMENTO DE HARDWARE 13
10.2. TREINAMENTO DE SOFTWARE 14
10.3. TREINAMENTO DE GERENCIAMENTO 14
10.4. TREINAMENTO DE SUPORTE 15
10.5. TREINAMENTO OFICIAL 16
11 MODELO DOS EQUIPAMENTOS PROPOSTOS 17
11.1 SERVIDOR INTEL TIPO 1 17
11.2 SERVIDOR INTEL TIPO 2 17
11.3 SERVIDOR INTEL TIPO 3 17
11.4 SERVIDOR RISC TIPO 01 18
11.5 SWITCH TIPO 1 19
11.6 SWITCH TIPO 2 19
11.7 SWITCH TIPO 3 19
11.8 SWITCH TIPO 4 (KVM) 19
11.9 SWITCH TIPO 5 19
11.10 ROTEADOR TIPO 1 20
11.11 ROTEADOR TIPO 2 20
11.12 UNIDADE DE BACKUP ROBOTIZADO 20
11.13 SERVIDOR DE SEGURANÇA LÓGICA TIPO 1 20
11.14 SERVIDOR DE SEGURANÇA LÓGICA TIPO 2 20
11.15 SERVIDOR PARA DETECÇÃO DE INTRUSÃO 20
11.16 LICENÇAS DE CONCORD ENHANCED SYSTEMEDGE 21
12. MODO DE APRESENTAÇÃO DA COMPROVAÇÃO DAS ESPECIFICAÇÕES EXIGIDAS NO EDITAL 21
12.1 SERVIDOR INTEL TIPO 1 21
12.2 SERVIDOR INTEL TIPO 2 21
12.3 SERVIDOR INTEL TIPO 3 21
12.4 SERVIDOR RISC TIPO 1 21
12.5 SWITCH TIPO 01 21
12.6 SWITCH TIPO 02 21
12.7 SWITCH TIPO 03 21
12.8 SWITCH TIPO 04 21
12.9 SWITCH TIPO 05 21
12.10 ROTEADOR TIPO 01 22

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

RQS nº 03/2005 - 25CN - CPMI - CORREIOS
Fls Nº 590
Nº 3702
Doc:

12.10 ROTEADOR TIPO 02 22
12.11 UNIDADE DE BACKUP ROBOTIZADO 22
12.12 SERVIDOR DE SEGURANÇA LÓGICA 01 22
12.13 SERVIDOR DE SEGURANÇA LÓGICA 02 22
12.14 SERVIDOR PARA DETECÇÃO DE INTRUSÃO 22
12.15 SOFTWARES 22
13 CONFORMIDADE COM REQUISITOS GERAIS 22

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 591
Nº 3702
Doc:

17174

1. ASPECTOS GERAIS

a) A Empresa Brasileira de Correios e Telégrafos será tratada como **CORREIOS,** a COBRA TECNOLOGIA S.A. será tratada como COBRA. Entende-se por **PRODUTO** todo e qualquer componente de hardware, software ou serviço fornecido pela **COBRA**;

b) A COBRA fornecerá, garantirá compatibilidade e portabilidade, instalará, configurará, dará garantia e assistência técnica aos PRODUTOS fornecidos e treinará a equipe técnica da CORREIOS, durante a vigência do Contrato;

c) O fornecimento contemplará os **PRODUTOS** descritos nesta proposta, provendo a:
- Preparação do ambiente de produção, realizando integração e interoperabilidade com o ambiente já existente, relativamente aos itens Rede TCP/IP e Segurança de Rede;
- Integração e interoperabilidade da Rede SAN – Storage Area Network, existente no **CORREIOS** com a Rede SAN fornecida, de forma que os Servidores e o Sistema de Backup fornecidos pela **COBRA** possam acessar os dados armazenados no atual sistema de armazenamento (Storage IBM 2105 F20), com a performance compatível com as aplicações existentes.

d) Os PRODUTOS descritos nesta proposta possuem quantidades e especificações suficientes para a execução das funcionalidades solicitadas pelo edital 050/2003 do CORREIOS. PRODUTOS adicionais, necessários ao cumprimento das exigências funcionais e de performance, verificadas durante a vigência do Contrato, serão fornecidos pela COBRA;

e) Caberá à COBRA, a obrigatoriedade de fornecer, instalar e configurar, a critério exclusivo da CORREIOS, as atualizações e correções de todos os softwares fornecidos, englobando, inclusive, a evolução das versões, sem ônus adicionais à CORREIOS, durante a vigência do Contrato;

f) Serão de exclusiva responsabilidade da COBRA a entrega, a instalação, a configuração, os testes, a garantia e assistência técnica dos PRODUTOS, bem como o fornecimento dos recursos adicionais que sejam necessários ao pleno atendimento das funcionalidades exigidas neste Edital;

g) A COBRA procederá a entrega e a instalação física de todos os PRODUTOS nas Salas de Segurança Física, nas cidades de Brasília/DF e São Paulo/SP, conforme pauta de distribuição descrita no Item 01 do ANEXO 1-B do edital o50/2003 do CORREIOS;

h) Serão fornecidos pela COBRA, quando da instalação dos PRODUTOS, todos os insumos, suprimentos e componentes, tais como, e não se limitanto a: cabos, acessórios, mídias, manuais e documentações necessárias;

i) Serão fornecidos pela COBRA todos os controladores (drivers) necessários para o funcionamento dos equipamentos fornecidos, bem como todos os demais programas necessários à instalação, configuração e diagnóstico dos equipamentos, periféricos e interfaces;

j) A COBRA, na data de assinatura do contrato, apresentará equipe de trabalho e seus integrantes, relacionando-os nominalmente e informando currículo e telefone para contato, e será alocado um profissional como gestor do projeto durante a vigência do Contrato;

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

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 592
Nº Doc: 3702

k) O gestor do projeto alocado será certificado PMP (Project Management Professional) pelo PMI (Project Management Institute). Uma cópia deste certificado, atualizado e vigente,constará na Proposta Econômica da COBRA;

l) O CORREIOS poderá solicitar, a qualquer momento da vigência do Contrato, a seu critério, a substituição de qualquer membro da equipe de trabalho, comprometendo-se a comunicar com antecedência de 15 (quinze) dias;

m) O CORREIOS deverá indicar, na data da assinatura do contrato, o nome do Gestor e o nome dos componentes da sua equipe técnica para coordenar e orientar todo o processo de instalação, configuração e testes dos PRODUTOS, cabendo ao Gestor acompanhar o cumprimento dos prazos e atestar a qualidade dos PRODUTOS entregues;

n) A COBRA detalhará o plano de trabalho, conforme Item 1.2 deste Anexo, para implantação dos PRODUTOS, informando o cronograma de atividades detalhado em fases, atividades, prazos e recursos alocados;

o) No que se refere a PRODUTOS, periféricos, acessórios, instalação, garantia, recursos humanos, translado, tarifas telefônicas, transporte, hospedagem, embalagens, e outras despesas, diretas e indiretas, necessárias ao cumprimento das obrigações da COBRA, serão de responsabilidade da COBRA e não gerarão qualquer ônus ao CORREIOS;

q) O CORREIOS poderá, a seu critério, solicitar o deslocamento e/ou movimentação dos equipamentos dentro das Salas de Segurança Física de Brasília-DF e São Paulo-SP. Todos as despesas relativas a este movimentação serão de responsabilidade da COBRA. O CORREIOS poderá solicitar os deslocamentos durante a vigência do contrato.

2. DETALHAMENTO DO CRONOGRAMA DE TRABALHO

a) A COBRA apresentará, para validação da CORREIOS, até 45 (quarenta e cinco) dias após a assinatura do Contrato, cronograma detalhado de atividades contendo, os seguintes itens:
- Planejamento da adequação dos recursos de suporte à instalação dos equipamentos;
- Cronograma de Entrega e Instalação dos Equipamentos;
- Arquitetura detalhada da interligação de todos os **PRODUTOS** fornecidos;
- Cronograma de Instalação e Configuração do Ambiente Operacional e dos Softwares;
- Arquitetura planejada para a interconexão dos elementos que compõem a Rede TCP/IP,
- Rede SAN e a Rede de Segurança com os atuais equipamentos existentes nos CCDs;
- Planejamento do treinamento dos técnicos da **CORREIOS**.

b) Sempre que houver alteração/atualização do cronograma, uma nova versão será imediatamente encaminhada, para validação da CORREIOS, com respectivos relatórios de impacto;

c) Qualquer alteração no corpo técnico ou gerencial da COBRA não afetará o cronograma nem tampouco a qualidade dos PRODUTOS contratados.

2.1. CRONOGRAMA DE EXECUÇÃO

Será obedecido o seguinte cronograma de execução:

Fase	Descrição	Prazo (dias)
I	**Apresentação do Cronograma de Trabalho em até**	**D + 45**

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

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 593
3702
Doc:

II	**Entrega, Instalação e Configuração dos Equipamentos ematé**	**D + 90**
III	**Aceitação Final dos Equipamentos em até**	**D + 120**
IV	**Treinamento Operacional em até**	**FIII + 30**
V	**Treinamento Oficial em até**	**FIII + 720**
VI	**Treinamento On-Site em até**	**FIII + 1440**

Onde: **D = Data de Assinatura do Contrato.**
FIII = Data de Emissão do Termo de Aceite da Fase III.

3. ENTREGA E INSTALAÇÃO

3.1. RECURSOS DE SUPORTE AOS EQUIPAMENTOS

a) A COBRA fornecerá, instalará e adequará todas as conexões lógicas e elétricas necessárias à instalação de todos os equipamentos ofertados para os CCDs de Brasília e São Paulo, levando em consideração a padronização e garantia das Salas de Segurança Física – SSF;

b) Todos os PRODUTOS utilizados na adequação das instalações lógicas e elétricas permanecerão em caráter definitivo na CORREIOS após o término do Contrato;

c) Para efeito de quantitativo de conexões lógicas que serão fornecidas e instaladas pela COBRA, serão consideradas todas as interfaces de rede de todos os equipamentos fornecidos, inclusive os equipamentos adicionais, mais o percentual de 25% sobre esta quantidade;

d) Para efeito de quantitativo de conexões elétricas a serem fornecidas e instaladas pela COBRA, serão consideradas todas as entradas de energia elétrica de todos os equipamentos fornecidos, inclusive os equipamentos adicionais, mais o percentual de 20% sobre esta quantidade;

e) O fornecimento englobará todos os cabos, fibras óticas, conectores, disjuntores, quadros elétricos, leitos aramados, tomadas e demais equipamentos e componentes necessários à interligação de todos os equipamentos ofertados, tanto lógica quanto eletricamente, levando em consideração a padronização e garantia das Salas de Segurança Física – SSF;

g) Todos os cabos, conectores e fibras fornecidos serão certificados por órgãos competentes e possuirão o comprimento suficiente para inteligar todos os equipamentos. Será entregue um percentual adicional de 20% (vinte por cento) sobre as quantidades fornecidas de cabos de rede e fibras óticas;

h) O cabeamento lógico UTP CAT 6 a ser lançado pela COBRA será certificado para suportar operação a velocidade de 1Gbps;

i) O fornecimento de toda e qualquer ferramenta, instrumento, material e equipamento de proteção, bem como materiais complementares necessários à instalação serão de inteira responsabilidade da COBRA e não gerará ônus ao CORREIOS;

k) A COBRA entregará toda a documentação da implantação dos PRODUTOS, conforme forem implantados, inclusive, alterando as documentações existentes de maneira a retratar as novas configurações dos ambientes das SSF´s após a implantação. Serão entregues 4 (quatro) cópias impressas e 4 (quatro) cópias em CDROM de toda a documentação.

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

RQS nº 03/2005 - CN - CPMI - CORREIOS
6/25
Fls Nº 594
Doc: 3702

3.2. RELATÓRIO DE INSTALAÇÃO (RI)

a) Será elaborado em formulário impresso apresentando, os seguintes itens:
- Confirmação de todos os requisitos necessários para o perfeito funcionamento de cada PRODUTO, nos locais onde estará instalado, de maneira distinta, com um item para cada caso;
- Confirmação da presença e funcionamento adequado de acessórios, cabos de interface, cabos de alimentação, softwares, manual de instalação, manual de operação, manual de manutenção, discriminando um item para cada caso;
- Confirmação do perfeito funcionamento do hardware e do software para os todos os **PRODUTOS**;
- A identificação de cada produto (marca, modelo, versão de software, número de série e outras informações pertinentes);
- A identificação da instalação, condições das tensões de alimentação e demais informações identificadoras da instalação;
- Nome, Matrícula, Data e assinatura do técnico da **COBRA** que instalou o**PRODUTO**;
- Nome, Matrícula, Data e assinatura do representante técnico da **CORREIOS**.

b) O CORREIOS, através de seu representante técnico, poderá conferir o completo preenchimento do RI. Todas as informações fornecidas nesse RI serão de responsabilidade única da própria COBRA;

c) O CORREIOS, através de seu representante técnico e de posse do RI, poderá acompanhar o técnico da COBRA no teste de aceitação do Período de Funcionamento Experimental – PFE, de cada PRODUTO, quando serão verificados todos os itens apresentados no RI;

f) Quando não aprovado o funcionamento de qualquer PRODUTO, a COBRA anotará no RI as ocorrências e suas origens, e tomará toda e qualquer providência necessária para resolvê-las, indicando no RI a condução sobre as ocorrências, pelo representante técnico do CORREIOS, sem gerar ônus ao CORREIOS e sem prejudicar o tempo previsto de instalação;

i) Desde que por escrito e a critério da CORREIOS, a instalação dos PRODUTOS poderá ser:
- Alterada em sua seqüência;
- Prorrogada por prazo determinado.

4. INSTALAÇÃO E HOMOLOGAÇÃO DO AMBIENTE

a) Após o fornecimento, instalação e configuração dos PRODUTOS fornecidos (conforme requisitos de segurança recomendados pelo fabricante e de acordo com a política de segurança do CORREIOS), poderá ser estabelecido pela CORREIOS um PFE – Período de Funcionamento Experimental – para testar o perfeito funcionamento dos PRODUTOS, verificar as funcionalidades dos mesmos analisando sua aderência às especificações do Edital e a sua compatibilidade com a estrutura já existente na CORREIOS;

b) Durante o PFE, todos os PRODUTOS poderão ser testados quanto à configuração realizada. Poderão ser efetivados testes de acesso através da Rede TCP/IP, Rede SAN, Equipamentos de Segurança Lógica bem como a realização de procedimentos de BACKUP e RESTORE.

c) Durante o período de avaliação, que poderá estender-se por até 7 (sete) dias consecutivos, não deverá ocorrer qualquer falha ou interrupção em qualquer uma das funcionalidades dos PRODUTOS fornecidos, durante este período;

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

RQS nº 03/2005 - CN - CPMI - CORREIOS
7/25
Fls Nº 595
Doc: 3702

e) A COBRA entregará todos os comprovantes que atestem o licenciamento dos softwares fornecidos. A relação detalhadas dos softwares e seu quantitativo constará em planilha a ser entregue à CORREIOS.

g) Durante o PFE, os PRODUTOS que apresentarem defeitos, ou apresentarem mau funcionamento serão reparados ou substituídos imediatamente e, se dentro do conjunto composto por equipamentos do mesmo tipo, o número de equipamentos defeituosos ultrapassar 10% (dez por cento) do seu total, todo o conjunto desse tipo de equipamento será substituído sem ônus para o CORREIOS;

h) Para os servidores INTEL de todos os tipos, a COBRA executará, nos servidores indicados pela CORREIOS, o software MS SYSTEM STRESS da MICROSOFT pelo período de 72 (setenta e duas) horas ininterruptas em cada equipamento. Caso o servidor apresente problemas de hardware durante este período, a COBRA executará o reparo ou substituição e o teste poderá ser executado novamente. Caso o equipamento volte a apresentar defeito ou mau funcionamento em outras 2 (duas) tentativas, o equipamento será substituído sem ônus para a CORREIOS;

i) Para os servidores RISC TIPO 1, a COBRA realizará teste de 'STRESS' dos componentes de processamento, memória e I/O. Os testes proporcionarão intensiva utilização do poder de processamento, alocação intensiva de memória RAM e componentes de I/O, devendo ainda realizar intensiva escrita e leitura no equipamento de Storage da CORREIOS. A COBRA, em estrita concordância com a CORREIOS, poderá lançar mão de qualquer ferramenta que realize os testes especificados. O período de testes não será inferior a 24 (vinte e quatro) horas ininterruptas nos equipamentos apontados pela CORREIOS. Caso o servidor presente problemas de hardware durante este período, a COBRA executará o reparo ou substituição e o teste será executado novamente. Caso o equipamento volte a apresentar defeito ou mau funcionamento em outras 2 (duas) tentativas, o equipamento será substituído sem ônus para a CORREIOS;

j) Poderão ser também objetos de avaliação pela CORREIOS o atendimento, suporte, execução dos serviços, bem como os planos de Treinamento;

k) A equipe de implantação da COBRA deverá permanecer alocada e presente durante o prazo de 30 (trinta) dias após emitido o Termo de Aceitação da Fase III.

5. DISPONIBILIDADE

a) Os PRODUTOS deverão estar disponíveis 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, 365 (trezentos e sessenta e cinco) dias por ano;

b) Os valores mínimos de disponibilidade para cada PRODUTO, apurados mensalmente, serão de 98,33%, (noventa e oito virgula trinta e três por cento);

c) A disponibilidade de cada PRODUTO será calculada para o período de 30 (trinta) dias corridos, pela seguinte operação:
D = [(To – Ti)/To] * 100%
onde: D = disponibilidade (em %);
To = período de operação (últimos 30 dias corridos) em minutos;
Ti = somatório dos minutos com interrupções do serviço durante os últimos 30 (trinta) dias corridos de operação).

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

RQS nº 03/2005 - CN - CPMI - CORREIOS
8725
Fls Nº 596
Doc: 3702

d) Sempre que forem apurados valores de disponibilidade mensais abaixo dos valores mínimos estabelecidos, poderá ser calculado o período (tempo) de indisponibilidade do serviço, que poderá ser o somatório dos tempos de indisponibilidade, desde a zero hora do primeiro dia até as vinte e quatro horas do último dia do mês corrente;
e) No cálculo de disponibilidade não serão computadas as interrupções previamente acordadas entre a COBRA e CORREIOS.

6. COMPATIBILIDADE E PORTABILIDADE

a) A COBRA garante que os PRODUTOS referentes aos servidores RISC Tipo 1, serão compatíveis com os softwares relacionados a seguir:
Softwares
- Aplicação OneWorld JDEdwards XE;
- Servidor de Aplicação Websphere Application Server v 4.0;
- Banco de Dados Oracle v 9i - 64 bits.

A documentação correspondente a essas compatibilidades se encontram no ANEXO SOFTWARE.

A comprovação está no ANEXO COMPATIBILIDADE E PORTABILIDADE.

b) A COBRA será responsavel, a qualquer tempo da vigência do contrato, pelas correções e customizações dos PRODUTOS fornecidos para a plataforma de servidores RISC. Ficando a cargo da CORREIOS as correções ou customizações das Aplicações Corporativas (aplicativos) migrados para os equipamentos RISC fornecidos.

7. GARANTIA E ASSISTÊNCIA TÉCNICA

a) Todos os PRODUTOS fornecidos possuirão garantia de funcionamento durante a vigência do Contrato;

b) A garantia e a assistência técnica cobrirão as localidades de Brasília/DF e São Paulo/SP, através de filiais da própria empresa, quer seja através de representantes credenciados;

c) Sem apresentar qualquer ônus à CORREIOS, a garantia e a assistência técnica de todos os PRODUTOS abrangerão a manutenção preventiva e corretiva com a cobertura de todo e qualquer defeito apresentado, inclusive, não se restringindo a: substituição de peças, partes, componentes e acessórios;

d) A manutenção corretiva é a série de procedimentos executados, mediante solicitação do CORREIOS, para recolocar os PRODUTOS em seu perfeito estado de uso, funcionamento e desempenho, inclusive com a substituição de componentes, partes, ajustes, reparos e demais serviços necessários de acordo com os manuais de manutenção do fabricante e normas técnicas específicas para cada caso;

e) Os serviços de manutenção corretiva serão prestados nas dependências da CORREIOS, onde se encontrarem instalados os PRODUTOS. Esses serviços de manutenção corretiva serão executados pela COBRA, a pedido da CORREIOS;

f) A COBRA não deixará de executar a manutenção corretiva sob qualquer alegação, mesmo sob pretexto de não ter sido executada anteriormente qualquer tipo de intervenção no respectivo PRODUTO, quer seja tal intervenção a limpeza externa, a manutenção preventiva ou qualquer outra;

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

RQS nº 03/2005 - CN - CPMI - CORREIOS
9/25
Fls Nº 597
Doc: 3702

g) Todas as despesas decorrentes da necessidade de substituição dos PRODUTOS, transporte, deslocamento, embalagem, peças, partes, manuais do fabricante, serão de inteira responsabilidade da COBRA, não devendo gerar qualquer ônus à CORREIOS;

h) A COBRA prestará os serviços de manutenção através de empresas credenciadas, desde que os interventores técnicos dessas credenciadas também tenham habilitação legal e técnica, as quais deverão ser apresentadas, à CORREIOS, na ocasião da manutenção. Tais habilitações também poderão ser solicitadas a qualquer momento pela CORREIOS, sem que com isso diminua a responsabilidade única e exclusiva da COBRA sobre a instalação e manutenção;

i) A COBRA deverá ser a única responsável por todo e qualquer ato de seus empregados, credenciados e representantes, inclusive sobre danos causados à CORREIOS ou a terceiros, por negligência, imperícia, imprudência e/ou dolo, durante toda a vigência do contrato;

j) O tempo de atendimento para efeito de aplicação de penalidades decorrentes do não cumprimento dos prazos de atendimento aos chamados técnicos será contabilizado a partir do registro da ocorrência pela CORREIOS;

k) A COBRA se compromete a substituir, sem ônus para a CORREIOS, os PRODUTOS instalados por novos com as mesmas especificações, funcionalidades e capacidade dos contratados, durante a vigência do Contrato, sempre que forem enquadrados em qualquer uma das seguintes situações:
- PRODUTOS que apresentarem 2 (dois) ou mais defeitos que comprometam o seu
- funcionamento e desempenho, dentro de um período de 30 (trinta) dias;
- quando a soma dos tempos de paralisação do PRODUTO ultrapassar 20 (vinte) horas,
- dentro de um período de 30 (trinta) dias.

l) A substituição de que trata a alínea anterior ocorrerá no prazo de 10 (dez) dias corridos, a partir do registro da ocorrência pela CORREIOS;

m) A COBRA contará, ela mesma ou seus representantes, com estoques de peças e componentes dos equipamentos fornecidos nas cidades de Brasília/DF e São Paulo/SP;

n) Faz parte desta proposta DECLARAÇÃO de que a COBRA manterá por no mínimo 5 (cinco) anos peças em estoque para os PRODUTOS fornecidos;

o) A COBRA se coloca como única responsável pelos PRODUTOS fornecidos ao CORREIOS.

8. CHAMADOS TÉCNICOS

a) Todas as demandas, inclusive as que resultem em manutenção de natureza corretiva, bem como o fluxo de resolução de problemas será documentado por sistema informatizado de gerenciamento do Serviço de Atendimento/Suporte Técnico;

b) A cada chamado técnico a COBRA emitirá, por escrito, ordem de serviço discriminando os seguintes itens: o número identificador do chamado, a data e a hora do chamado, a data e a hora do atendimento, o motivo da chamada, causa do defeito, a situação do chamado, a data e a hora da solução, os trabalhos executados, a marca, modelo, número de série do equipamento, o técnico executante da solução definitiva e as peças substituídas, tudo de forma clara, compreensível e facilmente legível;

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 598
Nº 3702
Doc:

c) Todas as informações relativas aos chamados técnicos serão disponibilizadas ao CORREIOS através de relatórios mensais de acompanhamento, a serem entregues em cópia impressa e em mídia eletrônica, até o 5º (quinto) dia útil do mês subseqüente;

d) A COBRA apresentará e fornecerá ao empregado do CORREIOS, responsável pelo acompanhamento do chamado, logo após a conclusão do mesmo, a ordem de serviço mencionada no item anterior, para aceite e atesto;

e) Mesmo se permitido pela CORREIOS, a permanência do técnico além do tempo de resolução do problema, para a continuidade de solução de um problema, não representará qualquer ônus adicional à CORREIOS;

f) A CORREIOS permitirá o acesso dos técnicos credenciados pela COBRA às instalações onde se encontrarem os equipamentos para a prestação dos serviços de manutenção. Entretanto, tais técnicos ficarão sujeitos às normas internas de segurança da CORREIOS, notadamente àquelas atinentes à identificação, trânsito e permanência nas dependências;

g) As interrupções programadas para manutenções preventivas dos equipamentos contratados serão comunicadas à CORREIOS com antecedência mínima de 5 (cinco) dias úteis. O horário será negociado de forma a não haver impacto na produção;

h) A COBRA disponibilizará ao CORREIOS um serviço de atendimento com discagem gratuita (0800), sem ônus para a CORREIOS, para chamada do serviço de suporte técnico que estará acessível durante 24h x 7 x 365 (vinte e quatro horas por dia, sete dias na semana, trezentos e sessenta e cinco dias por ano).

8.1. CHAMADO DE SUPORTE DE HARDWARE

a) Com atendimento "on site" (atuação de um técnico no local onde está instalado o equipamento), no prazo máximo de 02 (duas) horas. O Prazo máximo para restauração do equipamento inoperante é de até 06 (seis) horas e o prazo máximo para solução total do problema é de até 12 (doze) horas. Todos os prazos serão contabilizados a partir do registro de ocorrência pela CORREIOS. A solução do problema engloba a substituição por outro equipamento com capacidade similar ou superior, até o conserto integral do equipamento com defeito, caso o reparo não seja possível dentro do prazo acima;

b) A COBRA disponibilizará ao CORREIOS um serviço de atendimento com discagem gratuita (0800) ou qualquer outro meio de comunicação de disponibilidade imediata, sem ônus para a CORREIOS, para chamada do serviço de suporte técnico que estará acessível durante 24h x 7 x 365 (vinte e quatro horas por dia, sete dias na semana, trezentos e sessenta e cinco dias).

8.2. CHAMADO DE SUPORTE DO AMBIENTE OPERACIONAL

a) Com atendimento "on site" (atuação de um técnico no local onde está instalado o ambiente operacional), no prazo máximo de 02 (duas) horas. O prazo máximo para restauração das funcionalidades inoperantes é de até 06 (seis) horas e o prazo máximo para solução total do problema é de até 12 (doze) horas. Todos os prazos serão contabilizados a partir do registro de ocorrência pela CORREIOS.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 599
Doc: 3702

b) Os prazos estabelecidos acima não se referem a BUGS de software que necessitem de apoio de laboratório do fabricante, nestes casos os prazos deverão ser definidos pela CORREIOS em conjunto com a COBRA.

c) Entende-se como AMBIENTE OPERACIONAL todos os softwares instalados ou embarcados nos equipamentos, tais como e não se limitando a: sistemas operacionais, softwares de backup, ferramentas de gerência, microcódigo, bios e firmware.

8.3. HORÁRIO DE ATENDIMENTO DE SUPORTE

a) A COBRA disporá de estrutura que permita o registro de ocorrência pela CORREIOS e atendimento de suporte em horário integral, sendo 24h x 7 x 365 (vinte e quatro horas por dia, sete dias na semana, trezentos e sessenta e cinco dias por ano).

9. TREINAMENTO OPERACIONAL

a) A COBRA ministrará WORKSHOPS, com 2 (duas) turmas de até 12 (doze) participantes cada, sendo 1 (uma) turma em Brasília e 1 (uma) turma em São Paulo.

b) Os WORKSHOPS serão realizados em locais disponibilizados pela COBRA nas cidades de Brasília e São Paulo, próximo aos locais de instalação dos PRODUTOS.

c) Cada WORKSHOP abordará os itens citados abaixo, sendo que a carga horária de cada um será negociada previamente com o CORREIOS, de forma a permitir aos técnicos do CORREIOS o conhecimento pleno dos seguintes itens:

Conectividade
- Topologia e equipamentos da rede TCP/IP (Switches e Roteadores)
- Operação dos softwares de gerenciamento da rede TCP/IP

Rede SAN e Backup
- Características dos equipamentos e política de backup implantada
- Topologia e equipamentos da rede SAN
- Operação dos equipamentos de Backup
- Operação dos softwares de gerenciamento da Rede SAN e do Backup
- Geração de relatórios de estatísticas de utilização dos equipamentos

Servidores RISC e INTEL
- Características dos equipamentos
- Implementação e operação do particionamento lógico/físico
- Implementação e operação do Gerenciamento de pré-falha dos Servidores
- Implementação do ambiente de alta disponibilidade em RISC
- Implementação do ambiente de alta disponibilidade em INTEL

Equipamentos de Segurança Lógica
- Características dos equipamentos e softwares envolvidos no ambiente de segurança
- Operação dos softwares utilizados na segurança lógica
- Configuração de regras, restrições e políticas nos equipamentos de segurançalógica
- Definição, configuração e geração de relatórios

Chamados Técnicos
- Características do contrato de garantia dos **PRODUTOS**
- Check-list de ocorrências mais comuns e soluções
- Verificações mínimas antes de acionar o suporte
- Levantamento das informações necessárias para abertura de chamado técnico

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 600
Doc: 3702

17.165

- Contatos com a **COBRA** para suporte e manutenção.

d) A COBRA entregará, a cada participante, em cada WORKSHOP realizado, material didático elaborado de acordo com o assunto a ser abordado. O material deverá ser entregue ao CORREIOS, 15 (quinze) dias antes da realização de cada WORKSHOP para avaliação quanto aos padrões de qualidade estabelecidos pela CORREIOS.

e) No material a ser entregue estará inserido todo o assunto abordado durante o WORKSHOP. Estarár previsto espaço para anotações de itens relevantes. Todo o material fornecido será de boa edição, impressão e possuirá encadernação. Existirá impressão a cores sempre que for indicada para melhor visualização de gráficos, desenhos,tabelas e fotos.

f) Todas as despesas com material, impressão e encadernação serão por conta da COBRA.

g) As datas de realização dos WORKSHOPS serão negociadas com o CORREIOS, no mínimo, 5 (cinco) dias úteis antes da realização do referido workshop, de forma a permitir disponibilidade dos participantes.

h) O CORREIOS terá o direito de acompanhar e avaliar os WORKSHOPS, com instrumento próprio de avaliação.

10. TREINAMENTO ON-SITE

a) A Equipe de Projeto da COBRA realizará a passagem de conhecimento sobre os PRODUTOS e a arquitetura implantada para os profissionais que irão atuar no TREINAMENTO ON-SITE. A duração desta transferência de conhecimento não será inferior a 30 (trinta) dias a partir da data do aceite da FASE III.

b) O CORREIOS poderá solicitar, a qualquer momento da vigência do Contrato, a seu critério, a substituição de qualquer membro da equipe de treinamento, comprometendo-se a comunicar com antecedência de 15 (quinze) dias;

c) A COBRA alocará profissionais nas instalações da CORREIOS, nas cidades de Brasília/DF e São Paulo/SP, para realizar a transferência de tecnologia, através de treinamentos práticos, nas 4 (quatro) especialidades descritas abaixo.

10.1. TREINAMENTO DE HARDWARE

a) A COBRA alocará e manterá, sem gerar ônus à CORREIOS, 02 (dois) profissionais especializados em atendimento de hardware, nas dependências da CORREIOS, sendo 01 (um) no CCD de Brasília e 01 (um) no CCD de São Paulo.

b) Estes profissionais estarão presentes em cada CCD, nas cidades de Brasília/DF e São Paulo/SP, das 08:00 às 18:00h, com intervalo de até 2 (duas) horas, de segunda a sexta, e estarão disponíveis para consultas através de celular ou pager nos demais dias e horários.

c) Os profissionais realizarão a transferência de conhecimento da tecnologia e da operação do hardware fornecido pela COBRA.

d) O treinamento ocorrerá durante o período de 6 (seis) meses a partir da data do aceite da FASE III.

RQS nº 03/2005 - CN - CPMI - CORREIOS
13/23
Fls Nº 601
Nº 3702
Doc:

17.164
L

10.2. TREINAMENTO DE SOFTWARE

a) A COBRA alocará e manterá, sem gerar ônus à CORREIOS, 02 (dois) profissionais especializados em atendimento de software, nas dependências da CORREIOS, sendo 01 (um) profissional no CCD de Brasília e 01 (um) profissional no CCD de São Paulo.

b) Estes profissionais estarão presentes em cada CCD, nas cidades de Brasília/DF e São Paulo/SP, das 08:00 às 18:00h, com intervalo de até 2 (duas) horas, de segunda a sexta, e estarão disponíveis para consultas através de celular ou pager nos demais dias e horários.

c) Os profissionais realizarão a transferência de conhecimento da tecnologia e daoperação dos softwares fornecido pela COBRA.

d) Os profissionais designados pela COBRA possuirão conhecimentos técnicos aprofundados, no mínimo, das seguintes especialidades:
- Sistemas Operacionais Unix em Alta Disponibilidade;
- Análise de Performance de Sistemas Operacionais Unix;
- Unidades de Backup;
- Gerenciadores de Backup;
- Redes SAN.

e) Estes conhecimentos estarão atualizados nas versões/modelos dos PRODUTOS fornecidos pela COBRA.

f) Os profissionais serão apresentados, pelo menos 15 (quinze) dias antes do início do treinamento de software, munidos de currículo com os respectivos certificados para entrevista e análise pela equipe técnica da CORREIOS.

g) O treinamento ocorrerá durante o período de 48 (quarenta e oito) meses a partir da data do aceite da FASE III.

10.3. TREINAMENTO DE GERENCIAMENTO

a) A COBRA alocará e manterá, sem gerar ônus à CORREIOS, 1 (um) profissional especializado em gerenciamento, nas dependências da CORREIOS, no CCD de Brasília-DF.

b) Este profissional estará presente no CCD, nas cidade de Brasília/DF, das 08:00 às 18:00h, com intervalo de até 2 (duas) horas, de segunda a sexta, devendo estar disponível para consultas através de celular ou pager nos demais dias e horários.

c) Este profissional realizará a integração dos PRODUTOS fornecidos à Plataforma de Gerenciamento da CORREIOS, repassando aos técnicos da mesma os detalhes técnicos necessários à integração.

d) O profissional poderá, a critério do CORREIOS, ser convocado a realizar os trabalhos de integração das ferramentas no CCD/SPM, na cidade de São Paulo-SP. Todas as despesas relativas a passagens, alimentação e estadas serão de responsabilidade da COBRA.

e) O profissional designado pela COBRA, possuirá conhecimentos técnicos profundados, no mínimo, das seguintes especialidades:
- Implantação de Gerenciamento de Ambiente de Produção baseado na Plataforma HP
- OpenView (Network Node Manager – NNM e OpenView Operations – OVO);

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 602
Nº 3702
Doc:

- Implantação de Gerenciamento de Ambiente de Produção baseado na Plataforma Concord eHealth.

f) O profissional designado terá participado da elaboração e implantação de projetos de gerencimento utilizando as duas plataformas mencionadas, HP Openview e Concord eHealth, em pelo menos, 3 (três) empresas de médio/grande porte.

g) A participação nestes projetos será comprovada através de declarações emitidas pelas empresas nas quais os projetos foram desenvolvidos ou pelas empresas pelas quais o profissional prestou os serviços.

h) O profissional possuirá treinamento oficial nas principais ferramantas das plataformas mencionadas, HP Openview e Concord eHealth, especificamente, NNM e OVO.

i) O profissional será apresentado, pelo menos 15 (quinze) dias antes do início do treinamento de gerenciamento, munido de currículo com os respectivas certificados e declarações, para entrevista e análise pela equipe técnica da CORREIOS.

j) O treinamento ocorrerá durante o período de 48 (quarenta e oito) meses a partir da data do aceite da FASE III.

10.4. TREINAMENTO DE SUPORTE

a) A COBRA alocará e manterá, sem gerar ônus à CORREIOS, 4 (quatro) profissionais especializados no atendimento de suporte técnico, nas dependências do CORREIOS, sendo 02 (dois) profissionais no CCD de Brasília e 02 (dois) profissionais noCCD de São Paulo.

b) Estes profissionais estarão presentes em cada CCD, nas cidades de Brasília/DF e São Paulo/SP, das 08:00 às 18:00h, com intervalo de até 2 (duas) horas, de segunda a sexta, e estarão disponíveis para consultas através de celular ou pager nos demais dias e horários.

d) Cada profissional, mediante solicitação do CORREIOS, poderá ser convocado a trabalhar fora do horário pré-determinado até o limite de 32 (trinta e duas) horas extras por mês, cabendo a COBRA os encargos financeiros e trabalhistas resultantes destas convocações.

e) O conjunto formado por estes profissionais possuirá, no mínimo, treinamento oficial dos fabricantes dos softwares e hardware, nos modelos e versões fornecidos pela COBRA. A capacitação dos profissionais permitirá a resolução de problemas relacionados as seguintes especialidades:
- Sistemas Operacionais Unix em Alta Disponibilidade;
- Sistemas Operacionais Windows em Alta Disponibilidade;
- Unidades de Armazenamento e Backup;
- Gerenciadores de Backup e Redes SAN.

f) Estes conhecimentos estarão atualizados nas versões/modelos dos PRODUTOS fornecidos pela COBRA.

g) Os profissionais serão apresentados, pelo menos 15 (quinze) dias antes do início do treinamento de suporte, munidos de currículo com os respectivos certificados para entrevista e análise pela equipe técnica da CORREIOS. Caso sejam considerados com perfil técnico ou profissional inadequados, deverão ser substituídos pela COBRA, sem qualquer ônus para a CORREIOS.

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

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 603
Doc: 3702

h) Os diplomas terão sido emitidos por centros de formação autorizados pelos fabricantes/desenvolvedores dos PRODUTOS fornecidos pela COBRA.

i) O treinamento ocorrerá durante o período de 48 (quarenta e oito) meses a partir da data do aceite da FASE III.

10.5. TREINAMENTO OFICIAL

a) Os cursos serão ministrados por Instrutores Certificados pelo fabricante/desenvolvedor dos PRODUTOS;

b) O treinamento poderá ocorrer pelo período de até 24 (vinte e quatro) meses, a partir do aceite da FASE III;

c) Os cursos serão ministrados por Instrutores Certificados pelo fabricante/desenvolvedor dos PRODUTOS fornecidos;

d) A grade de cursos será elaborada pela COBRA de forma a atender os valores mínimos especificados para cada item:

Formação de Especialista em Sistemas Operacionais MICROSOFT
- Mínimo de 160 horas-aula por aluno;
- 4 (quatro) turmas com 6 (seis) alunos cada, sendo 3 (três) turmas em Brasília e 1 (uma) turma em São Paulo.

Formação de Especialista em Sistemas Operacionais UNIX
- Mínimo de 160 horas-aula por aluno;
- 4 (quatro) turmas com 6 (seis) alunos cada, sendo 3 (duas) turmas em Brasília e 1 (uma) turma em São Paulo.

Formação de Administradores de Banco de Dados MS SQL SERVER 2000
- Mínimo de 80 horas-aula por aluno;
- 2 (duas) turmas com 6 (seis) alunos cada, sendo 2 (duas) turmas em Brasília.

Formação de Especialista em Segurança Lógica
- Mínimo de 160 horas-aula por aluno;
- 2 (duas) turmas com 6 (seis) alunos cada, sendo 2 (duas) turmas em Brasília ou São Paulo ou Rio de Janeiro.

Formação de Especialista em Conectividade - Switches TCP/IP e Roteadores
- Mínimo de 220 horas-aula por aluno;
- 3 (três) turmas com 6 (seis) alunos cada, sendo 2 (duas) turmas em Brasília e 1 (uma) turma em São Paulo.

Formação de Especialista nas Ferramentas de Gerenciamento
- Mínimo de 80 horas-aula por aluno;
- 3 (três) turmas com 6 (seis) alunos cada, sendo 2 (duas) turmas em Brasília e 1 (uma) turma em São Paulo.

e) As turmas serão prioritariamente fechadas.

f) A COBRA apresentará a grade detalhada com proposta de cronograma dos treinamentos oficiais para validação pela CORREIOS.

g) A COBRA ministrará todos os treinamentos tendo como idioma o português (Brasil).

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 604
Nº 3702
Doc:

17.161
L

h) A COBRA fornecerá ao final de cada conjunto de cursos oficiais, as provas de certificação, em Centros Autorizados na cidade de Brasília. As certificações que serão oferecidas são as seguintes:

Plataforma INTEL (12 vagas)
- MICROSOFT – Microsoft Certified System Administrator – MCSA

Plataforma RISC (12 vagas)
- HP – HP-UX System Administration

Conectividade (12 vagas)
- as provas serão fornecidas de acordo com o programa de certificação de fabricante de equipamentos de rede, prevendo nível de especialista em switches e roteadores.

11 MODELO DOS EQUIPAMENTOS PROPOSTOS

11.1 SERVIDOR INTEL TIPO 1

- HP Proliant DL 760 G2 montado em rack
- 8 processadores Intel Xeon MP de 2.0 Ghz
- Barramento de sistema de 400 Mhz
- Memória cache de 2Mb por processador
- Memória RAM de 8Gb ECC SDRAM
- Controladora integrada Ultra 3 SCSI com suporte a RAID 0, 1, 0+1, 5
- 2 discos rígidos SCSI Ultra 3 de 10K rpm de 72,8 Gb – Hot Swap
- Controladora de vídeo SVGA integrada com 8Mb
- Uma unidade de CD-ROM IDE 24 X
- 2 controladoras Fiber Channel operando a 2 GB com 2 canais
- 3 interfaces de rede local em barramento PCI padrão Ethernet 10/100/1000 Base-T com gerenciamento SNMP
- 2 Fontes de Alimentação operando de forma redundante

Quantidade proposta: 14 para CCD/BSB e 7 para CCD/SP.

11.2 SERVIDOR INTEL TIPO 2

- HP Proliant DL 580 G2 montado em rack
- 4 processadores Intel Xeon MP de 2.0 Ghz
- Barramento de sistema de 400 Mhz
- Memória cache de 2Mb por processador
- Memória RAM de 4Gb ECC SDRAM
- Controladora integrada Ultra 3 SCSI com suporte a RAID 0, 1, 0+1, 5
- 2 discos rígidos SCSI Ultra 3 de 10K rpm de 72,8 Gb – Hot Swap
- Controladora de vídeo SVGA integrada com 8Mb
- Uma unidade de CD-ROM IDE 24 X
- 2 controladoras Fiber Channel operando a 2 GB com 2 canais
- 2 interfaces de rede local em barramento PCI padrão Ethernet 10/100/1000 Base-T com gerenciamento SNMP
- 2 Fontes de Alimentação operando de forma redundante

Quantidade proposta: 29 para CCD/BSB e 6 para CCD/SP.

11.3 SERVIDOR INTEL TIPO 3

- HP Proliant DL 380 G3 montado em rack
- 2 processadores Intel Xeon de 3.06 Ghz
- Barramento de sistema de 533 Mhz
- Memória cache de 512 Kb por processador
- Memória RAM de 2Gb ECC SDRAM

RQS nº 03/2005 - CN -
CPMI - CORREIOS
605
Fls Nº
3702
Doc:

- Controladora integrada Ultra 3 SCSI com suporte a RAID 0, 1, 0+1, 5
- 2 discos rígidos SCSI Ultra 3 de 10K rpm de 72,8 Gb – Hot Swap
- Controladora de vídeo SVGA integrada com 8Mb
- Uma unidade de CD-ROM IDE 24 X
- 2 interfaces de rede local em barramento PCI padrão Ethernet 10/100/1000 Base-T com gerenciamento SNMP
- 2 Fontes de Alimentação operando de forma redundante
- HP Proliant DL 380 G3 montado em rack

Quantidade proposta: 27 para CCD/BSB e 24 para CCD/SP.

11.4 SERVIDOR RISC TIPO 01

11 x Servidores RISC Tipo 01, marca HP, modelo SuperDome com a seguinte configuração por Servidor:

- 24 x CPU PA-RISC PA8700 de 875 MHz e 2,25 MB de memória cache L1
- 64 Gbytes de memória RAM
- 04 x Placa PCI Core I/O com uma interface 100 BT Ethernet
- 16 x Placa PCI com uma interface 10/100/1000BaseT Ethernet LAN
- 16 x Placa PCI com uma interface Fiber Channel de 2GB/s
- 08 x Placa PCI com duas interfaces U160 LVD/SE SCSI
- 04 x Placa PCI com 2 portas Ultra-2 SCSI e 2 portas 100BaseT
- 24 x licença de 1 CPU para HP-UX 11i
- 24 x licença de 1 CPU para HP-UX Virtual Partitions (vPar)
- 24 x licenças de 1 CPU para Online JFS
- 24 x licenças de 1 CPU para MirrorDisk/UX
- 06 fontes independentes e redundantes, configuradas para atender a capacidade máxima de expansão solicitada , com alimentação redundante através de 2 (dois) circuitos.
- 16 x Gabinete de disco HP SureStore DS2100 montados em rack
- 16 x Disco de 36GB 10K, para DS2100
- 02 x Gabinete para dispositivos HP SureStore TA5300 para rack
- 02 x HP SureStore DVD-ROM para TA5300
- 02 x HP SureStore DAT 24 DDS-3 para TA5300
- 40 x Fitas novas padrão DDS-3
- 08 x Fitas novas para limpeza.

Adicionais:

- 240 x licenças de 1 CPU para MC/ServiceGuard extensão para Oracle 9i Real Application Cluster - RAC ou Oracle 8i Parallel Server - OPS, permitindo a criação de até 10 partições ,em Servidores RISC Tipo 1, com Oracle 9i Real Application Cluster - RAC ou Oracle 8i Parallel Server - OPS.
- 144 x licenças de 1 CPU para Compilador C padrão ANSI C, totalizando a quantidade 6 servidores RISC Tipo 1 com compilador C padrão C/ANSI para número de usuários ilimitados.
- 09 x Rack HP de 41 U padrão 19"
- 04 x Console rp2470 ,2 (duas) para cada localidade, para gerenciamento de todos os equipamentos em cada localidade e criação/gerenciamento das partições

Observação: Para criação de uma partição virtual é necessário uma CPU, um disco de boot , 2 GB de memória e uma interface SCSI, desta forma, atendemos a capacidade de criação de no mínimo 8 partições lógicas, expansível a no mínimo 16 (dezesseis) partições lógicas.

Quantidade proposta: 8 para CCD/BSB e 3 para CCD/SP.

RQS nº 03/2005 - CN - CPMI - CORREIOS
0825
Fls Nº 606
Nº Doc: 3702

11.5 SWITCH TIPO 1

- Fabricante Cisco
- Modelo Catalyst 6513
- Descrição - Switch de núcleo, modular de 13 slots, interfaces Fast Ethernet e Giga Ethernet
- Software de Gerenciamento - CiscoWorks LAN Management Solution

Quantidade proposta: 2 para CCD/BSB e 2 para CCD/SP.

11.6 SWITCH TIPO 2

- Fabricante Cisco
- ModeloCatalyst 2950G-48EI
- Descrição - Switch de acesso, empilhável, 48 portas 10/100, uplink 1000Base-SX

Quantidade proposta: 4 para CCD/BSB e 2 para CCD/SP.

11.7 SWITCH TIPO 3

Quantidade proposta para CCD/BSB = 4

- 02 EMC Racks EC-1230B
- 04 (quatro) Directors Fibre Channel EMC Connectrix ED-12000B com 64 portas FibreChannel 2Gbit/s cada
- Total de 256 portas FibreChannel de 2Gbit/s
- 370 (trezentos e oito) cabos FibreChannel de 50 metros
- Software Fabric OS, Fabric Manager e Fabric Watch

Quantidade proposta para CCD/SP = 2

- 01 EMC Rack EC-1230B
- 02 (quatro) Directors Fibre Channel EMC Connectrix ED-12000B com 64 portas FibreChannel 2Gbit/s cada
- Total de 128 portas FibreChannel de 2Gbit/s
- 185 (cento e cinquent e quatro) cabos FibreChannel de 50 metros
- Software Fabric OS, Fabric Manager e Fabric Watch

11.8 SWITCH TIPO 4 (KVM)

Configuração proposta para BSB

- Fabricante BlackBox
- Modelo AFFINITY
- Total de 160 Portas
- 01 Rack BlackBox Padrão 19" 40 U de altura
- 08 Monitores Compaq S7500 17"
- 08 Teclados PS/2 ABNT2
- 08 Mouses PS/2

Configuração proposta para SP

- Fabricante BlackBox
- Modelo AFFINITY
- Total de 96 Portas
- 01 Rack BlackBox Padrão 19" 40 U de altura
- 04 Monitores Compaq S7500 17"
- 04 Teclados PS/2 ABNT2
- 04 Mouses PS/2

11.9 SWITCH TIPO 5

- Fabricante Cisco
- Modelo VPN 3060 Concentrador de VPN e Servidor de Autenticação ACS 3.2

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

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 607
Nº 3702
Doc:

- Descrição - Concentrador de VPN
- Software de Gerenciamento - CiscoWorks VPN/Security Management Solution (VMS)

Quantidade proposta: 1 para CCD/BSB e 1 para CCD/SP.

11.10 ROTEADOR TIPO 1

- Fabricante Cisco
- Modelo Router Cisco 3745
- Descrição - Roteador modular Multi-Serviço
- Software de Gerenciamento - CiscoWorks 2000 Routed WAN Management Solution

Quantidade proposta: 1 para CCD/BSB e 1 para CCD/SP.

11.11 ROTEADOR TIPO 2

- Fabricante Cisco
- Modelo Router Cisco 1751-V
- Descrição - roteador modular com suporte de Voz

Quantidade proposta: 2 para CCD/BSB.

11.12 UNIDADE DE BACKUP ROBOTIZADO

Para Brasília

- 2 (duas) Hp StorageWorks ESL9595 com:
- 400 Slots,
- 20 drives ultrium 460,
- 5 bridges modelo e2400-160 FC com 20 canais SCSI
- 1 (um) Pass-through para conecção das ESL9595
- 600 cartuchos
- 20 cartuchos de limpeza

Para São Paulo

- 1 (uma) Hp storageworks ESL9595 com:
- 400 Slots,
- 12 drives Ultrium 460,
- 3 bridges modelo e2400-160 FC com 12 canais SCSI
- 400 cartuchos
- 12 cartuchos de limpeza

11.13 SERVIDOR DE SEGURANÇA LÓGICA TIPO 1

- Fabricante Cisco
- Modelo PIX 535
- Descrição - Servidor de Firewall

Quantidade proposta: 2 para CCD/BSB e 2 para CCD/SP.

11.14 SERVIDOR DE SEGURANÇA LÓGICA TIPO 2

- Fabricante Cisco
- Modelo PIX 525
- Descrição - Servidor de Firewall

Quantidade proposta: 1 para CCD/BSB e 1 para CCD/SP.

11.15 SERVIDOR PARA DETECÇÃO DE INTRUSÃO

- Fabricante Cisco
- Modelo IDS 4250
- Descrição - Servidor de Detecção de Instrusão

Quantidade proposta: 1 para CCD/BSB e 1 para CCD/SP.

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

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 608
Doc: 3702

17.157
L

11.16 LICENÇAS DE CONCORD ENHANCED SYSTEMEDGE

- 107 licenças para os servidores INTEL
- 88 licenças para os servidores Risc

12. MODO DE APRESENTAÇÃO DA COMPROVAÇÃO DAS ESPECIFICAÇÕES EXIGIDAS NO EDITAL

O documento COMPROVAÇÃO DAS ESPECIFICAÇÕES TÉCNICAS está dividido em diversos cadernos de ANEXOS, de encadernação espiralada, na mesma ordem da tabela TIPO DE EQUIPAMENTO, do item 1, do ANEXO 1-B, do edital em questão.

12.1 SERVIDOR INTEL TIPO 1

Os documentos referentes a este item se encontram nos seguintes anexos:

- ANEXO INTEL
- ANEXO CONCORD SYSTEMEDGE PARTE 1
- ANEXO CONCORD SYSTEMEDGE PARTE 2

12.2 SERVIDOR INTEL TIPO 2

Os documentos referentes a este item se encontram nos seguintes anexos:

- ANEXO INTEL
- ANEXO CONCORD SYSTEMEDGE PARTE 1
- ANEXO CONCORD SYSTEMEDGE PARTE 2

12.3 SERVIDOR INTEL TIPO 3

Os documentos referentes a este item se encontram nos seguintes anexos:

- ANEXO INTEL
- ANEXO CONCORD SYSTEMEDGE PARTE 1
- ANEXO CONCORD SYSTEMEDGE PARTE 2

12.4 SERVIDOR RISC TIPO 1

Os documentos referentes a este item se encontra no seguinte anexo:

- ANEXO SERVIDOR RISC TIPO 01

12.5 SWITCH TIPO 01

Os documentos referentes a este item se encontra no seguinte anexo:

- ANEXO SWITCH TIPO 01 PARTE 1

12.6 SWITCH TIPO 02

Os documentos referentes a este item se encontra no seguinte anexo:

- ANEXO SWITCH TIPO 02 PARTE 1

12.7 SWITCH TIPO 03

Os documentos referentes a este item se encontra nos seguintes anexos: ANEXO SWITCH TIPO 03 PARTE 1, 2, 3A, 3B, 4A, 4B, 5, 6, 7, 8, 9, 10A, 10B, 11, 12, 13, 14A, 14B, 14C, 14D, 15A, 15B, 15C, 15D, 15E, 15F.

12.8 SWITCH TIPO 04

Os documentos referentes a este item se encontram no seguinte anexo:

- ANEXO INTEL

12.9 SWITCH TIPO 05

Os documentos referentes a este item se encontra no seguinte anexo:

RQS nº 03/2005 - CN - CPMI - CORREIOS
21/25
Fls Nº 609
Nº 3702
Doc:

- ANEXO SWITCH TIPO 05 PARTE 1

12.10 ROTEADOR TIPO 01

Os documentos referentes a este item se encontra no seguinte anexo:

- ANEXO ROTEADOR TIPO 01 PARTE 1

12.10 ROTEADOR TIPO 02

Os documentos referentes a este item se encontra no seguinte anexo:

- ANEXO ROTEADOR TIPO 02 PARTE 1

12.11 UNIDADE DE BACKUP ROBOTIZADO

Os documentos referentes a este item se encontra nos seguintes anexos: ANEXO UNIDADE DE BACKUP ROBOTIZADO A, B, C, D1, D2, D3, D4, D5, D6, D7, D8, D9, E1, E2, F, G1, G2, G3, H, I, J, K, L, M, N, O, P, Q, R, S, T, U.

12.12 SERVIDOR DE SEGURANÇA LÓGICA 01

Os documentos referentes a este item se encontra no seguinte anexo:

- ANEXO SERVIDOR DE SEGURANÇA LÓGICA 01 PARTE 1

12.13 SERVIDOR DE SEGURANÇA LÓGICA 02

Os documentos referentes a este item se encontra no seguinte anexo:

- ANEXO SERVIDOR DE SEGURANÇA LÓGICA 01 PARTE 1

12.14 SERVIDOR PARA DETECÇÃO DE INTRUSÃO

Os documentos referentes a este item se encontra no seguinte anexo:

- ANEXO SERVIDOR PARA DETEÇÃO DE INTRUSÃO PARTE 1, PARTE 2 e PARTE 3

12.15 SOFTWARES

Os documentos referentes a este item se encontra no seguinte anexo:

- ANEXO SOFTWARES

13. CONFORMIDADE COM REQUISITOS GERAIS

Todos os equipamentos ofertados são novos de fábrica e entregues acondicionados adequadamente em caixas fechadas, de forma a permitir completa segurança durante o transporte.

Serão entregues com todos os equipamentos os cabos, acessórios, manuais e documentações completas, que são necessários ao pleno funcionamento dos equipamentos, softwares e periféricos.

Não estão sendo consideradas para efeitos de somatório das quantidades mínimas exigidas, controladoras Fibre Channel e de Rede integradas na placa de sistema, nos "Servidores RISC Tipo 01".

Está sendo considerado para efeito de somatório, placa de rede Ethernet com até 2 (duas) interfaces por placa, na montagem da configuração dos "Servidores RISC Tipo 1".

Estamos ofertando o remanejamento de módulos de switch, interfaces de rede ou fibre channel entre os servidores fornecidos, a qualquer momento da vigência do Contrato, sem ônus adicionais.

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

RQS nº 03/2005 - CNT - CPMI - CORREIOS
Fls Nº 610
Doc: 3702

17.155
L

Todos os equipamentos ofertados são novos e possuem garantia de 48 (quarenta e oito) meses.

A COBRA prestará os serviços assistência técnica nos locais de instalação dos equipamentos, nas cidades de Brasília/DF e São Paulo/SP;
Os serviços prestados irão englobar a substituição de peças e componentes defeituosos dos equipamentos, bem como a depuração e resolução de problemas relacionados ao AMBIENTE OPERACIONAL fornecido pelo Correios.

Os equipamentos RISC Tipo 01 serão fornecidos com 8 (oito) partições lógicas (vPar) e sendo expansível a, no mínimo, 16 (dezesseis) partições lógicas (vPar).

O número especificado de partições é alcançado com a simples configuração de software fornecido para este fim, sem a necessidade de adição de nenhum hardware ou software adicionais. Estão sendo entregues 2 (duas) consoles rp2470 em Brasília e 2 (duas) consoles rp2470 em São Paulo para gerenciamento de todos os equipamentos em cada localidade e criação/gerenciamento das partições.

Os equipamentos "RISC Tipo 01" serão fornecidos com todos os recursos de hardware e software necessários à criação do número mínimo de partições especificadas para cada equipamento.

A Cobra Tecnologia fornecerá 4 notebooks para o CCD de Brasília e 1 notebook para o CCD de São Paulo do modelo EVO N1020v com as seguintes configuração:

- Processador Pentium IV 2.4GHz
- 256MB de memória RAM do tipo DDR (PC2100)
- Disco rígido de 30GB
- DVD-ROM
- Unidade de disquete 1.44MB
- Interface de Fax-Modem
- Interface de rede 10/100
- Tela de 15"
- 1 (uma) licença do agente 'Concord SystemEdge', devidamente instalado e configurado conforme orientação da equipe técnica dos Correios;
- Está sendo ofertado licenças de software agente de backup (HP Openview Data Protector) compatível com o gerenciador de fitoteca especificado no subitem 5.13, devidamente instalado e configurado conforme orientação da equipe técnica dos Correios.

A Cobra Tecnologia fornecerá e instalará, para todos os servidores RISC cotados adicionalmente, os seguintes componentes de hardware:

Os sevidores RISC adicionais estarão sendo fornecidos com 1 (uma) unidade interna de fita DDS 3. No fornecimento está previsto a entrega de 10 (dez) fitas DDS 3 novas e 2 (duas) fitas para limpeza para cada servidor RISC fornecido adicionalmente.
Toda a documentação será fornecida e catalogada conforme o exigido.
A Cobra Tecnologia disponibilizará todos os PRODUTOS necessários à implementação de uma estrutura de acesso remoto que permita a COBRA acesso a rede corporativa do Correios, utilizando o Switch Tipo 5 a ser fornecido.
Esta estrutura de acesso remoto será utilizada para que a Cobra Tecnologia possa prestar serviço de suporte remoto nas situações em que o Correios julgue necessária. A estrutura de acesso remoto seguirá estritamente as Normas de Segurança definidas pelo Correios.

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

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 611
Doc: 3702

Durante o Treinamento de Gerenciamento, descrito no Subitem 1.9.2.3. do ANEXO 1-A do edital, a COBRA instalará e configurará os novos agentes 'Concord SystemEdge', integrando conforme os padrões da plataforma de Gerência já existente do Correios;
A COBRA configurará os agentes 'Concord SystemEdge' para, entre outras coisas, medir o tempo de resposta dos serviços de infra-estrutura, não se limitando a: DNS, HTTP, HTTPS, SMTP, POP3, FTP e TCP;
A COBRA configurará os agentes 'Concord SystemEdge' para que monitore o desempenho e falhas das aplicações Exchange, Oracle, MS SQL, APACHE e IIS;
A COBRA habilitará o agente SNMP dos Roteadores, Switches e servidores fornecidos, conforme os padrões do Correios;
A COBRA configurará as ferramentas de gerenciamento existentes no Correios, não se limitando a:
Integração de eventos no HP OpenView Operations;
Criação e integração de regras inteligentes do Concord Live Health para envio de eventos ao HP OpenView Operations;
Criação e geração de relatórios do Concord eHealth.
O servidor "RISC Tipo 01" será fornecido com 64 Gbytes de memória RAM , instaladas, com possibilidade de expansão de no mínimo 128 Gbytes de memória RAM, e com disponibilidade de recursos para verificação e correção de erro.

O servidor "RISC Tipo 01" terá número de fontes instaladas suficiente para suportar a operação do equipamento na configuração máxima especificada.

- Serão fornecidos com os servidores "RISC Tipo 01" 16 (dezesseis) discos de 36GB, com funcionalidade de troca sem interrupção, com tempo médio de acesso de 5,2 ms com velocidade de rotação de 10.000 RPM.

- Serão fornecidos com os servidores "RISC Tipo 01" 8 (oito) controladoras de discos Ultra 2 SCSI ou superior, não incorporadas na placa de sistema.

Serão fornecidas com os servidores "RISC Tipo 01" 16 (dezesseis) controladoras FIBER CHANNEL, operando a 2Gb/s.

Serão fornecidas com os servidores "RISC Tipo 01" 16 (dezesseis) interfaces de rede padrão Ethernet PCI 10/100/1000 Base-T em conformidade com os padrões IEEE 802.3ab e 802.3u, com possibilidade de gerenciamento SNMP

Interfaces de rede que irão conectar os servidores a Rede do CCD utilizando cabeamento UTP CAT-6 e conectores RJ-45.
Serão fornecidos com os servidores "RISC Tipo 01" 4 (quatro) unidades de DVD-ROM e 4 (quatro) unidades leitora/gravadora de fitas DDS-3 por equipamento, totalizando 1 (uma) unidade de DVD-ROM e 1 (uma) unidade leitora/gravadora de fitas para cada conjunto de 2 (duas) partições
No fornecimento está previsto a entrega de 10 (dez) fitas novas, padrão DDS-3 e 2 (duas) fitas para limpeza para cada unidade leitora/gravadora de fitas.

Os servidores "RISC Tipo 01" serão fornecidos com o ambiente operacional HP-UX 64 bits, instalado e configurado para Rede dos Correios, com número ilimitado de usuários simultâneos, licenciado para cada uma das 8 (oito) partições do equipamento, contendo:

1 (uma) licença do agente 'Concord SystemEdge', devidamente instalado e configurado conforme orientação da equipe técnica dos Correios;

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

RQS nº 03/2005 - CN -
CPMI - CORREIOS
24 / 25
Fls Nº 612
Doc: 3702

1 (uma) licença de software agente de backup compatível com o gerenciador de fitoteca especificado no subitem 5.13, devidamente instalado e configurado conforme orientação da equipe técnica dos Correios

Serão fornecidas e instaladas as ferramentas, agentes e demais softwares que permitam a criação de ambientes clusterizados entre os equipamentos fornecidos. Para todos os servidores "RISC Tipo 01" foram incluídos os software MC/ServiceGuard extension for RAC, MirrorDisk UX e Online JFS.

Deverão ser montados dois ambientes de gerenciamento da Rede SAN, sendo um no CCD de Brasília e um no CCD de São Paulo.

14. RELAÇÃO DE PROFISSIONAIS ALOCADOS NO PROJETO ECT 050/2003

Nome	Produto	Telefone fixo	Telefone celular
Pedro Luiz Dias	Servidores RISC	(21) 2442-8888	(21) 9618-0743
Patrícia Abreu	Backup	(21) 2442-8639	(21) 9807-8362
Walter Fantoni	Servidores Intel	(21) 2442-8872	(21) 9431-7493
Euvaldo Dutra	Conectividade	(21) 2442-8960	(21) 9986-5575

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 613
Doc: 3702

SWITCH TIPO 1					
ATRIBUTO	REQUISITOS DO EDITAL	ATRIBUTOS OFERTADOS	ATRIBUTOS OFERTADOS ADICIONALMENTE	CONFIRMA ATENDIMENTO (SIM / NÃO)	PÁGINA DA DOCUMENTAÇÃO TÉCNICA
1- Características Físicas	Switch tipo Chassis	Cisco Catalyst 6513 chassis (13 slots)	N/A	SIM	Anexo 1 - pág. 23
2 - Gabinete	Chassis para ser instalado em Rack 19"	Dimensões (em polegadas) H=33.3, W=17.3, D=18.1	N/A	SIM	Anexo 1 - pág. 21
	Todos os módulos de interface, Fontes de Alimentação e Ventiladores devem ser do tipo Hot-Swappable ou Hot-Pluggable	Todos os módulos utilizados na configuração proposta são do tipo Hot-Swapping	N/A	SIM	Anexo 1 - pág. 2, 10, 20 - Anexo 2 - pág. 5 - Anexo 3 - pág 7 Anexo 1A - pág. 1-15 Anexo 30 - pág. 12
3 - Portas Gigabit-Ethernet	Mínimo de 192 portas 10/100/1000 compatíveis com o padrão IEEE 802.3ab, para cabos UTP cat. 6 e conectores RJ-45	Estão sendo fornecidas 192 portas 10/100/1000 compatíveis com o padrão IEEE 802.3ab, para cabos UTP cat. 6 e conectores RJ-45	N/A	SIM	Anexo 5 - pág. 1, 2, 17, 18 e 20
	Mínimo de 16 portas 1000SX compatíveis com o padrão IEEE 802.3z	Estão sendo fornecidas 16 portas 1000SX compatíveis com o padrão IEEE 802.3z	N/A	SIM	Anexo 3 - pág. 1, 3, 8 e 11 - Anexo 4 - pág. 1 e 3 (Ver quantidade nas propostas técnica e comercial)

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 614
Doc: 3702

OBRA
12.52

	Suportar a inclusão futura de mais 48 portas 10/100/1000Base-T	Foi deixado pelo menos um slot livre para inserção de mais um módulo WS-X6548-GE-TX	N/A	SIM	Ver quantidade de slots (13) versus placas fornecidas nas propostas Técnica e Comercial (12)
4 - Hot-Swapping	Deverá ser do tipo Hot-Swappable ou Hot-Pluggable em todos os módulos	Todos os módulos são do tipo Hot-Swapping ou/ Hot-Pluggable	N/A	SIM	Anexo 1 - pág. 2, 10, 20 - Anexo 2 - pág. 5 - Anexo 3 - pág 7 Anexo 1A - pág. 1-15
5 - Balanceamento de Carga	Balanceamento de carga baseado em Weighted Round Robin, Weighted Least Connections e URL Hashing	Todos os exigidos	N/A	SIM	Anexo 6 - pág 2
	Balanceamento baseado em protocolos das camadas 4 a 7, incluindo TCP,UDP,FTP,DNS,SMTP, HTTP e IPSec	Todos os exigidos	N/A	SIM	Anexo 6 - pág. 1, 2 e Anexo 9A - pág 2
	Capacidade de vincular conexões por meio de endereçamento IP da fonte, cookies e SSL	Todos os exigidos	N/A	SIM	Anexo 6 - pág. , 2
	Redundância via HSRP ou VRRP	Todos os exigidos	N/A	SIM	Anexo 3 - pág. 1 e Anexo 5 - pág. 2
	Capacidade para implementar QoS	Todos os exigidos	N/A	SIM	Anexo 6 - pág. 3
	Deverá suportar balanceamento global para servidores localizados em sites com diferentes saídas para internet	Conforme Edital	N/A	SIM	Anexo 6 - pág. 3

ECT
Doc: 3702
RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 615

17.151

7 - Gerenciamento	Suportar SNMP e MIB II conforme RFC 1213, bem como RMON I (mínimo de 04 grupos) e RMON II completo	Todos os exigidos	SNMP v1 e v2, SMON, DSMON e HC-MON	SIM	Anexo 7 - pág. 10 e 11
8 - Conectividade	Mínimo de 08 grupos de agregação com no mínimo 08 enlaces cada conforme padrão IEEE 802.3ad	Todos os exigidos	N/A	SIM	Anexo 7 - pág. 11 - Anexo 5 - pág. 18 - Anexo 3 - pág. 11 Anexo 31 - pág. 13-1 e 13-2
9 - Roteamento	Os Switches deverão realizar roteamento (Camada 3)	Conforme Edital	N/A	SIM	Anexo 3 - pág. 4 - Anexo 5 - pág. 6
10 - QoS	Os Switches deverão implementar um mínimo 04 filas de prioridade em cada porta , permitindo a priorização do tráfego de rede e integração transparente de dados, voz e vídeo através do protocolo IEEE 802.1p com CoS (Class of Service)	Conforme Edital	N/A	SIM	Anexo 3 - pág. 11 - Anexo 5 - pág. 1, 18 Anexo 32 - pág. 32-1, 32-3
	Instaladas na configuração máxima do equipamento com recurso de troca sem interrupção (Hot-Swappable ou Hot-Pluggable) e alimentação elétrica de acordo com a localidade onde serão instaladas e com frequência de 60Hz	Fontes de Alimentação totalmente Hot-Swappable, com frequência de operação de 60Hz	N/A	SIM	Anexo 1 - pág. 20 - Anexo 9 - pág. A-6

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 616
Doc: 3702

12150

11 - Fonte de Alimentação	Deverão ser redundantes por fontes internas independentes com alimentação redundante, de tal forma que em caso de falha de uma das fontes por defeito ou por falta de alimentação elétrica em um dos 02 (dois) circuitos, o equipamento continue a funcionar sem prejuízo das aplicações	Conforme Edital	N/A	SIM	Anexo 30 - pág. 9, 10, 12, 15 a 18
12 - Forwarding Performance	Deve possuir um mínimo de 100 Mpps para Layer 2, Layer 3 e Layer 4	Somatório do troughput do Supervisor module mais os módulos Gigabit Ethernet, montados com cartões DFC	Capacidade total de 105 Mpps em Layer 2, 3 e 4	SIM	Anexo 2 - pág. 4 Anexo 27 - pág. 1 Anexo 28 (todas as páginas)
	Implementar o protocolo STP para cada VLAN configurada (uma sessão STP por grupo de porta)	Conforme Edital	N/A	SIM	Anexi 1 - pág. 5, 25, 28 Anexo 33 - pág. 15-1, 15-2, 15-15 Anexo 35 - (todo o documento)
	Suportar múltiplos agrupamentos simultâneos de no mínimo 08 interfaces cada um em quaisquer interface de rede e em módulos diferentes de forma a agregar taxa de transmissão	Conforme Edital	N/A	SIM	Anexo 7 - pág. 11 - Anexo 5 - pág. 18 - Anexo 3 - pág. 11 Anexo 31 - pág. 13-1 e 13-2
	Deverá possuir a facilidade de trunking (IEEE 802.1Q) com outros Switches	Conforme Edital	N/A	SIM	Anexo 7 - pág. 11 - Anexo 5 - pág. 18 - Anexo 3 - pág. 11 Anexo 31 - pág. 13-1 e 13-2
13 - Gerais					

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 917
Doc: 3702

27.149

	Deverá ser capaz de implementar no mínimo duas sessões simultâneas de espelhamento de tráfego, entrada e saída de interfaces ou VLANs	Conforme Edital	N/A	SIM	Anexo 34 - pág. 34-1 até 34-8 - Anexo 35 (todo o documento)
	A CONTRATADA deverá fornecer ferramentas que permitam o gerenciamento dos equipamentos e de todas as suas interfaces através de aplicação gráfica	Conforme Edital	N/A	SIM	Ver propostas Técnica e Comercial (Softwares de Gerenciamento)
	Deverão ser fornecidos servidores adicionais para instalação dessa,e gerência	Conforme Edital	N/A	SIM	Ver propostas Técnica e Comercial (Servidores Intel)

SWITCH TIPO 2

ATRIBUTO	REQUISITOS DO EDITAL	ATRIBUTOS OFERTADOS	ATRIBUTOS OFERTADOS ADICIONALMENTE	CONFIRMA ATENDIMENTO (SIM / NÃO)	PÁGINA DA DOCUMENTAÇÃO TÉCNICA
1- Switch	Deverá ser do tipo Stackable (empilhável)	Conforme Edital	N/A	SIM	Anexo 14A - pág 1
	Deve permitir empilhamento de no mínimo 06 unidades por meio de links de no mínimo 1 Gbps redundantes, formando uma unidade gerenciável na rede através de um único endereço IP	Conforme Edital	Empilha até 09 unidades	SIM	Anexo 10 - pág. 2, 5, 7, 11 - Anexo 11 - pág. 1-1
	Deverão ser compatíveis com Rack 19¨ a ser fornecido	Conforme Edital	N/A	SIM	Anexo 14C (todas as páginas)

RQS nº 03/2005 - CN - CPM - CORREIOS
Fls Nº 6128
Doc: 3702

2- Interfaces Fast e Gigabit Ethernet	Possuir um mínimo de 48 portas 10/100TX , UTP, categoria 6, RJ-45 + 02 duas portas para interfaces de empilhamento e uplink	Conforme Edital	N/A	SIM	Anexo 10 - pág. 14, 17 - Anexo 11 - Anexo 10A
	Sinalização visual de funcionamento e de status das portas.	Conforme Edital	N/A	SIM	Anexo 10 - pág. 10 - Anexo 14 pág.10
	Compatível com os padrões IEEE 802.3u, IEEE 802.3Q e IEEE 802.3p.	Conforme Edital	N/A	SIM	Anexo 10 - pág. 14
	Deverá ser capaz de implementar espelhamento de tráfego de entrada e saída de interfaces ou de VLANs	Conforme Edital	N/A	SIM	Anexo 10B (todo o documento)
	Gerenciável via SNMP, com suporte a MIB II conforme RFC 1213 e 04 grupos de RMON.	Conforme Edital	N/A	SIM	Anexo 10 - pág. 1, 10, 13
	Controle de Broadcast Storm	Conforme Edital	N/A	SIM	Anexo 10 - pág. 7
	Suporte a protocolo que permita limitar tráfego de IP Multicast.	Suporte a IGMP Snooping por hardware	N/A	SIM	Anexo 10 - pág. 5
	Deve implementar no mínimo 04 filas de prioridade em cada porta, permitindo a priorização do tráfego de rede e uma integração transparente de dadso, voz e vídeo através do protocolo IEEE 802.1p com CoS (Class of Services).	Conforme Edital	N/A	SIM	Anexo 10 - pág. 4, 14 Anexo 14 - pág 3
	Deverá possuir kits de fixação para instalação em racks de 19¨ e cabos de ligação lógica e elétrica necessária à instalação e perfeito funcionamento	Conforme Edital	N/A	SIM	Anexo 14C - pág. 2-9
3 - Gerais					

RQS nº 03/2005 - CN - CPMI CORREIOS
Fls- Nº 619
Doc: 3702

7

Deverão ser fornecidos todos os acessórios necessários à composição do empilhamento do Switch, tais como cabos, conectores e interfaces	Conforme Edital (Os cabos para empilhamento (50cm) são parte integrante das GBIC)	N/A	SIM	Anexo 14B - pág. 5 Ver propostas Técnica e Comercial
Deverá implementar no mínimo, 200 VLANs no padrão IEEE 802.1Q, inclusive no empilhamento, isto é, deverá permitir o agrupamento em VLANs de portas de quaisquer Switches da pilha.	Conforme Edital	N/A	SIM	Anexo 14 - pág 4, 12 Anexo 14D (todas as páginas)
Deverá implementar o protocolo STP (Spanning Tree Protocol) para cada VLAN configurada (uma sessão STP por grupo de portas)	Conforme Edital	N/A	SIM	Anexo 10 - pág. 2, 7, 8 - Anexo 14 - pág 7, 12 - Anexo 14E e Anexo 14F
Deverá possui barramento para empilhamento igual ou superior a 1 Gbps	Conforme Edital	N/A	SIM	Anexo 10 - pág. 11
A CONTRATADA deverá fornecer ferramentas que permitam o gerenciamento dos equipamentos e de todas as suas interfaces através de aplicação gráfica. Também deverão ser fornecidos servidores adicionais para instalação dessa gerência	Conforme Edital	N/A	SIM	Ver propostas Técnica e Comercial (Softwares de Gerenciamento)
Alimentação elétrica de acordo com a localidade onde serão instalados os equipamentos e frequência de 60Hz	Redundante interna ou externa independente. Frequência = 60Hz	N/A	SIM	Anexo 10 - pág. 16 - Anexo 13 - pág. 1, 3 e 4

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 6190
Doc: 3702

4 - Fonte de Alimentação	As fontes de alimentação deverão ser redundantes por fontes internas ou externas independentes com alimentação redundante de tal forma que, em caso de falha de uma das fontes por defeito ou por falta de alimentação elétrica em um dos 02 circuitos, o equipamento continue a funcionar sem prejuízo das aplicações	Conforme Edital	N/A	SIM	Anexo 13 - (todas as páginas)

SWITCH TIPO 5 **Concentrador de VPNs**

ATRIBUTO	REQUISITOS DO EDITAL	ATRIBUTOS OFERTADOS	ATRIBUTOS OFERTADOS ADICIONALMENTE	CONFIRMA ATENDIMENTO (SIM / NÃO)	PÁGINA DA DOCUMENTAÇÃO TÉCNICA
1- Descrição	Deverá operar como concentrador de VPN, devendo ser composto por sistema integrado de hardware e software, com o objetivo de concentrar, configurar e monitorar acessos remotos via VPN	A solução está composta por um concentrador de VPNs (Cisco 3060) e um servidor de autenticação com software Cisco Secure ACS 3.2 (Cisco CSACSE-1111-K9)	N/A	SIM	Anexo 15 - pág. 1 Anexo 15B (todas as páginas) Ver propostas Técnica e Comercial
	Capacidade de Firewall	Capacidade de Firewall	N/A	SIM	Anexo 15 - pág. 4
	Suporte aos protocolos de tunelamento PPTP, IPSec, L2TP, L2TP/IPSec for Windows 2000 e NAT transparent IPSec	Todos os exigidos	N/A	SIM	Anexo 15 - pág 5
	O suporte a serviços deve ser estendido a todo e qualquer serviço que funcione sobre o protocolo IP, com a possibilidade de customização	Conforme Edital	N/A	SIM	Anexo 15C (todas as páginas)

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 6211
Doc 3702

2- Características e Funcionalidades do Sistema	Suporte a certificados digitais padrão X 509v3	Todos os exigidos	N/A	SIM	Anexo 15 - pág. 7
	Capacidade de tolerância a falhas (failover)	Todos os exigidos	N/A	SIM	Anexo 15 - pág. 4
	Suporte ao gerenciamento de chaves tipo IKE	Todos os exigidos	N/A	SIM	Anexo 15 - pág. 6
	Capacidade de registrar eventos e de envio de notificações por e-mail	Todos os exigidos	N/A	SIM	Anexo 15 - pág. 6
	Suporte aos protocolos de roteamento RIP, RIP2, OSPF e estático	Todos os exigidos	N/A	SIM	Anexo 15 - pág. 6
	Permitir aplicação de configurações e políticas de acesso	Todos os exigidos	N/A	SIM	Anexo 15F - pág. 14-1
	Possuir no mínimo 03 interfaces 10baseT	Conforme Edital	Possui 03 interfaces 10/100TX já montadas no equipamento	SIM	Anexo 15 - pág. 5
	O sistema deverá se integrar com um sistema de autenticação externa	Conforme Edital	N/A	SIM	Anexo 15D (todas as páginas) e Anexo 15E (todas as páginas)
	Capacidade para autenticação de no mínimo 5000 usuários	Até 5000 sessões simultâneas	N/A	SIM	Anexo 15 - pág. 2
	Suporte ao padrão LDAP	Todos os exigidos	N/A	SIM	Anexo 15 -pág. 7
	Integração com o domínio Microsoft Windows	Todos os exigidos	N/A	SIM	Anexo 15 - pág. 1
	Permitir configuração de níveis de acesso administrativos	Todos os exigidos	N/A	SIM	Anexo 15 - pág. 4
	Permitir a configuração de poíticas de segurança nas estações clientes	Conforme Edital	N/A	SIM	Anexo 16B
	Capacidade de gerenciamento de política para usuários e grupos	Todos os exigidos	N/A	SIM	Anexo 15 - pág. 7
	Controle de tempo e horário de acesso do usuário	Todos os exigidos	N/A	SIM	Anexo 15- pág. 7

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 622
Doc:

17.144
2

3 - Características e Funcionalidades do Software Cliente VPN	Suporte ao gerenciamento utilizando SNMP MIB II	Todos os exigidos	N/A	SIM	Anexo 15 - pág. 6
	Oferecer ferramentas de gerenciamento que possibilite a verificação de estatísticas de tráfego criptografado, negociações de handshake e resposta a pacotes	Conforme Edital	N/A	SIM	Anxo 16A pág. 17-2
	Possibilidade de crescimento (escalabilidade) conforme demanda, com configuração e gerência centralizadas	Conforme Edital	N/A	SIM	Anexo 16 (todas as páginas)
	Capacidade de geração de relatórios gerenciais	Conforme Edital	N/A	SIM	Anexo 16C (todas as páginas)
	Sistema de gerenciamento em Hardware do tipo Servidor	Conforme Edital	N/A	SIM	Anexo 16D (todas as páginas)
	Número mínimo de 5.000 licenças	Todos os exigidos	Sem limite de liceças	SIM	Anexo 15 - pág. 3
	Auto-atualização	Conforme Edital	N/A	SIM	Anexo 16E (todas as páginas) - Anexo 16F (todas as páginas) - Anexo 16G (todas as páginas)
	Suporte aos Sistemas Operacionais Windows 95, 98, ME, NT 4.0, 2000 e XP	Todos os exigidos	N/A	SIM	Anexo 15 - pág. 1
	Interface padronizada com o Logotipo da Contratada	Conforme Edital	N/A	SIM	Ver propostas Técnica e Comercial
4 - Características de Desempenho	Capacidade de tratar no mínimo 5000 usuários ao mesmo tempo	Capacidade para 5000 usuários simultâneos	N/A	SIM	Anexo 15 - pág. 2
	Capacidade de processamento de encriptação mínima de 100Mbps	Encryption Troughput	N/A	SIM	Anexo 15 -pág. 3

ECT - DR/DF
Doc. 2702
Fls. 623
SCS nº 03/2005 - CN - CPMI - CORREIOS

1.7.143

5 - Fonte de Alimentação	Instalada na configuração máxima do equipamento	Conforme Edital	N/A	SIM	Anexo 15 (todas as páginas)
	Hot-Swappable / Hot-Pluggable	Conforme Edital	N/A	SIM	Ver Carta do Fabricante
	Deverá possuir alimentação elétrica de acordo com a localidade ond serão instalados os equipamentos e operar na frequência de 60Hz	Voltagem de entrada de 100 a 240 VAC - 50/60 Hz	N/A	SIM	Anexo 15 - pág. 8
	As fontes de alimentação deverão ser redundantes por fontes internas independentes, com alimentação redundante	Conforme Edital	N/A	SIM	Anexo 15 (todas as páginas)

ROTEADOR TIPO 1

ATRIBUTO	REQUISITOS DO EDITAL	ATRIBUTOS OFERTADOS	ATRIBUTOS OFERTADOS ADICIONALMENTE	CONFIRMA ATENDIMENTO (SIM / NÃO)	PÁGINA DA DOCUMENTAÇÃO TÉCNICA
1 - Router	Possuir estrutura de Chassis modular com pelo menos 04 slots para inserção de módulos e interfaces	Rack-mountable chassis - 04 slots para módulos de rede	N/A	SIM	Anexo 17 - pág. 1, 2 e 3
	Deverá ser montado em Rack de 19"	Montável em Rack de 19"	Pode ser montado opcionalmente em Rack de 23	SIM	Anexo 17 - pág. 3, 11
2 - Processamento	Possuir capacidade de roteamento de pelo menos 225.000 pps utilizando pacotes de 64 bytes	Performance de 225 Kpps	N/A	SIM	Anexo 17 - pág. 11 Ver Carta do Fabricante
	Possuir no mínimo 03 interfaces 10/100TX, fast Ethernet, Full Duplex, para cabos UTP categoria 5, com conectores tipo RJ-45	02 portas 10/100 integradas + 01 porta no módulo NM-1FE2W	N/A	SIM	Anexo 17 - pág. 3 e Anexo 18 - pág. 3

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 624
Doc: 3702

AJ-142

3 - Interfaces	Possuir no mínimo 08 interfaces síncronas V.35 de alta velocidade (atpe 2Mbps)	Foram colocados 02 cartões tipo WIC-2T, cada um com duas portas de WAN, perfazendo um total de 08 portas	N/A	SIM	Anexo 17 - pág. 2 e Anexo 19 - pág. 3
	Possuir no mínimo 02 interfaces ATM E3, compatível com o padrão ITU-T G703	Conforme Edital	N/A	SIM	Anexo 17A - pág. 5
	Possuir no mínimo 01 interface Gigabit Ethernet 1000BaseT	Foi colocada uma porta tipo GBIC, part-number WS-G5483	N/A	SIM	Ver propostas Técnica e Comercial
	Possuir MTBF de pelo menos 50.000 horas	Conforme Edital	N/A	SIM	Ver Carta do Fabricante
	Permitir o gerenciamento através de aplicação gráfica	Conforme Edital	N/A	SIM	Ver propostas Técnica e Comercial (Softwares de Gerenciamento)
	Implementar o protocolo SNMP, incluindo a geração de traps	Conforme Edital	N/A	SIM	Anexo 19B - pág. 14 Anexo 19C (todas as páginas)
	Gerenciável através do protocolo SNMP, com suporte a MIB II, conforme RFC 1213	Conforme Edital	N/A	SIM	Anexo 19D - pág. 10
	Possuir descrição completa da MIB implementada no equipamento, inclusive as extensões privadas se existirem	Conforme Edital	N/A	SIM	Anexo 19D - pág. 5, 7, 8, 9, 10
	Implementar TELNET para acesso a interface da linha de comando	Conforme Edital	N/A	SIM	Anexo 19D - pág. 12
	Implementar protocolo SSH	Conforme Edital	N/A	SIM	Anexo 19B - pág. 13
	Possuir proteção contra ataques de Denial of Services do tipo TCP SYN attack	Conforme Edital	N/A	SIM	Anexo 19E (todas as páginas)

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 625
Doc: 3702

17.41

4 - Geral	Implementar IPSec padrão IETF com criptografia Triple DES	Todos os exigidos	AES (Advabced Encryption Standard)	SIM	Anexo 17 - pág. 5
	Suporte para SYSLOG externo que deverá ser dimendionado e fornecido em hardware à parte	Conforme Edital	N/A	SIM	Anexo 17 (todas as páginas) Anexo 19D (todas as páginas) Anexo 19 (todas as páginas) Anexo 19H (todas as páginas)
	Permitir a atualização de softwares utilizados no equipamento, através da Rede	Todos os exigidos	N/A	SIM	Anexo 19F (todas as páginas)
	Implementar mecanismo de autenticação para acesso ao equipamento, baseado em servidor de autenticação / autorização do tipo RADIUS ou TACACS	Conforme Edital	N/A	SIM	Anexo 19B - pág. 12, 15
	Proteger a interface de comando do equipamento, através de senha	Conforme Edital	N/A	SIM	Anexo 19 (todas as páginas) Anexo 19B (todas as páginas) Anexo 19D (todas as páginas) Anexo 19H (todas as páginas)
	Implementar o potocolo VRRP ou similar, em todas as interfaces disponibilizadas	Conforme Edital	N/A	SIM	Anexo 19B - pág. 15
	Implementar o protocolo PIM para roteamento de Multicast	Conforme Edital	N/A	SIM	Anexo 19B - pág. 11
	Implementar roteamento IP usando os protocolos OSPF, RIP, RIP II e BGP4	Conforme Edital	N/A	SIM	Anexo 19D (todas as páginas)
	Implementar DHCP	Conforme Edital	N/A	SIM	Anexo 19B - pág. 3, 4

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 6262
Doc: 3702

Permitir a configuração de pelo menos 1024 rotas estáticas	Conforme Edital	N/A	SIM	Ver Carta do Fabricante
Implementar Pollicy-based routing	Conforme Edital	N/A	SIM	Anexo 19I (todas as páginas)
Implementar filtros para redistribuição de rotas entre RIP, OSPF e BGP4	Conforme Edital	N/A	SIM	Anexo 19B - pág. 2, 11, 12 - Anexo 19G (todas as páginas)
Implementar as seguintes características para o protocolo BGP4: Route Reflectors, Route Confederations, Route Aggregation, IGP Synchronization e Route Flap Dampening	Conforme Edital	N/A	SIM	Anexo 19H (todas as páginas)
Permitir a configuração de Policy-based routing baseado no endereço de origem da rede	Conforme Edital	N/A	SIM	Anexo 19I (todas as páginas)
Suporta a implementação de NAT	Conforme Edital	N/A	SIM	Anexo 19B - pág. 10
Deverá suportar inserção em rede com servidores de VOIP e VOFR	Conforme Edital	N/A	SIM	Anexo 19B - pág. 16
Deverá suportar os protocolos G.711 e G.729 para o tráfego de voz e funcionar como Gateway H.323	Conforme Edital	N/A	SIM	Anexo 19B - pág. 6 Anexo 19J - pág. 1, 7, 8
Servidores adicionais para instalação da gerência	Conforme Edital	N/A	SIM	Ver propostas Técnica e Comercial
Instalada na configuração máxima do equipamento	Conforme Edital	N/A	SIM	Anexo 19K (todas as páginas)
Hot-Swappable / Hot-Pluggable	Conforme Edital	N/A	SIM	Anexo 17

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 627
3702

1739

5 - Fonte de Alimentação	Deverá possuir alimentação elétrica de acordo com a localidade onde serão instalados os equipamentos, na frequência de 60Hz	Conforme Edital	N/A	SIM	Anexo 19K (todas as páginas)
	Fontes redundantes internas e independentes com alimentação redundante	Conforme Edital	N/A	SIM	Anexo 19K (todas as páginas) Anexo 17 - pág. 12

ROTEADOR TIPO 2

ATRIBUTO	REQUISITOS DO EDITAL	ATRIBUTOS OFERTADOS	ATRIBUTOS OFERTADOS ADICIONALMENTE	CONFIRMA ATENDIMENTO (SIM / NÃO)	PÁGINA DA DOCUMENTAÇÃO TÉCNICA
1 - Router - Processamento	Capacidade mínima de 12Kpps	Capacidade de até 12.500pps	N/A	SIM	Anexo 21 - pág. 2
	Montado em bandejas instaladas no interior do Rack 19"	Serão montados em bandejas internas oferecidas juntamente com o Rack 19"	N/A	SIM	Ver Racks de 19" a serem fornecidos pela CONTRATADA
2 - Gerenciamento	Deverá ser gerencial via SNMP v1, v2 e v3, TELNET e acesso local.	Gerenciável por qualquer ferramenta SNMP	N/A	SIM	Anexo 20 - pág. 5 e 6 Anexo 20A - pág. 311 Anexo 20B - pág. 2
	Deverá possuir suporte a MIB II RFC 1213	Conforme Edital	N/A	SIM	Anexo 20A - pág.311
3 - Interfaces	Possuir no mínimo 01 interface Ethernet 10BaseT/100BaseTX, auto-negociável, integrada ao chassis, com conectores tipo RJ-45	Conforme Edital	N/A	SIM	Anexo 20 - pág. 2, 10
	Possuir no mínimo 02 intrfaces seriais, sendo uma do tipo DCE e outra do tipo DTE, com conectores do tipo V.35 ou EIA/TIA-232, com compressão e encriptação de dados	Conforme Edital	N/A	SIM	Anexo 19 - pág. 3 Anexo 20C (todas as páginas)

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 628
Doc: 3702

17.138
7

4- Gerais	Cabos e acessórios	Estão contemplados todos os cabos e acessórios pertinentes	N/A	SIM	Anexo 22 - pág. 1-11
	Sinalização visual do funcionamento e "status"das portas	Led´s indicativos para status e funções	N/A	SIM	Anexo 22 - pág. 1-4 até 1-9
	Atualização de softwares pela rede	Conforme Edital	N/A	SIM	Anexo 19I (todas as páginas)
	Suportar e implementar recursos de QoS avançados tais como: CAR, Custom, Low Latency Fair Queueing e WFQ, BoD, RSVP, WRED, Policy based Routing (FRF.12) e cRTP	Conforme Edital	N/A	SIM	Anexo 20 - pág. 7 e 17
	Implementar e permitir o roteamento entre VLANs suportando o padrão IEEE 802.1Q	Conforme Edital	N/A	SIM	Anexo 20 - pág. 7
	Permitir VPN Tunneling com IPSec, L2TP e L2F	Conforme Edital	N/A	SIM	Anexo 20 - pág. 6
	Permitir roteamento IP usando os protocolos OSPF, RIP, RIPv2 e BGP4, PIM-DM e PIM-SM	Conforme Edital	N/A	SIM	Anexo 20D - pág. 6, 7
	Suporte a criptografia 3DES	Conforme Edital	N/A	SIM	Anexo 20 - pág. 6
	Suporte a autenticação através dos protocolos RADIUS, TACACS+ e PAP/CHAP	Conforme Edital	N/A	SIM	Anexo 20 - pág. 6
	Suportar inserção em redes com serviços de VOIP e VOFR	Conforme Edital	N/A	SIM	Anexo 20 - pág. 17
	Funcionalidades de Firewall, incluindo ACL e AAA, criptografia, VPN Tunnel Server integradas ao roteador	Conforme Edital	N/A	SIM	Anexo 20D - pág. 1 Anexo 20 - pág 1, 4, 6, 7, 8
	Suportar Digital Voice, e voz analógica na infra-estrutura telefônica existente	FXO, FXS, E&M	N/A	SIM	Anexo 21 - pág 2 Anexo 20 - pág 3

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 629
Doc: 3792

17.137

Possuir duas interfaces do tipo FXS para conexão de telefones analógicos e 02 interfaces do tipo FXO para conexão em interfaces de ramal de PABX	Foram colocadas interfaces do tipo VIC-2FXO e VIC-2FXS, fornecendo as portas requeridas	N/A	SIM	Anexo 23 e Anexo 24 Ver propostas Técnica e Comercial
Entrada entre 90 e 240 Volts, com comutação automática e frequência de 60 Hz	Conforme Edital	N/A	SIM	Ver Carta do fabricante

Servidor de Segurança Lógica - Tipo 1

PIX535

ATRIBUTO	REQUISITOS DO EDITAL	ATRIBUTOS OFERTADOS	ATRIBUTOS OFERTADOS ADICIONALMENTE	CONFIRMA ATENDIMENTO (SIM / NÃO)	PÁGINA DA DOCUMENTAÇÃO TÉCNICA
	Operar como Firewall, sendo formado por no mínimo por dois módulos que deverão integrar-se aos dois Switches Tipo 1 a serem instalados em BSB e dois módulos que deverão integrar-se aos dois Switches Tipo 1 a serem instalados em SPO	Foram utilizados dois Servidores PIX535, externos aos Switches tipo 1	N/A	N/A	N/A

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 630
Nº 3702

17.136

1 - Descrição	Será permitida a utilização de servidores, em substituição aos módulos, considerando-se a razão de um par de servidores em substituição a um módulos. Os servidores deverão trabalhar em pares , com o objetivo de manter a alta disponibilidade do sistema	Conforme Edital Foram utilizados dois Servidores PIX535, externos aos Switches tipo 1	N/A	SIM	Ver propostas Técnica e Comercial
	O produto tem que oferecer controle de acesso, permitindo-se atender a uma política de segurança, definindo o tipo de tráfego que pode entrar/sair das redes protegidas por ele.	Conforme Edital	N/A	SIM	Anexo 29 - pág. 1, 2
	Autenticação	Conforme Edital	N/A	SIM	Anexo 29 - pág. 4
	NAT 1-1 e NAT 1-n	Conforme Edital	N/A	SIM	Anexo 29 - pág. 4
	Segurança de conteúdo (antivírus, checagem de URL e Java/ActiveX	Conforme Edital	N/A	SIM	Anexo 40 - pág. 1 Anexo 41 - pág. 1 Anexo 42 - pág. 1
	Auditoria	Conforme Edital	N/A	SIM	Anexo 29 - pág. 3
	Disponibilidade. No caso de falha, uma segunda máquina ou módulo deve assumir o controle de forma transparente ao usuário (Stateful Firewall Failover)	Conforme Edital	N/A	SIM	Anexo 29 - pág. 6
	Gerar alertas em tempo real por meio de e-mail quando se tentar violar a política de segurança	Conforme Edital	N/A	SIM	Anexo 43 - pág. 1

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 631
Doc: 3702

2 - Características e Funcionalidades	Proteção baseada no algoritmo de segurança adaptável (ASA - Adaptive Secure Algorithm) ou compatível, que ofereça um firewall orientado à conexão com classificação	Conforme Edital	N/A	SIM	Anexo 29 - pág. 1
	Prevenção contra ataques de negação de serviço (Denial-of-Service)	Conforme Edital	N/A	SIM	Anexo 29 - pág. 2
	Suporte à aplicações Multimídia	Conforme Edital	N/A	SIM	Anexo 29 - pág. 1
	Suporte à gerência de Listas de Acesso em roteadores	Conforme Edital	N/A	SIM	Anexo 44 (todas as páginas) Anexo 45 (todas as páginas) Anexo 46 (todas as páginas)
	Configuração e gerência centralizada em cada um dos sites	Conforme Edital	N/A	SIM	Anexo 29 (todas as páginas)
	Capacidade de gerenciamento remoto	Conforme Edital	N/A	SIM	Anexo 29 (todas as páginas)
	Suporte de serviços estendido para todo o protocolo IP, com possibilidade de customização	Conforme Edital	N/A	SIM	Anexo 48 (todas as páginas) Anexo 49 (todas as páginas)
	A Interface deve permitir a visualização da política de segurança definida, com opção de ocultar e visualizar grupos de regras desejados e o diagrama da rede protegida	Conforme Edital	N/A	SIM	Anexo 49 (todas as páginas) Anexo 50 (todas as páginas)
	Capacidade de gerar relatóros gerenciais, com informações sobre estatísticas de tráfego, regras mais utilizadas e etc.	Conforme Edital	N/A	SIM	Anexo 51 (todas as páginas)

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 632
Doc: 3702

12.134

	Suportar integração com produtos para sistemas de inspeção de conteúdo (HTTP, FTP, SMTP) de terceiros e suporte ao protocolo H.323	Conforme Edital	N/A	SIM	Anexo 52 - pág. 4-6, 4-8, 4-9, 4-13
	O produto deverá integrar-se perfeitamente com o Sistema para Detecção de Intruso oferecido	Conforme Edital	N/A	SIM	Anexo 29 - pág. 4
	Suportar autenticação de usuário, autenticação de sessão e autenticação de cliente, bem como interagir com sistemas de autenticação RADIUS e TACACS	Conforme Edital	N/A	SIM	Anexo 29 (todas as páginas)
	O sistema de gerenciamento de Firewalls deverá ser disponibilizado pela CONTRATADA em hardware à parte, sendo um sistema em BSB e um sistema em SPO, podendo ser integrado em um mesmo frame work de gerenciamento dos servidores para Detecção de Intrusos, Switch tipo 6 e roteaor tipo 1.	Conforme Edital Foram disponibilizados dois servidores Intel para o gerenciamento. Um em BSB e outro em SPO	N/A	SIM	Ver propostas Técnica e Comercial
3 - Características de Desempenho	Capacidade de tratar no mínimo 400.000 conexões simultâneas	Conforme Edital	N/A	SIM	Anexo 29 - pág. 6
	Capacidade de processamento superior a 1.5 Gbps em texto claro	Conforme Edital	N/A	SIM	Anexo 29 - pág. 6
4 - Configuração Física do Equipamento	Em caso de fornecimento de equipamentos externos ao Switch tipo 1, estes deverão possuir no mínimo 06 interfaces 10/100TX e 02 interface 1000BaseSX	Conforme Edital	N/A	SIM	Anexo 29 - pág. 6 Anexo 54 (todas as páginas) Anexo 55 (todas as páginas)

RDS nº 03/2005 - CN - CORREIOS
Fls Nº 633
Doc: 3202

17.133

5- Características Adicionais	Todo o ambiente de Firewall deverá ser acompanhado de documentação de instalação e configuração	Conforme Edital	N/A	SIM	A CONTRATADA se responsabilizará por toda a documentação de instalção e configuração
	Possuir alimentação elétrica de acordo com a localidade onde serão instalados os equipamentos, com frequência de 60Hz	Conforme Edital	N/A	SIM	Anexo 29 - pág. 7

Servidor de Segurança Lógica - Tipo 2

PIX525

ATRIBUTO	REQUISITOS DO EDITAL	ATRIBUTOS OFERTADOS	ATRIBUTOS OFERTADOS ADICIONALMENTE	CONFIRMA ATENDIMENTO (SIM / NÃO)	PÁGINA DA DOCUMENTAÇÃO TÉCNICA
1 - Descrição	Operar como Firewall, devendo ser formados por pares de máquinas, com cada par trabalhando em conjunto, com o objetivo de manter a alta disponibilidade do sistema: Um par deverá ser instalado em BSB e um par deverá ser instalado em SPO	Conforme Edital	N/A	SIM	Anexo 53 - pág. 1
	Oferecer controle de acesso permitindo atendimento a política de segurança, definindo o tipo de tráfego de entrada e saída da rede, protegida po ele	Conforme Edital	N/A	SIM	Anexo 53 (todas as páginas)
	Autenticação	Conforme Edital	N/A	SIM	Anexo 53 - pág. 4
	NAT 1-1 e NAT 1-n	Conforme Edital	N/A	SIM	Anexo 53 - pág. 4

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 634
Doc:

17.132

17.132

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 635
Nº 3702
Doc:

Segurança de conteúdo (antivírus, checagem de URL e Java/ActiveX	Conforme Edital	N/A	SIM	Anexo 40 - pág. 1 Anexo 41 - pág. 1 Anexo 42 - pág. 1
Auditoria	Conforme Edital	N/A	SIM	Anexo 53 - pág. 3
Gerenciamento Corporativo, permitindo que vários equipamentos sejam gerenciados de uma única console	Conforme Edital	N/A	SIM	Anexo 53 - pág. 6
Disponibilidade. No caso de falha, uma segunda máquina ou módulo deve assumir o controle de forma transparente ao usuário (Stateful Firewall Failover)	Conforme Edital	N/A	SIM	Anexo 43 - pág. 1
Gerar alertas em tempo real por meio de e-mail quando se tentar violar a política de segurança	Conforme Edital	N/A	SiM	Anexo 53- pág. 1
Proteção baseada no algoritmo de segurança adaptável (ASA - Adaptive Secure Algorithm) ou compatível, que ofereça um firewall orientado à conexão com classificação	Conforme Edital	N/A	SIM	Anexo 53 - pág. 2
Prevenção contra ataques de negação de serviço (Denial-of-Service)	Conforme Edital	N/A	SIM	Anexo 53 - pág. 1
Suporte à aplicações Multimídia	Conforme Edital	N/A	SIM	Anexo 44 (todas as páginas) Anexo 45 (todas as páginas) Anexo 46 (todas as páginas)
Suporte à gerência de Listas de Acesso em roteadores	Conforme Edital	N/A	SIM	Anexo 53 (todas as páginas)

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 636
Doc: 3702

17.130

2 - Características e Funcionalidades	Configuração e gerência centralizada em cada um dos sites	Conforme Edital	N/A	SIM	Anexo 53 (todas as páginas)
	Capacidade de gerenciamento remoto	Conforme Edital	N/A	SIM	Anexo 48 (todas as páginas) Anexo 49 (todas as páginas)
	Suporte de serviços estendido para todo o protocolo IP, com possibilidade de customização	Conforme Edital	N/A	SIM	Anexo 49 (todas as páginas) Anexo 50 (todas as páginas)
	A Interface deve permitir a visualização da política de segurança definida, com opção de ocultar e visualizar grupos de regras desejados e o diagrama da rede protegida	Conforme Edital	N/A	SIM	Anexo 51 (todas as páginas)
	Capacidade de gerar relatóros gerenciais, com informações sobre estatísticas de tráfego, regras mais utilizadas e etc.	Conforme Edital	N/A	SIM	Anexo 52 - pág. 4-6, 4 8, 4-9, 4-13
	Suportar integração com produtos para sistemas de inspeção de conteúdo (HTTP, FTP, SMTP) de terceiros e suporte ao protocolo H.323	Conforme Edital	N/A	SIM	Anexo 53 - pág. 4
	O produto deverá integrar-se perfeitamente com o Sistema para Detecção de Intruso oferecido	Conforme Edital	N/A	SIM	Anexo 53 (todas as páginas)
	Suportar autenticação de usuário, autenticação de sessão e autenticação de cliente, bem como interagir com sistemas de autenticalção RADIUS e TACACS	Conforme Edital Foram disponibilizados dois servidores Intel para o gerenciamento. Um em BSB e outro em SPO	N/A	SIM	Ver propostas Técnica e Comercial

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 637
Doc: 3792

47.129

	Suportar VPN padrão IPSec, com as seguintes características: Algoritmos de criptografia (DES e 3DES), capacidade superior a 1000 conexões simultâneas, capacidade de processamento em 3DES superior a 50Mbps, suporte a certificados digitais X.509v3	Conforme Edital	N/A	SIM	Anexo 53 - pág. 6
	O sistema de gerenciamento de Firewalls deverá ser disponibilizado no mesmo hardware gerenciador dos Servidores de Segurança Lógica tipo 1 em BSB e SPO	Conforme Edital	N/A	SIM	Anexo 53 - pág. 6
3 - Características de Desempenho	Capacidade de tratar no mínimo 280.000 conexões simultâneas	Conforme Edital	N/A	SIM	Anexo 53 - pág. 6 Anexo 54 (todas as páginas) Anexo 55 (todas as páginas)
	Capacidade de processamento superior a 350Mbps em texto claro	Conforme Edital	N/A	SIM	A CONTRATADA se responsabilizará por toda a documentação de instalção e configuração
4 - Configuração Física do Equipamento	Em caso de fornecimento de equipamentos externos ao Switch tipo 1, estes deverão possuir no mínimo 06 interfaces 10/100TX e 01 interface 1000BaseSX	Conforme Edital	N/A	SIM	Anexo 53 - pág. 7
5- Características Adicionais	Todo o ambiente de Firewall deverá ser acompanhado de documentação de instalação e configuração	Conforme Edital	N/A	SIM	A CONTRATADA se responsabilizará por toda a documentação de instalção e configuração

RQS nº 03/2013 - CN - CPMI - CORREIOS
Fls Nº 0638
Doc:

Adicionais	Possuir alimentação elétrica de acordo com a localidade onde serão instalados os equipamentos, com frequência de 60Hz	Conforme Edital	N/A	SIM	Anexo 53 - pág. 7

Sistema para Detecção de Intruso	**IDS**				
ATRIBUTO	REQUISITOS DO EDITAL	ATRIBUTOS OFERTADOS	ATRIBUTOS OFERTADOS ADICIONALMENTE	CONFIRMA ATENDIMENTO (SIM / NÃO)	PÁGINA DA DOCUMENTAÇÃO TÉCNICA
1 - Descrição	O Servidor de detecção deverá operar como IDS, sendo formado por dois módulos que deverão integrar-se ao Switch tipo 1, tomando o tráfego diretamento no painel traseiro desse Switch. Um módulo em BSB e outro em SPO	Não estao sendo ofertados modulos internos ao chassis	N/A	SIM	(Ver Proposta Técnica e Proposta Comercial)
	Será permitida a utilização de 02 equipamentos externos. Um em BSB e outro SPO. Desde que a tomada de tráfego seja realizada através de uma das portas SPAN do Switch tipo 1	Todos os exigidos	N/A	SIM	Ver Proposta Técnica e Comercial

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 639
Doc: 3702

	O ambiente do IDS deve ser composto por 02 elementos complementares, quais sejam: **Sensor** (responsável por monitorar a rede a que está conectado) de análise de cabeçalho e da área de dados de cada pacote que trafega pela rede citada	Conforme Edital	N/A	SIM	Anexo 25 - pág. 1 Anexo 26A (todas as pãginas)
	O sensor deve ser capaz de monitorar o tráfego de rede TCP/IP observando no mínimo uma interface de rede com 500 Mbps em tráfego Full	Conforme Edital	N/A	SIM	Anexo 25 - pág. 2 Anexo 26F (todas as páginas)
	O sensor deve oferecer 01 interface de controle 10/100TX (em caso de equipamento externo ao tipo 1)	Todos os exigidos	A interface é do tipo 10/100/1000T	SIM	Anexo 25 - pág. 3
	O sensor deve funcionar de forma transparente, ou seja, não deve causar impacto no desempenho do Switch, monitorando o tráfego no painel traseiro de comutação do Switch (em caso da utilização de módulos para o Switch tipo 1)	Todos os exigidos	N/A	SIM	Anexo 26A - pág. 3
	O sensor deve possuir a capacidade de monitorar diversas VLANs simultâneamente utilizando recurso de captura de VLANs ACL ou SPAN	Todos os exigidos	N/A	SIM	Anexo 26A - pág. 4 Anexo 26G (todas as paginas)

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 640
Doc: 3792

17.126
7

Software de Controle: Baseado em sistema operacional HP-UX, Solaris, AIX, Windows 2000 ou LINUX, capaz de monitorar de forma centralizada a atividade de múltiplos sensores, estejam estes localizados em segmentos de redes locais ou remotos. Deve ser possível configurar remotamente os sensores utilizando-se o software de controle. O software de controle deve registrar em uma base de dados as configurações de cada um dos sensores que lhes são subordinados. A comunicação entre os sensores e o software de controle deve ser autenticada. O software de controle deve permitir a integração com a base de dados ORACLE 8i ou superior, ou SQL Server versão 2000 ou superior.	Todos os exigidos	N/A	SIM	Anexo 16B (todas as páginas) Anexo 26I (todas as paginas) Anexo 26J (todas as paginas) Anexo 26K (todas as paginas) Anexo 26L (todas as paginas)

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 641
Doc: 3702

17.125
7

O sistema deve analisar cada um dos pacotes que trafegam pela rede a que está conectado e também as relações de tais pacotes pacotes, como os adjacentes a ele no fluxo de dados da rede. Imediatamente após a identificação de uma eventual violação da política de segurança, o sensor deve enviar um alarme para o software de controle.	Todos os exigidos	N/A	SIM	Anexo 26G (todas as paginas) Anexo 26M (todas as paginas)
O bloqueio de uma tentativa de invasão não deve afetar os demais usuários.	Todos os exigidos	N/A	SIM	Anexo 26 (todas as páginas) Anexo 26G (todas as paginas) Anexo 26M (todas as paginas)
Capacidade de detecção de PHF e SMURF	Conforme Edital	N/A	SIM	Anexo 26C (todas as páginas) Anexo 26D (todas as páginas) Anexo 26H (todas as paginas) Anexo 26N - pag. 1
Capacidade de detecção de ataques genéricos de pacotes IP fragmentados e TEARDROP	Conforme Edital	N/A	SIM	Anexo 25 - pág. 4
Capcidade de detecção de ataques que utilizam sistemas Whisker anti-IDS	Conforme Edital	N/A	SIM	Ver Carta do Fabricante
Capacidade de detecção de ataques com assinaturas complexas tais como SIMPLEX MODE TCP hijacking e e-mail SPAN	Conforme Edital	N/A	SIM	Anexo 25 - pág. 4 Anexo 26O - pag. 1

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 642
Doc: 3702

17.124

2 - Características e Funcionalidades	Capacidade de detecção de ataques a servidores de WEB, servidores de e-mail (Denial of Services), FTP exploits, acesso não autorizado a servidores de banco de dados, servidores de aplicação e serviço (NT, Solaris, HP-UX, AIX e LINUX), servidores DNS e PROBIN ATTACKS	Conforme Edital	N/A	SIM	Anexo 25 - pág. 3
	Deve permitir a criação de regras personalizadas de identificação de invasões para que possa ser adaptado à estrutura particular disponível na CONTRATANTE. À medida que novos ataques forem sendo descobertos deve ser possível criar "assinaturas" associadas ao mesmo, de modo a previnir a reincidência	Conforme Edital	N/A	SIM	Anexo 26B (todas as páginas) Anexo 26K (todas as paginas)
	O Software de controle deve ser capaz de enviar alarmes via e-mail para notificar violação de uma dada regra de segurança.	Conforme Edital	N/A	SIM	Anexo 25 -pág. 6 Anexo 26Q (todas as paginas)
	O sistema deve registar informações tais como origem e destino, horário e tipo dos ataques ocorridos	Conforme Edital	N/A	SIM	Anexo 25 - pág. 6 Anexo 26R (todas as paginas)
	O sistema deve possibiltar atualização automática das assinaturas através de download seguro via WEB.	Conforme Edital	N/A	SIM	Anexo 25 - pág. 4 Anexo 26S (todas as paginas)
	O sitema deve possuir suporte a SSH para comunicação e comunicação segura	Conforme Edital	N/A	SIM	Anexo 25 - pág. 4 Anexo 26T (todas as paginas)

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 643
Doc. 3702

17.123
7

O sistema deve realizar a verificação do TCP (Three Way Handshake)	Conforme Edital	N/A	SIM	Anexo 26 (todas as páginas) Anexo 26T (todas as paginas)
Deve oferecer respostas em tempo real para ataques via rede, com possibilidade de término da sessão e reconfiguração de regras de acesso em Firewall, que seja possível configurar	Conforme Edital	N/A	SIM	Anexo 25 - pág. 5 Anexo 26M (todas as paginas)
Deve suportar captura de LOG de sessão no formato padrão TCP DUMP	Conforme Edital	N/A	SIM	Anexo 26A - pág. 6 Anexo 26G (todas as paginas)
Deve bloquer tentativas de invasão que seja possível configurar	Conforme Edital	N/A	SIM	Anexo 25 - pág. 4 Anexo 26K (todas as paginas)
Deve permitir verificação de codificação de protocolos, scripts CGI, DNS e acesso remoto via BIND e DAEMONS	Conforme Edital	N/A	SIM	Anexo 25 - pág.3, 4 Anexo 26U (todas as paginas)
Deve permitir customização de rsposta a intrusões, mascaramento de tráfego, criação de conexões e modificação de ação de resposta	Conforme Edital	N/A	SIM	Anexo 25 - pág. 3, 4, 5 Anexo 26K (todas as assinaturas)
Deve possuir ferramentas de configuração com interface gráfica, controlando múltiplos sistemas de detecção	Conforme Edital	N/A	SIM	Anexo 25 - pág. 6 Anexo 26T (todas as paginas)
Deve registrar sessões de ataques com a possibilidade de PLAYBACK	Conforme Edital	N/A	SIM	Anexo 26A - pág. 6 Anexo 25 (todas as paginas)

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 644
Doc: 3702

17.122

Deve utilizar base de dados em tempo real para ajuda a resposta a incidentes ocorridos	Conforme Edital	N/A	SIM	Anexo 26E - pág 1 Anexo 26V (todas as paginas)
Deve gerar sumários de relatórios das atividades registradas	Conforme Edital	N/A	SIM	Anexo 25 - pág. 5 Anexo 26X (todas as paginas)
Deve utilizar recursos de e-mail e traps SNMP para envio de informações à consoles com plataforma de gerenciamento	Conforme Edital	N/A	SIM	Anexo 25
Deve detectar eventos em ambientes computacionais com os sistemas operacionais Windows NT, 4.0 (server e Workstation) e UNIX (AIX, Solaris, LINUX, HP-UX)	Conforme Edital	N/A	SIM	Anexo 25 Anexo 26Z (todas as paginas)
Deve fornecer suporte ao gerenciamento de riscos através de relatórios técnicos e gerenciais pré-definidos, com detalhamento das informações coletadas	Conforme Edital	N/A	SIM	Anexo 26E - pág. 1, 2 Anexo 26X (todas as paginas)
Deve permitir a criação de relatórios técnicos e gerenciais personalizados, em formas textuais e gráficas	Conforme Edital	N/A	SIM	Anexo 26E - pág. 1, 2 Anexo 26X (todas as paginas)
Deve possuir documentação detalhada para possibilitar a configuração	Conforme Edital	N/A	SIM	Anexo 26E - pág. 1, 2 Anexo 26AA (todas as paginas)
Deve ser robusto para suportar qualquer tipo de ataque contra si próprio	Conforme Edital	N/A	SIM	Anexo 26A - pág. 5 Anexo 26O (todas as paginas)

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 645
Doc: 3702

17.121

	Deve permitir instalação sem necessidade de alteração na infra-estrutura de rede e sem causar degradação do seu desempenho	Conforme Edital	N/A	SIM	Anexo 26A - pág. 5 Anexo 26G (todas as paginas)
	Deve permitir configuração remota à partir da console de gerenciamento	Conforme Edital	N/A	SIM	Anexo 25 - pág.6 Anexo 26T (todas as paginas)
3 - Características Adicionais	O ambiente de gerenciamento dos servidores IDS deverá ser disponibilizado pela CONTRATADA em Hardware exclusivo, à parte, podendo estar integrado em um mesmo framework de gerenciamento dos servidores de segurança lógica, Switch tipo 5 e roteador tipo 1	Conforme Edital	N/A	SIM	A CONTRATADA disponibilizara o hardware exclusivo, à parte. Anexo 26L (todas as paginas)
	Todo o ambiente deverá ser acompanhado de documentação de instalação e configuração	Conforme Edital	N/A	SIM	A CONTRATADA Fornecerá a documentação pertinente e acompanhará toda a instalação. Anexo 26L (todas as paginas)
	O produto deverá integrar-se de forma transparente com o ambiente da gerência dos aservidores de segurança lógica, sendo capaz de reconfigurar automáticamente as regras destes equipamentos	Conforme Edital	N/A	SIM	Anexo 25 (todas as páginas) Anexo 26M (todas as paginas)

RQS nº 03/2003 - CN - CPMI - CORREIOS
Fls Nº 646
Doc: 3702

17.119

ANEXO SWITCH TIPO 01
PARTE 1

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

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 647
Doc: 3702

SWITCH TIPO 1					
ATRIBUTO	REQUISITOS DO EDITAL	ATRIBUTOS OFERTADOS	ATRIBUTOS OFERTADOS ADICIONALMENTE	CONFIRMA ATENDIMENTO (SIM / NÃO)	PÁGINA DA DOCUMENTAÇÃO TÉCNICA
1- Características Físicas	Switch tipo Chassis	Cisco Catalyst 6513 chassis (13 slots)	N/A	SIM	Anexo 1 - pág. 23
2 - Gabinete	Chassis para ser instalado em Rack 19"	Dimensões (em polegadas) H=33.3, W=17.3, D=18.1	N/A	SIM	Anexo 1 - pág. 21
	Todos os módulos de interface, Fontes de Alimentação e Ventiladores devem ser do tipo Hot-Swappable ou Hot-Pluggable	Todos os módulos utilizados na configuração proposta são do tipo Hot-Swapping	N/A	SIM	Anexo 1 - pág. 2, 10, 20 - Anexo 2 - pág. 5 - Anexo 3 - pág 7 Anexo 1A - pág. 1-15 Anexo 30 - pág. 12
3 - Portas Gigabit-Ethernet	Mínimo de 192 portas 10/100/1000 compatíveis com o padrão IEEE 802.3ab, para cabos UTP cat. 6 e conectores RJ-45	Estão sendo fornecidas 192 portas 10/100/1000 compatíveis com o padrão IEEE 802.3ab, para cabos UTP cat. 6 e conectores RJ-45	N/A	SIM	Anexo 5 - pág. 1, 2, 17, 18 e 20
	Mínimo de 16 portas 1000SX compatíveis com o padrão IEEE 802.3z	Estão sendo fornecidas 16 portas 1000SX compatíveis com o padrão IEEE 802.3z	N/A	SIM	Anexo 3 - pág. 1, 3, 8 e 11 - Anexo 4 - pág. 1 e 3 (Ver quantidade nas propostas técnica e comercial)

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 648
3702

	Suportar a inclusão futura de mais 48 portas 10/100/1000Base-T	Foi deixado pelo menos um slot livre para inserção de mais um módulo WS-X6548-GE-TX	N/A	SIM	Ver quantidade de slots (13) versus placas fornecidas nas propostas Técnica e Comercial (12)
4 - Hot-Swapping	Deverá ser do tipo Hot-Swappable ou Hot-Pluggable em todos os módulos	Todos os módulos são do tipo Hot-Swapping ou/ Hot-Pluggable	N/A	SIM	Anexo 1 - pág. 2, 10, 20 - Anexo 2 - pág. 5 - Anexo 3 - pág 7 Anexo 1A - pág. 1-15
5 - Balanceamento de Carga	Balanceamento de carga baseado em Weighted Round Robin, Weighted Least Connections e URL Hashing	Todos os exigidos	N/A	SIM	Anexo 6 - pág 2
	Balanceamento baseado em protocolos das camadas 4 a 7, incluindo TCP,UDP,FTP,DNS,SMTP, HTTP e IPSec	Todos os exigidos	N/A	SIM	Anexo 6 - pág. 1, 2 e Anexo 9A - pág 2
	Capacidade de vincular conexões por meio de endereçamento IP da fonte, cookies e SSL	Todos os exigidos	N/A	SIM	Anexo 6 - pág. , 2
	Redundância via HSRP ou VRRP	Todos os exigidos	N/A	SIM	Anexo 3 - pág. 1 e Anexo 5 - pág. 2
	Capacidade para implementar QoS	Todos os exigidos	N/A	SIM	Anexo 6 - pág. 3
	Deverá suportar balanceamento global para servidores localizados em sites com diferentes saídas para internet	Conforme Edital	N/A	SIM	Anexo 6 - pág. 3

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 649
Doc: 3702

17.117

7 - Gerenciamento	Suportar SNMP e MIB II conforme RFC 1213, bem como RMON I (mínimo de 04 grupos) e RMON II completo	Todos os exigidos	SNMP v1 e v2, SMON, DSMON e HC-MON	SIM	Anexo 7 - pág. 10 e 11
8 - Conectividade	Mínimo de 08 grupos de agregação com no mínimo 08 enlaces cada conforme padrão IEEE 802.3ad	Todos os exigidos	N/A	SIM	Anexo 7 - pág. 11 - Anexo 5 - pág. 18 - Anexo 3 - pág. 11 Anexo 31 - pág. 13-1 e 13-2
9 - Roteamento	Os Switches deverão realizar roteamento (Camada 3)	Conforme Edital	N/A	SIM	Anexo 3 - pág. 4 - Anexo 5 - pág. 6
10 - QoS	Os Switches deverão implementar um mínimo 04 filas de prioridade em cada porta , permitindo a priorização do tráfego de rede e integração transparente de dados, voz e vídeo através do protocolo IEEE 802.1p com CoS (Class of Service)	Conforme Edital	N/A	SIM	Anexo 3 - pág. 11 - Anexo 5 - pág. 1, 18 Anexo 32 - pág. 32-1, 32-3
	Instaladas na configuração máxima do equipamento com recurso de troca sem interrupção (Hot-Swappable ou Hot-Pluggable) e alimentação elétrica de acordo com a localidade onde serão instaladas e com frequência de 60Hz	Fontes de Alimentação totalmente Hot-Swappable, com frequência de operação de 60Hz	N/A	SIM	Anexo 1 - pág. 20 - Anexo 9 - pág. A-6

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 650
Doc: 3702

17.116

11 - Fonte de Alimentação	Deverão ser redundantes por fontes internas independentes com alimentação redundante, de tal forma que em caso de falha de uma das fontes por defeito ou por falta de alimentação elétrica em um dos 02 (dois) circuitos, o equipamento continue a funcionar sem prejuízo das aplicações	Conforme Edital	N/A	SIM	Anexo 30 - pág. 9, 10, 12, 15 a 18
12 - Forwarding Performance	Deve possuir um mínimo de 100 Mpps para Layer 2, Layer 3 e Layer 4	Somatório do troughput do Supervisor module mais os módulos Gigabit Ethernet, montados com cartões DFC	Capacidade total de 105 Mpps em Layer 2, 3 e 4	SIM	Anexo 2 - pág. 4 Anexo 27 - pág. 1 Anexo 28 (todas as páginas)
13 - Gerais	Implementar o protocolo STP para cada VLAN configurada (uma sessão STP por grupo de porta)	Conforme Edital	N/A	SIM	Anexi 1 - pág. 5, 25, 28 Anexo 33 - pág. 15-1, 15-2, 15-15 Anexo 35 - (todo o documento)
	Suportar múltiplos agrupamentos simultâneos de no mínimo 08 interfaces cada um em quaisquer interface de rede e em módulos diferentes de forma a agregar taxa de transmissão	Conforme Edital	N/A	SIM	Anexo 7 - pág. 11 - Anexo 5 - pág. 18 - Anexo 3 - pág. 11 Anexo 31 - pág. 13-1 e 13-2
	Deverá possuir a facilidade de trunking (IEEE 802.1Q) com outros Switches	Conforme Edital	N/A	SIM	Anexo 7 - pág. 11 - Anexo 5 - pág. 18 - Anexo 3 - pág. 11 Anexo 31 - pág. 13-1 e 13-2

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 3702
Doc: 651

17.115
7

	Deverá ser capaz de implementar no mínimo duas sessões simultâneas de espelhamento de tráfego, entrada e saída de interfaces ou VLANs	Conforme Edital	N/A	SIM	Anexo 34 - pág. 34-1 até 34-8 - Anexo 35 (todo o documento)
	A CONTRATADA deverá fornecer ferramentas que permitam o gerenciamento dos equipamentos e de todas as suas interfaces através de aplicação gráfica	Conforme Edital	N/A	SIM	Ver propostas Técnica e Comercial (Softwares de Gerenciamento)
	Deverão ser fornecidos servidores adicionais para instalação dessa,e gerência	Conforme Edital	N/A	SIM	Ver propostas Técnica e Comercial (Servidores Intel)

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 3702
Doc: 652

ANEXO (1)

17.113
2

Cisco Systems

Data Sheet

Cisco Catalyst **6500** Series Switch

The Catalyst 6500 Series sets the new standard for IP communications and application delivery in enterprise campus and service provider networks by maximizing user productivity and enhancing operational control while providing unprecedented investment protection. As Cisco's premier intelligent multilayer modular switch, the Catalyst® 6500 Series delivers secure, converged services, end-to-end, from the wiring closet to the core, to the data center, to the WAN edge.

Ideal for enterprises and service providers seeking to reduce their total cost of ownership, the Cisco Catalyst 6500 Series delivers scalable performance and port density across a range of chassis configurations and LAN/WAN/MAN interfaces. Available in 3-, 6-, 9-, and 13-slot chassis, Cisco Catalyst 6500 Series switches feature an unparalleled range of integrated services modules, including multigigabit network security, content switching, telephony, and network analysis modules.

By taking advantage of a forward-thinking architecture that uses a common set of modules and operating system software across all Cisco Catalyst 6500 Series chassis, the Catalyst 6500 Series delivers a high level of operational consistency that optimizes IT infrastructure usage and enhances return on investment. From 48-port to 576-port 10/100/1000 Ethernet wiring closets to hundreds-of-Mpps network cores supporting up to 192 1-Gbps or 32 10-Gbps trunks, the Cisco Catalyst 6500 Series provides an optimal platform that maximizes network uptime with stateful failover capability between redundant routing and forwarding engines.

With numerous industry-firsts and industry-leading features to its credit, the Catalyst 6500 Series supports three generations of modules that continue to demonstrate the Catalyst 6500 value and Cisco's commitment to innovation. Cisco's new generation of Catalyst 6500 Series modules and Supervisor Engine 720 incorporate 11 new Cisco-developed application specific integrated circuits (ASICs)—extending Cisco's leadership in networking while providing unparalleled investment protection.

Figure 1
Cisco Catalyst 6500 Series Chassis

RQS nº 03/2005 - CN -
CPMI - CORREIOS
653
Fls Nº
3702
Doc:

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

17.112
L

Cisco Catalyst 6500 Series Benefits

The Cisco Catalyst 6500 Series provides market-leading services, performance, port densities, and availability with investment protection for enterprise and service provider markets. These include:

- *Maximum network uptime*—With platform, power supply, supervisor engine, switch fabric, and integrated network services redundancy provides one- to three-second stateful failover and delivers application and services continuity in a converged network environment, minimizing disruption of mission-critical data and services
- *Comprehensive network security*—Integrates proven, multigigabit Cisco security solutions, including intrusion detection, firewall, VPN, and SSL into existing networks
- *Scalable performance*—Provides up to 400 Mpps performance with distributed forwarding architecture
- *Forward-Thinking architecture with investment protection*—Supports three generations of interchangeable, hot-swappable modules in the same chassis, optimizing IT infrastructure usage, maximizing return on investment, and reducing total cost of ownership
- *Operational consistency*—Features 3-, 6-, 9-, and 13-slot chassis configurations sharing a common set of modules, Cisco IOS Software, Cisco Catalyst Operating System Software, and network management tools that can be deployed anywhere in the network
- *Unparalleled services integration and flexibility*—Integrates advanced services such as security and content with converged networks, provides the widest range of interfaces and densities, from 10/100 and 10/100/1000 Ethernet to 10 Gigabit and from DS0 to OC-48, and performs in any deployment end to end

Operational Consistency in End-to-End Cisco Catalyst 6500 Series Deployments

- Features 3-, 6-, 9-, and 13-slot chassis configurations that share a common set of modules, software, and network management tools
- Deploys anywhere in the network—from the wiring closet to the core, to the data center, to the WAN edge
- Shares WAN port adapters with Cisco 7xxx router Series for reduced sparing and training costs
- Offers choice of Cisco IOS Software and Cisco Catalyst Operating System Software supported on all supervisor engines, providing smooth migration from Cisco Catalyst 5000 Series and Cisco 7500 Series deployments

Maximum Network Uptime and Network Resiliency

- Provides packet-loss protection and the fastest recovery from network disruption
- Features fast, one- to three-second stateful failover between redundant supervisor engines
- Offers optional, redundant high-performance Cisco Catalyst 6500 Series Supervisor Engine 720, passive backplane, multimodule Cisco EtherChannel® technology, IEEE 802.3ad link aggregation, IEEE 802.1s/w, and Hot Standby Router Protocol/Virtual Router Redundancy Protocol (HSRP/VRRP) high-availability features

Integrated High-performance Security and Network Management

Integrated gigabit-per-second services modules, deployed where external devices would not be feasible, simplify network management and reduce total cost of ownership. These include:

- Gigabit firewall—provides access protection
- High-performance intrusion detection system (IDS)—provides intrusion detection protection
- Gigabit Network Analysis Module—provides a more manageable infrastructure and full Remote Monitoring (RMON) support
- High-performance SSL—provides high-performance, secure e-commerce traffic termination
- Gigabit VPN and standards-based IP Security (IPSec)—support lower cost Internet and intracampus connections

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 654
Nº 3702
Doc.

17.111
L

Content-and Application-Aware Layers 2 Through 7 Switching Services

- Integrated content switching module (CSM) brings high-performance, feature-rich server and firewall load balancing to the Cisco Catalyst 6500 Series, ensuring a safer and more manageable infrastructure with unprecedented control
- Integrated multigigabit SSL acceleration combined with CSM provides a high-performance e-commerce solution
- Integrated multigigabit firewall and CSM provide a secure, high-performance, data-center solution
- Software features such as Network Based Application Recognition (NBAR) enhance network management and control of bandwidth utilization

Scalable Performance

- Delivers the industry's highest LAN switch performance, 400 Mpps, using the distributed Cisco Express Forwarding dCEF720 platform
- Supports a mix of Cisco Express Forwarding (CEF) implementations and switch fabric speeds for optimal wiring closet, core, data center, and WAN edge deployments, as well as service provider networks

Rich Layer 3 Services

- Multiprotocol Layer 3 routing supports traditional network requirements and provides a smooth transition mechanism in the enterprise
- Provides hardware support for enterprise-class and service-provider-scale routing tables
- Provides IPv6 support in hardware (using Supervisor Engine 720) with an unparalleled high-performance suite of services
- Provides hardware support for large enterprise-class and service-provider-scale routing tables
- Provides MPLS support in hardware to enable VPN services within the enterprise and facilitate smooth integration with new high-speed service provider core infrastructures and Metro Ethernet deployments

Enhanced Data Voice, and Video Services

- Provides integrated IP communications throughout all Cisco Catalyst 6500 Series platforms
- Provides 10/100 and 10/100/1000 line cards, field upgradable with inline power using a daughter card and offering future support for IEEE 802.3af to protect today's investments
- Provides dense T1/E1 and foreign Exchange Station (FXS) voice-over-IP (VoIP) gateway interfaces for public switched telephone network (PSTN) access and traditional phone, fax, and private branch exchange (PBX) connections
- Supports high-performance IP multicast video and audio applications
- Provides integrated management necessary to effectively deploy a scalable enterprise-converged network

Highest Level of Interface Flexibility, Scalability, and Density

- Provides the port densities and interface choices that large mission-critical wiring closets, enterprise core, and distribution networks require
- Supports up to 576 voice 10/100/1000 Gigabit-over-copper ports with inline power per system
- Provides up to 192 Gigabit Ethernet ports

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 655
Doc: 3702

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

17.110
L

- Features the industry's first 10 Gigabit Ethernet, Channelized OC-48 dense OC-3 Packet over Synchronous Optical Network (SONET) (PoS)
- Provides investment protection by using Cisco 7xxx Series port adapters on the Cisco Catalyst 6500 Series FlexWAN Line Card, supporting T1/E1 through OC-48 WAN interfaces
- Chassis sizes range from 3-slot (Cisco Catalyst 6503 Switch) to 13-slot (Cisco Catalyst 6513 Switch)

High-Speed WAN Interfaces

- Provides high-speed WAN, ATM, and SONET interfaces compatible with other core routers
- Provides single-device management for WAN aggregation and for campus and metro connectivity

Maximum Investment Protection

- Highly flexible modular architecture supports multiple generations of modules that are fully interoperable with each other in the same chassis
- Upgradable supervisor engines can add Layer 3 routing or forwarding capabilities over time
- Cisco IOS Software and Cisco Catalyst Operating System Software are supported across all supervisor engines
- Field-upgradable inline power for 10/100 Mbps and 10/100/1000 Mbps Ethernet modules for "pay as you go" IP telephony and wireless computing
- A steady stream of new services modules adds to the deployment options
- Includes Cisco Catalyst 6500 Series network security, content switching, and voice capabilities
- Future modules will increase performance, port density, and include additional services

Ideal for Metro Ethernet WAN Services

- 802.1Q and 802.1Q tunneling (QinQ) providing point-to-point and multipoint Ethernet services
- EoMPLS in MPLS backbones for superior network scaling providing virtual LAN (VLAN) translation capability
- Layer 2 and Layer 3 QoS enables tiered Ethernet service offerings through rate limiting and traffic shaping
- Superior high-availability features include enhanced Spanning Tree Protocol, IEEE 802.1s, IEEE 802.1w, and Cisco EtherChannel IEEE 802.3ad link aggregation

Table 1 Catalyst 6500 Series at a Glance

Feature	Catalyst 6500 Series
System Feature	
Chassis Configurations	3-slot 6-slot 9-slot 9 vertical slots 13-slot
Backplane Bandwidth	32Gbps shared bus 256Gbps switch fabric 720Gbps switch fabric
L3 Forwarding Performance	Supervisor 1 MSFC: 15 Mpps Supervisor 2 MSFC: up to 210 Mpps Supervisor 720: up to 400 Mpps

ROS nº 03/2005 - CN -
CPMI - CORREIOS
656
Fls Nº
3702
Doc:

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

17.109
4

Table 1 Catalyst 6500 Series at a Glance

Feature	Catalyst 6500 Series
Operating System	Catalyst OS (CatOS) Cisco IOS CatOS/IOS Hybrid Configuration
Redundant Supervisors	Yes, with stateful failover
Redundant Components	Power supplies (1+1) Switch fabric (1+1) Replaceable clock Replaceable fan tray
High Availability Features	Gateway Load Balancing Protocol Hot Standby Router Protocol Multimodule EtherChannel Rapid Spanning Tree Multiple Spanning Tree Per VLAN Rapid Spanning Tree Rapid Convergence L3 Protocols
Maximum System Port Densities	
10/100/1000 Ethernet	576 ports, all support Inline Power
10/100 Fast Ethernet	576 ports, all support Inline Power
100-Base-FX	288 ports
Gigabit Ethernet (GBIC)	194 ports (2 ports provided on supervisor engine)
10 Gigabit Ethernet (XENPAK)	32 ports
Integrated WAN Modules	
FlexWAN (DS0 to OC-3)	12 modules with 24 port adapters
OC-3 POS ports	192
OC-12 POS ports	48
OC-12 ATM ports	24
OC-48 POS/DPT ports	24
PSTN Interfaces	
Digital T1/E1 Trunk ports	216
FXS Interfaces	864
Advanced Services Modules	Gigabit Firewall Gigabit VPN High Performance Intrusion Detection Gigabit Content Switching Module High Performance SSL Termination Gigabit Content Services Gateway

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 657
3702

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

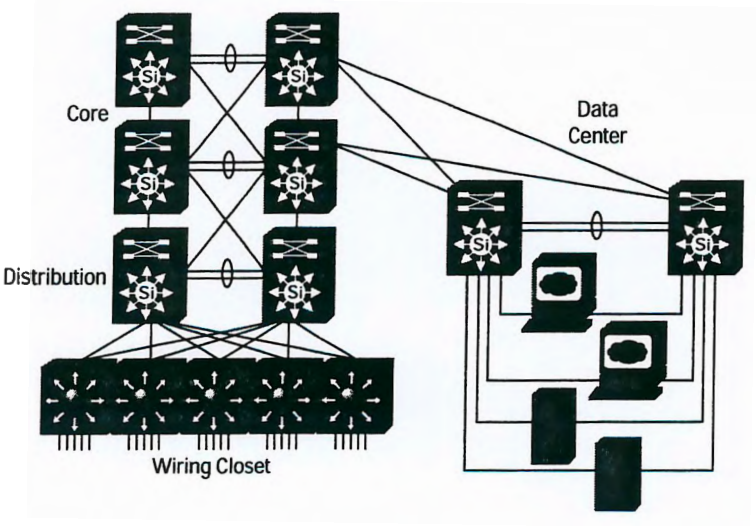
97 108
L

Deployment Scenarios

The Cisco Catalyst 6500 Series delivers secure converged services for campus, Internet service provider (ISP), metro edge, and research and grid computing networks.

- *Campus networks*—Features 10/100 and 10/100/1000 autosensing modules that provide inline power for the wiring closet, along with robust high availability, security, and manageability features; world-class networking software; high-performance Gigabit and 10 Gigabit interface modules; and network management for the distribution and core

Figure 2
Deployment Scenarios for Catalyst 6500 Series Switches in Campus Networks



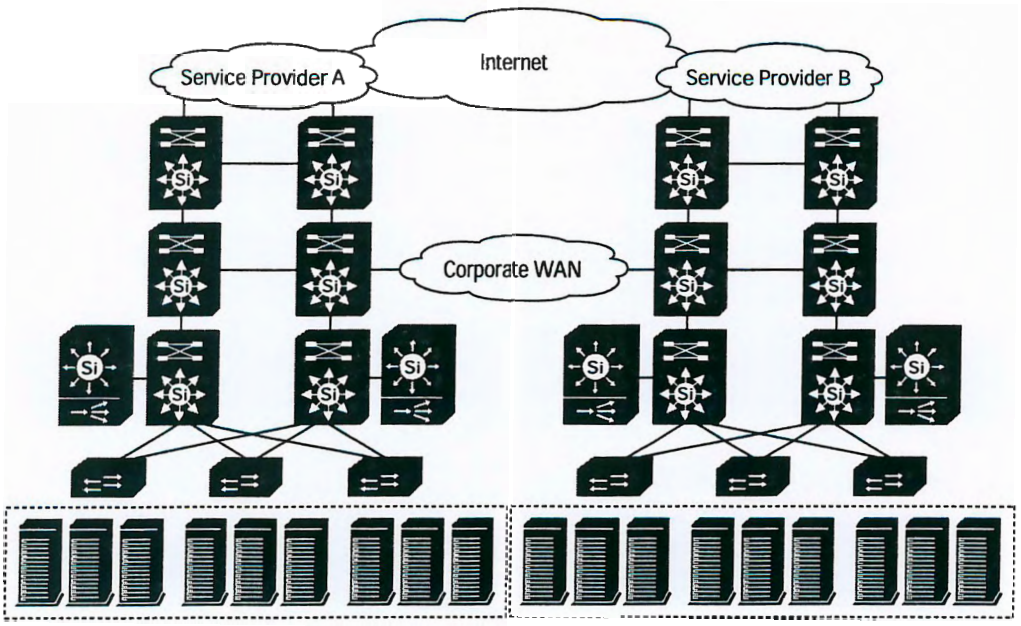
Cisco Systems, Inc.
All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 658
Nº 3702
Doc:

2107

- [*ISP network*—Provides robust high-availability, security, and manageability features; world-class networking software; high-performance Gigabit and 10 Gigabit interface modules; and network management for the most demanding service provider networking environments requiring Multiprotocol Label Switching (MPLS), Multicast, IP Version 6 (IPv6), an extensive set of WAN interfaces, and hierarchical traffic shaping.

Figure 3
Deployment Scenarios for Catalyst 6500 Series Switches in ISP Networks



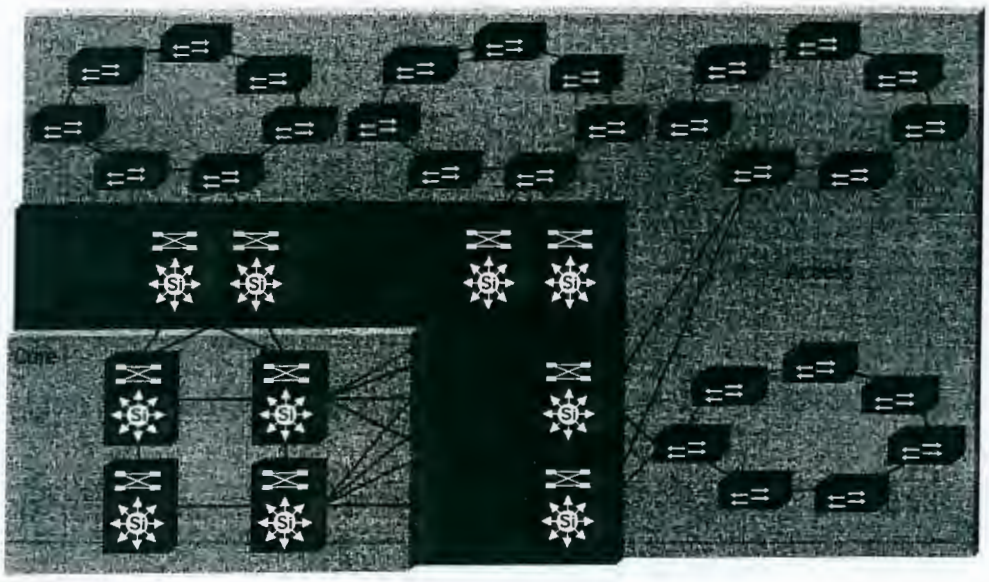
RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 659
Doc: 3702

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

17.106
L

- *Metro edge*—Features edge-, distribution-, and core-layer interfaces for point-to-point and multipoint Ethernet services for metro and inter-metro network deployments with the following features:
  - High-performance 10-Gigabit Ethernet uplinks
  - 802.1Q tunneling
  - Ethernet over MPLS (EoMPLS)
  - Layer 2 and Layer 3 QoS
  - Network Equipment Building Standards (NEBS) compliance
  - Security, high availability, and manageability

Figure 4
Deployment Scenarios for Catalyst 6500 Series Switches in Metro Edge



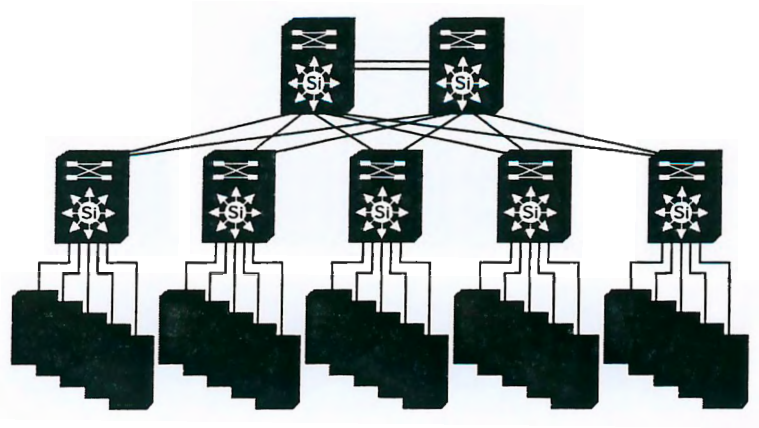
All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 660
3702
Doc:

17.106

- *Grid computing network*—Provides high-speed optical interface modules and world-class software required to handle high-volume traffic and build and manage large-scale networks

Figure 5
Deployment Scenarios for Catalyst 6500 Series Switches in Grid Computing Network



RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 661
Doc: 3702

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

17.104
L

System Overview

Modular Architecture

The Cisco Catalyst 6500 Series is a modular system that can grow as customer requirements expand and technology evolves, allowing customers to upgrade and reconfigure systems by adding new modules, replacing existing modules, and adding and redeploying systems. Throughout the Cisco Catalyst 6500 Series, modules are:

- *Configurable*—Separately, simplifying the addition of new services
- *Interoperable*—In the same chassis, providing flexible design options
- *Interchangeable*—Among Cisco Catalyst 6500 Series systems, simplifying sparing and network expansion
- *Hot-swappable*—Without requiring a chassis to be powered off, providing fast upgrade and repair
- *Upgradable*—As newer modules come along, providing investment protection

Cisco Catalyst 6500 Series Hardware-Forwarding Architectures

Cisco Catalyst 6500 Series modules use one of three forwarding technologies, each having a different architecture with different characteristics and capabilities:

- *Cisco Express Forwarding (CEF)*—Scaling to 30 Mpps, this technology uses a central CEF Cisco Express Forwarding engine located on the supervisor engine's policy feature card (PFC) daughter and CEF forwarding tables located on the supervisor engine. The supervisor engine makes all forwarding decisions for all interface modules centrally. For more information see *How Cisco Express Forwarding Works.*
- *Accelerated Cisco Express Forwarding (aCEF)*—Suited for high-performance enterprise environments, this technology uses the aCEF engine and aCEF tables located on the interface module, along with the central CEF engine located on the supervisor engine's PFC daughter card and central CEF forwarding tables located on the supervisor engine. The interface module makes high-volume forwarding decisions locally, and the supervisor engine makes the rest of the forwarding decisions centrally. For more information see *How Accelerated Cisco Express Forwarding (aCEF) Works.*
- *Distributed Cisco Express Forwarding (dCEF)* —Suited for the most demanding environments, this technology uses the dCEF engine located on the interface module's distributed forwarding card (DFC) daughter card and the dCEF table, a local copy of the supervisor engine's central CEF table located on the interface module's DFC. The interface module makes all the forwarding decisions locally, and provides maximum performance and scalability. For more information see *How Distributed Cisco Express Forwarding (dCEF) Works*

Cisco Catalyst 6500 Series Switching Architectures

Cisco developed the following switching architectures for Cisco Catalyst 6500 modules to allow platforms to scale in any deployment:

- 32-Gbps bus—Allowing access to a central shared bus
- 256-Gbps switch fabric—Located on the switch fabric module (SFM)
- 720 Gbps switch fabric—Located on Cisco Catalyst 6500 Series Supervisor Engine 720

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 662
3702
Doc:

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

17.103
L

Cisco Catalyst 6500 Series Modules

Cisco Catalyst 6500 Series interfacecmodules support the following forwarding technology and switch fabric combinations:

- *Classic Interface Modules*—Use the centralized CEF engine located on the supervisor engine's PFC, connect to the 32-Gbps switching bus only, and forward packets at up to 15 Mpps
- *CEF256 Interface Modules*—Use the centralized CEF engine located on the supervisor engine's PFC, connect to both the 256-Gbps fabric located on the supervisor engine with a single 8-Gbps full-duplex fabric connection and the 32-Gbps switching bus, and forward packets at up to 30 Mpps
- *dCEF256 Interface Modules*—Use the distributed CEF engine on the DFC (located on the interface module), connect to a 256-Gbps fabric located on the supervisor engine or a Switch Fabric Module with 16-Gbps full-duplex fabric connections, and forward packets at up to 210 Mpps
- *aCEF720 Interface Modules*—Use the accelerated CEF engine on the DFC3 (located on the interface module), connect to the 720-Gbps fabric located on the supervisor engine with 40-Gbps full-duplex fabric connections, and forward packets at up to 400 Mpps, peak performance
- *dCEF720 Interface Modules*—Use the distributed CEF engine on the DFC3 (located on the interface module), connect to the 720-Gbps fabric located on the supervisor engine with dual 20-Gbps full-duplex fabric connections, and forward packets at up to 400 Mpps, sustained performance

Note: All Performance numbers refer to IPv4 forwarding.

Cisco Catalyst 6500 Series Module Types

In the Cisco Catalyst 6500 Series architecture, special-purpose modules perform separate tasks—allowing the feature set to evolve quickly and allowing customers to add new features and enhanced performance by adding new modules. The Cisco Catalyst 6500 Series features the following types of special-purpose modules:

- *Supervisor engines*—Perform the control functions and make the forwarding decisions for packets routed to other networks
- *Ethernet interface modules*—Provide IEEE-standard receive and forwarding interfaces and forward packets within the defined network
- *WAN interface modules*—Provide the receive and forwarding interface at the WAN edge
- *Services modules*—Support multigigabit security, application-aware Layer 4 through 7 content switching, network management, and voice gateway services to traditional phones, fax machines, PBXs, and the PSTN
- *Switch Fabric Modules (SFMs)*—Pass network traffic from interface module to the supervisor engine or to another interface

Cisco Catalyst 6500 Series Supervisor Engines

The supervisor engines for the Cisco Catalyst 6500 Series support different forwarding technologies and achieve different forwarding rates, depending on the configuration of the supervisor engine and the capability of a particular interface module.

Supervisor engines can be configured with optional factory-installed daughter cards—a Policy Feature Card (PFC) providing hardware-based Layer-2 forwarding, and a Multilayer Switch Feature Card (MSFC) providing Layer 3 capabilities.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RGS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 663
Nº Doc: 3702

17.102
L

A supervisor engine performs control operations centrally on processors that run either Cisco IOS Software or Cisco Catalyst Operating System Software while special-purpose application-specific integrated circuits (ASICs) perform bridging and routing (based on Cisco Express Forwarding), QoS marking and policing, and access control. The same ASICs are used on the DFCs, daughter cards that can be installed on certain interface modules to distribute forwarding in a decentralized fashion to achieve system forwarding rates of up to 400 Mpps (Table 2).

For additional information about the following Cisco Catalyst 6500 Series supervisor engines visit: http://www.cisco.com/en/US/products/hw/switches/ps708/products_data_sheets_list.html

- Cisco Catalyst 6500 Series Supervisor Engine 720 Data Sheet
- Cisco Catalyst 6500 Series Supervisor Engine 1A and Supervisor Engine 2 Data Sheet

Table 2 Cisco Catalyst 6500 Supervisor Engines

Feature	Supervisor Engine 1	Supervisor Engine 2	Supervisor Engine 720
Solution and market	Wiring closet	Enterprise distribution, core, and WAN edge; service provider WAN and Internet edge	Enterprise core and data center; service provider metro; wireless; national research networks; grid computing
Fabric architectures supported	Centralized forwarding only—engine located on supervisor engine's PFCx daughter card	Centralized CEF—engine located on supervisor engine's PFCx daughter card; Distributed CEF—engine located on interface module's DFC daughter card	Centralized CEF—engine located on Supervisor Engine 720's PFC3 daughter card; Distributed CEF—engine located on interface module's DFC3 daughter card; Accelerated CEF—engine located on interface module's ASICs
Fabric connections	32-Gbps shared bus connection to modules	16 Gbps per slot; Dual-fabric connection to modules at 8 Gbps full duplex per channel	40 Gbps per slot; Dual-fabric connection to modules at 20 Gbps full duplex per channel
Performance maximum (Mpps)	15 Mpps	210 Mpps	Sustained 400 Mpps—dCEF720 Peak 400 Mpps—aCEF720
DFC modules	Not supported	DFC	DFC3

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 664
Doc: 3702

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

17.101
L

Table 2 Cisco Catalyst 6500 Supervisor Engines

Feature	Supervisor Engine 1	Supervisor Engine 2	Supervisor Engine 720
Route processor	On MSFC2 daughter card (optional)	On MSFC2 daughter card (optional)	MSFC3 integrated
PFC modules	PFC daughter card (optional)	PFC2 integrated	PFC3 integrated

Ethernet Interface Modules

Cisco Catalyst 6500 Series Ethernet interface modules, designed for wiring closet, distribution and core, and data center applications, as well as service provider and Metro Ethernet environments, use one of the following types of Ethernet interfaces:

- *10/100 Mbps over copper and 10/100/1000 Mbps Ethernet over copper*—For wiring closets providing 10/100- and 10/100/1000-Mbps performance with auto-negotiation and inline power for voice; up to 48 ports/module; includes Classic and CEF256 interface modules.
- *100 Mbps over fiber*—For secure wiring closets and long-haul router and switch interconnects; up to 24 ports per module; includes Classic and CEF256 interface modules.
- *1 Gbps*—For distribution and core layers and for data centers providing 1-Gbps performance in a 48-port module; includes Classic CEF256, and dCEF256 interface modules.
- 10 Gbps—For distribution and core layers providing 10-Gbps performance in 1-port or 2-port module; includes CEF256, aCEF720, and dCEF720 interface modules.

For more information, visit:
http://www.cisco.com/en/US/products/hw/switches/ps708/products_data_sheets_list.html

WAN Interface Modules

The Cisco Catalyst 6500 Series and Cisco 7600 Series support several WAN interfaces using two technologies:

- *FlexWAN module*—Accepts up to two plug-in port adapters that provide numerous WAN/MAN protocols and features
- *Optical Services Module (OSM)*—A dedicated line card that provides several interfaces, including OC-3/STM-1, OC-12/STM-4, OC-48/STM-16, Channelized T3, Channelized OC-12/STM-4 PoS, Gigabit Ethernet, OC-12/STM-4 ATM, and OC-48/STM-16 Dynamic Packet Transport (DPT)

FlexWAN Module

The FlexWAN module fits inside Cisco Catalyst 6500 Series and Cisco 7600 Series systems and uses Cisco 7200 and 7500 Series port adapters for a wide range of WAN/MAN protocols, including Frame Relay, ATM, PoS, Point-to-Point Protocol (PPP), and High-Level Data Link Control (HDLC). Additionally, the FlexWAN module provides media options such as clear channel and Channelized T1/E1, T3/E3, High-Speed Service Interface (HSSI), OC-3 PoS, and ATM.

- For information about the Cisco Catalyst 6500 Series and Cisco 7600 Series FlexWAN Module, visit: http://www.cisco.com/en/US/products/hw/routers/ps368/products_data_sheet09186a00800923bf.html

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 665
Nº 3702
Doc:

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

17.100

Optical Services Modules

OSMs are line cards that provide high-speed WAN connectivity with onboard network processors for distributed-line-rate IP service applications. For more information about OSMs, see the following data sheets:

- Cisco 7600 Series 4-, 8-, and 16-Port OC-3c/STM-1 PoS/SDH OSM: http://www.cisco.com/en/US/products/hw/routers/ps368/products_data_sheet09186a0080092249.html
- Cisco 7600 Series 4-Port Gigabit Ethernet OSM: http://www.cisco.com/en/US/products/hw/routers/ps368/products_data_sheet09186a008009223d.html
- Cisco 7600 Series 1-Port Channelized OC-12/STM-4 to DS3/E3 OSM: http://www.cisco.com/en/US/products/hw/routers/ps368/products_data_sheet09186a0080092250.html
- Cisco 7600 Series 1-Port OC-48c/STM-16 PoS/SDH/OSM: http://www.cisco.com/en/US/products/hw/routers/ps368/products_data_sheet09186a0080092241.html
- Cisco 7600 Series 2- and 4-Port OC-12c/STM-4 PoS/SDH OSM: http://www.cisco.com/en/US/products/hw/routers/ps368/products_data_sheet09186a008009223e.html
- Cisco 7600 Series 2-Port ATM OSM: http://www.cisco.com/en/US/products/hw/routers/ps368/products_data_sheet09186a008008876f.html
- Cisco 7600 Series 2-Port OC-48c/1-Port OC-48c DPT OSM: http://www.cisco.com/en/US/products/hw/routers/ps368/products_data_sheet09186a0080088774.html
  Layer 4 Through 7 Services Modules

The Cisco Catalyst 6500 Series offers an extensive set of services modules for Layer 4 through 7 applications, including content services, network monitoring, security, and telephony.

Content Services Modules

- *Content Services Gateway (CSG)*—Enables differentiated billing, user balance enforcement, and activity tracking for customer billing systems. For more information, visit: http://mobiletraining.cisco.com/csg/CSGe_ds_0211.pdf
- *Content Switching Module (CSM)*—Integrates advanced content switching into the Cisco Catalyst 6500 Series to provide high-performance, high-availability load balancing of caches, firewalls, Web servers, and other network devices. For more information, visit: http://www.cisco.com/en/US/products/hw/modules/ps2706/products_data_sheet09186a00800887f3.html

Network Monitoring

- *Network Analysis Module (NAM 1 and 2)*—Provides application-level visibility into the network infrastructure for real-time traffic analysis, performance monitoring, and troubleshooting; performs traffic monitoring with embedded Web-based traffic analyzer. For more information, visit: http://www.cisco.com/en/US/products/hw/modules/ps2706/products_data_sheet09186a00800a2c89.html

Security Services Modules

- *Firewall Services Module (FWSM)*—The FWSM allows any port in the chassis to operate as a firewall port and integrates stateful firewall security inside the network infrastructure. For more information, visit: http://www.cisco.com/en/US/products/hw/modules/ps2706/products_data_sheet09 186a00800c4fe7.html
  Intrusion Detection System Module (IDSM and IDSM-2)—Takes traffic from the switch backplane at wire speed, integrating IDS functions directly into the switch. For more information, visit: http://www.cisco.com/en/US/products/hw/modules/ps2706/products_data_sheet09186a00800092341.html

ECT nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 666
Nº 3702
Doc:

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

170099

- *IPSec VPN Module (IVSM)*—Provides infrastructure-integrated IPSec VPN services capable of 1.9-Gbps Triple Data Encryption Standard (3DES) performance, 8000 active tunnels, and up to 60 tunnels per second. For more information, visit: http://www.cisco.com/en/US/products/hw/modules/ps2706/products_data_sheet09 186a00800c4fe2.html
- *SSL Services Module (SSM)*—Offloads processor-intensive tasks related to securing traffic with SSL accelerating the performance and increasing the security of Web-enabled applications. For more information, visit: http://www.cisco.com/en/US/products/hw/modules/ps2706/products_data_sheet09186a00800c4fe9.html

Telephony Services Modules

- *Communications Media Module (CMM)*—Provides flexible, high-density T1 and E1 gateways, allowing organizations to connect their existing time-division multiplexing (TDM) networks to their IP communications networks, and providing connectivity to the PSTN. For more information, visit: http://www.cisco.com/en/US/products/hw/modules/ps3115/products_data_sheet09 186a00800e9c1f.html

Switch Fabric Modules

Designed to support distributed forwarding for interface modules that have distributed forwarding capability, the Cisco Catalyst 6500 Series SFM or SFM2, in combination with the Cisco Catalyst 6500 Series Supervisor Engine 2-MSFC2 and DFCs on interface modules, increases available system bandwidth from 32 to 256 Gbps. The SFM/SFM2 supports the Cisco Catalyst 6500 CEF256 and dCEF256 interface modules.

Designed to support new interface modules with 720 Gbps forwarding capabilities, the Supervisor Engine 720's onboard switch fabric increases available bandwidth to 720 Gbps and enables packet forwarding rates up to 400 Mpps. By using auto-sensing and auto-negotiation, the Supervisor 720 switch fabric is fully interoperable with the 8- and 16-Gbps switch fabric interconnections used by the CEF256 and dCEF256 interface modules. When a CEF256 or dCEF256 interface module is detected, the switch fabric will automatically connect those modules by offering 8-16 Gbps of bandwidth to each module, as applicable.

How Cisco Express Forwarding Works

Cisco Express Forwarding (CEF) is a Layer 3 technology that provides increased forwarding scalability and performance to handle many short-duration traffic flows common in today's enterprise and service provider networks. To meet the needs of environments handling large amounts of short-flow, Web-based, or highly interactive types of traffic, CEF forwards all packets in hardware, and maintains its forwarding rate completely independent of the number of flows going though the switch.

On the Cisco Catalyst 6500 Series, the CEF Layer 3 forwarding engine is located centrally on the supervisor engine's PFC2 or PFC3—the same device that performs hardware-based Layer 2 and 3 forwarding, ACL checking, QoS policing and marking, and NetFlow statistics gathering.

Using the routing table that Cisco IOS Software builds to define configured interfaces and routing protocols, the CEF architecture creates CEF tables and downloads them into the hardware-forwarding engine before any user traffic is sent through the switch. The CEF architecture places only the routing prefixes in its CEF tables—the only information it requires to make the Layer 3 forwarding decisions—relying on the routing protocols to do route selection. By performing a simple CEF table lookup, the switch forwards packets at wire-rate, independent of the number of flows transiting the switch.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 667
Doc: 3702

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

17098

CEF-based forwarding requirements: Requires a Cisco Catalyst Supervisor Engine 2 or Catalyst Supervisor Engine 720.

How Accelerated Cisco Express Forwarding (aCEF) Works

Accelerated Cisco Express Forwarding (aCEF) technology uses two forwarding engines working together in a master-slave relationship to accelerate high-rate traffic flows through the switch—a central CEF engine located on the Supervisor Engine 720's PFC3 and a scaled-down distributed aCEF engine located on the interface module.

The central PFC3 makes the initial forwarding decision, with the aCEF engine storing the result and making subsequent packet-forwarding decisions locally. aCEF forwarding works like this:

- As in standard CEF forwarding, the central PFC3 is loaded with the necessary CEF information before any user traffic arrives at the switch.
- As traffic arrives on an aCEF720 interface module, the aCEF engine inspects the packet, and finding that no specific packet forwarding information exists, consults the central PFC3.
- The PFC3 makes a hardware-based forwarding decision for this packet (including Layer 2, Layer 3, ACLs, and QoS).
- The aCEF engine stores the forwarding decision results and makes forwarding decisions locally for subsequent packets based on packet-flow history.
- The aCEF engine handles hardware-based Layer 2 and Layer 3 forwarding, ACLs, QoS marking, and NetFlow.
- The central PFC3 processes any forwarding decisions that the interface module's aCEF engine cannot handle.

aCEF-based forwarding requirements: Requires a Cisco Catalyst Supervisor Engine 720 and aCEF720 (WS-X67xx) class modules.

How Distributed Cisco Express Forwarding (dCEF) Works

With Distributed Cisco Express Forwarding (dCEF), forwarding engines located on the interface modules make forwarding decisions locally and in parallel, allowing the Cisco Catalyst 6500 Series to achieve the highest forwarding rates in the industry. With dCEF, forwarding occurs on the interface modules in parallel and system performance scales up to 400 Mpps—the aggregate of all forwarding engines working together.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

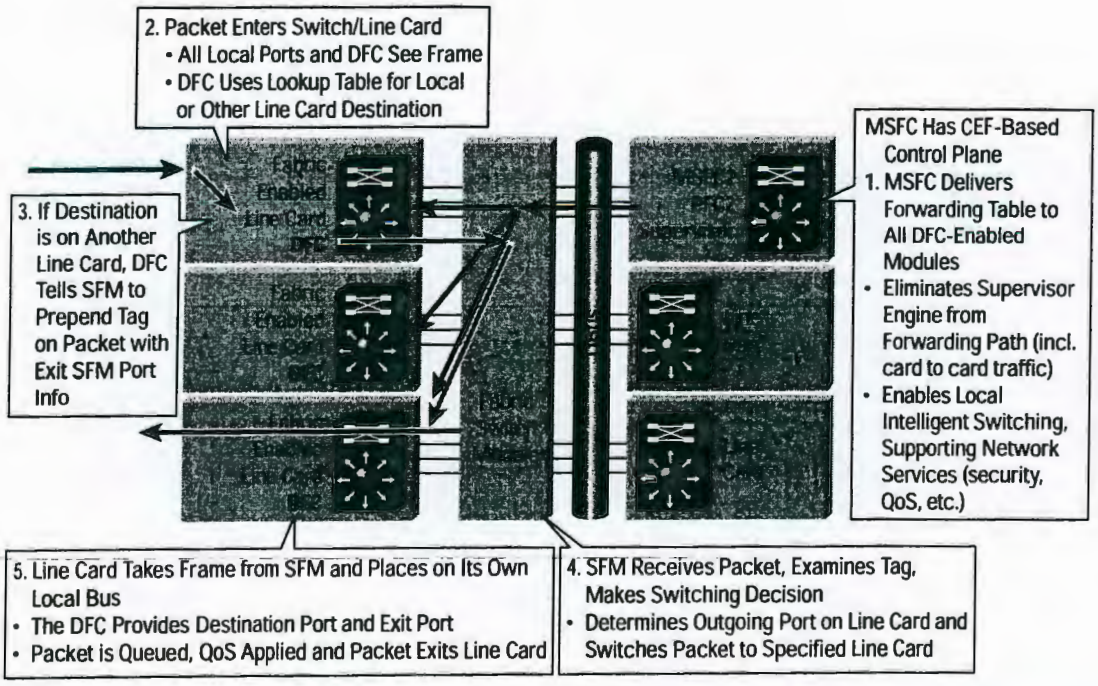
RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 668
Nº 3702
Doc:

17097
/

Using the same ASIC engine design as the central PFCx, DFCs located on the interface modules forward packets between two ports, directly or across the switch fabric, without involving the supervisor engine. With the DFC, each interface module has a dedicated forwarding engine complete with the full forwarding tables. dCEF forwarding works like this:

- As in standard CEF forwarding, the central PFC3 located on the supervisor engine and the DFC engines located on the interface modules are loaded with the same CEF information derived from the forwarding table before any user traffic arrives at the switch.
- As a packet arrives at an interface module, its DFC engine inspects the packet and uses the information in the CEF table (including Layer 2, Layer 3, ACLs, and QoS) to make a completely hardware-based forwarding decision for that packet.
- The dCEF engine handles all hardware-based forwarding for traffic on that module, including Layer 2 and Layer 3 forwarding, ACLs, QoS policing and marking, and NetFlow.
- Because the DFCs make all the switching decisions locally, the supervisor engine is freed from all forwarding responsibilities and can perform other software-based functions, including routing, management, and network services.

Figure 6
Distributed Cisco Express Forwarding Packet Flow



dCEF-based forwarding requirements: Requires a Cisco Catalyst Supervisor Engine 720 for the dCEF720 interface module; requires either a Catalyst Supervisor Engine 720 or a Catalyst Supervisor Engine 2 MSFC2 and a SFM for the dCEF256 interface module.

RECEBIDO em 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 669
Doc: 3702

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

17096
L

Cisco IOS Software and Catalyst Operating System Software

Cisco Catalyst 6500 Series switches offer two operating modes of software, the Cisco Catalyst Operating System Software with optional Cisco IOS Software on the MSFC, and Cisco IOS Software for the supervisor engines. Each operating mode can be deployed at different hierarchies of the network, depending on the network's requirements. These software solutions for the Cisco Catalyst 6500 Series switches provide full Layer 2 through 4 switching and routing functions at high performances.

Today, either of these operating modes can be deployed in an entire network environment, or the operating modes can vary within an environment to meet different requirements. One operating mode is not a replacement for another, but is recommended for varying feature requirements.

- Cisco IOS Software for the Cisco Catalyst 6500 Series
- Cisco Catalyst Operating System Software with optional Cisco IOS Software on the MSFC

Cisco IOS Software for the Cisco Catalyst 6500 Series

Cisco IOS Software for the Cisco Catalyst 6500 Series supervisor engines requires the MSFC on the supervisor engine. It provides integrated multilayer functions in a single image and is optimized for core, distribution, Internet access, and data center deployments. Cisco IOS Software combined with the performance of the Cisco Catalyst 6500 Series offers the necessary features for a high-performance Layer 3-enabled deployment, including support for a distributed architecture with the ability to scale the switch to 400 Mpps throughput. Additionally, Cisco IOS Software provides operational ease of use by offering a single image and configuration file to be deployed across the Cisco Catalyst 6500 Series switches.

Cisco Catalyst Operating System Software with Optional Cisco IOS Software on the MSFC

Cisco Catalyst Operating System Software is the premier software for the wiring closet on Cisco Catalyst 6500 Series switches offering high-performance Layer 2 forwarding. It is optimized to deliver the high availability, enhanced security, and integrated inline power support necessary for mission-critical wiring closet deployments. Cisco Catalyst Operating System Software can also be extended to the distribution and core layers of the network when coupled with Cisco IOS Software on the MSFC, providing robust and advanced Layer 3 and Layer 4 functions. This operating mode is often referred to as "hybrid mode." See Table 3 for software and hardware deployment options.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 670
Doc: 3702

17095
L

Table 3 Software and Hardware Deployment Options

Network Performance	Wiring Closet	Distribution/ Data Center	Core	WAN Edge
Highest-performance Cisco IOS Software end-to-end	Cisco IOS Software; Supervisor Engine 2-MSFC2; CEF256 interface modules	Cisco IOS Software; Supervisor Engine 720; dCEF720 and aCEF720 interface modules	Cisco IOS Software; Supervisor Engine 720; dCEF720 interface modules	Cisco IOS Software; Supervisor Engine 2-MSFC2; dCEF720 and aCEF720 interface modules
Higher-performance mixed operating system	Cisco Catalyst Operating System Software; Supervisor Engine 2-PFC2; CEF256 and Classic interface modules	Cisco IOS Software; Supervisor Engine 2-MSFC2; dCEF256 and CEF256 interface modules	Cisco IOS Software; Supervisor Engine 720; dCEF720 and aCEF720 interface modules	Cisco IOS Software; Supervisor Engine 2-MSFC2; dCEF256 and, CEF256 interface modules
High-performance Cisco Catalyst Operating System Software end-to-end	Cisco Catalyst Operating System Software; Supervisor Engine 1-2GE; CEF256 and Classic interface modules	Hybrid mode; Supervisor Engine 2-MSFC2; CEF256 and Classic interface modules	Hybrid mode; Supervisor Engine 2-MSFC2; dCEF720 Series and aCEF720 interface modules	Hybrid mode; Supervisor Engine 2-MSFC2; CEF256 and Classic interface modules

Cisco IOS Software and Cisco Catalyst Operating System Software Shared Features

All Cisco Catalyst 6500 Series supervisor engines, including the new Supervisor Engine 720, take advantage of the industry-leading software and management capabilities of the Cisco Catalyst 6500 Series. Customers can apply their knowledge of Cisco Catalyst Operating System Software, Cisco IOS Software, CiscoWorks, and other graphical and Web-based network management tools without the need to learn a new command-line interface (CLI) or management system.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 671
Nº 3702
Doc:

17094
L

Cisco Catalyst 6500 Series Chassis

Cisco Catalyst 6500 Series chassis can be deployed in the wiring closet, the distribution and core layers, the data center, and the WAN edge, providing the power and features required for end-to-end deployment for the enterprise campus, the ISP network, metro, and research computing networks.

Chassis Applications

The Cisco Catalyst 6500 Series provides a selection of chassis, including 3-, 6-, 9-, and 13-slot models with slots arranged horizontally and a 9-slot model with slots arranged vertically, with front-to-back airflow. Typical applications for Cisco Catalyst 6500 Series chassis include:

- *3-slot chassis*—Low-density, wiring-closet chassis sharing interface modules and supervisor engines with larger chassis for common sparing; low-density, high-performance specialized services modules chassis for network security and management; low-density, high-end chassis providing connectivity to the WAN edge
- *6- and 9-slot chassis*—Traditional chassis for the wiring closet, distribution and core, data center, and WAN edge
- *13-slot chassis*—Highest-capacity chassis for Ethernet connectivity, with slots to spare for services modules providing network security and management

Chassis Configuration

All Cisco Catalyst 6500 Series chassis are NEBS Level-3 compliant and use common power supplies. The 6- and 9-slot chassis require a 1000W or 1300W power supply and the 13-slot chassis requires a 2500W or 4000W power supply. The 3-slot chassis requires a 950W power supply. When ordering a Cisco Catalyst 6500 Series switch, use the online Cisco Dynamic Configuration Tool to assist you in selecting the chassis, power supplies, power cables, and fan trays that will meet your requirements. The tool is available at:
http://www.cisco.com/appcontent/apollo/configureHomeGuest.html

Power

All Cisco Catalyst 6500 chassis hold up to two load-sharing, fault-tolerant, hot-swappable AC or DC power supplies. Only one supply is required to operate a fully loaded chassis. If a second supply is installed, it operates in a load-sharing capacity. The power supplies are hot-swappable—a failed power supply can be removed without powering off the system.

Cisco Catalyst 6500 Series switch power supplies are available in five power ratings:

- 950W AC input (Cisco Catalyst 6503 chassis)
- 1000W AC input
- 1300W AC and DC input
- 2500W AC and DC input
- 4000W AC input

Table 4 outlines the power requirements and heat dissipation for the three different models of power supplies available for the Cisco Catalyst 6500 Series switch.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
672
Fls Nº
3702
Doc:

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

17093
L

Table 4 Power Supply VAC and VDC requirements

Power Supply	AC Input Voltage/Current	DC Input Voltage/Current
950W	100 to 240 VAC (10% for full range); 15 A	-48 VDC to –60 VDC continuous; 38 A @ –48 VDC, 30 A @ –60 VDC
1000W	100 to 240 VAC (10% for full range); 12 A @ 100 VAC, 6 A @ 240 VAC	Not supported
1300W	100 to 240 VAC (10% for full range); 17.25 A @ 100 VAC, 8 A @ 200 VAC	–48 VDC to –60 VDC continuous; 38 A @ –48 VDC, 30 A @ –60 VDC
2500W	100 to 120 VAC, 200 to 240 VAC (10% for full range); 16 A maximum at 200 VAC at 2500 W output; 16 A maximum at 100 VAC at 1300 W output	–48 VDC to –60 VDC continuous; 80 A @ –40.5 VDC, 70 A @ –48 VDC, 55 A @ –60 VDC
4000W	100 to 240 VAC (10% for full range); 23 A	Not supported

Fan Trays

Chassis that have a Supervisor Engine 720 installed require a high-speed fan tray. See Table 5 for part number information.

Table 5 Catalyst 6500 Chassis Fan Tray Part Numbers

Catalyst 6500 Chassis	Normal Speed Fan— Fan Tray Part Number	High Speed Fan— Fan Tray Part Number
6503	FAN-MOD-3	FAN-MOD-3-HS(=)
6506	WS-C6K-6SLOT-FAN	WS-C6K-6SLOT-FAN2
6509	WS-C6K-6SLOT-FAN	WS-C6K-9SLOT-FAN2
6509-NEB	WS-C6509-NEB-FAN	WS-C6509-NEB-FAN2
6509-NEB-A	N/A	FAN-MOD-09(=)
6513	WS-C6K-13SLOT-FAN	WS-C6K-13SLOT-FAN2

Dimensions

Table 6 provides Catalyst 6500 Series chassis dimensions.

Table 6 Catalyst 6500 Series Chassis Dimensions

Dimension	Cisco Catalyst 6503	Cisco Catalyst 6506	Cisco Catalyst 6509	Cisco Catalyst 6509-NEB	Cisco Catalyst 6513
H x W x D (in.)	7 x 17.37 x 21.75 in.	20.1 x 17.2 x 18.1 in.	25.2 x 17.2 x 18.1 in.	33.3 x 17.2 x 18.1 in.	33.3 x 17.3 x 18.1 in.
H x W x D (cm)	17.8 x 44.1 x 55.2 cm	51.1 x 43.7 x 46.0 cm	64.0 x 43.7 x 46.0 cm	84.6 x 43.7 x 46.0 cm	84.6 x 43.7 x 46.0 cm

RQS nº 03/2005 - CN -
CPMI - CORREIOS
673
Fls Nº
Doc: 3702

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

17092
L

Table 6 Catalyst 6500 Series Chassis Dimensions

Dimension	Cisco Catalyst 6503	Cisco Catalyst 6506	Cisco Catalyst 6509	Cisco Catalyst 6509-NEB	Cisco Catalyst 6513
Rack units (RU); 1.75 in., 4.4 cm	4 RU	12 RU	15 RU	20 RU	20 RU

Weight

Table 7 provides the weight information for empty and fully configured Catalyst 6500 Series chassis.

Table 7 Catalyst 6500 Series Chassis Weights

Weight	Cisco Catalyst 6503	Cisco Catalyst 6506	Cisco Catalyst 6509	Cisco Catalyst 6509-NEB	Cisco Catalyst 6513
Chassis only (lb)	27	45	55	55	98
Fully configured (lb)	83	115	135	135	240
Chassis only (kg)	12	20	25	25	45
Fully configured (kg)	38	52	61	61	109

Cisco Systems, Inc.
All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 674
3702
Doc:

17091
1

Ordering Information

Table 8 provides part number information for Catalyst 6500 Series chassis

Table 8 Catalyst 6500 Series Chassis Part Numbers

Part Number	Chassis
WS-C6503	Cisco Catalyst 6503 chassis (three slots)
WS-C6506	Cisco Catalyst 6506 chassis (six slots)
WS-C6509	Cisco Catalyst 6509 chassis (nine slots)
WS-C6509-NEB	Cisco Catalyst 6509-NEB chassis (nine vertically oriented slots)
WS-C6509-NEB-A	Cisco Catalyst 6509-NEB chassis (nine vertically oriented slots)–enhanced
WS-C6513	Cisco Catalyst 6513 chassis (13 slots)

Environmental Conditions

Table 9 provides environmental information for Catalyst 6500 Series Chassis.

Table 9 Catalyst 6500 Series Chassis Environmental Conditions

Parameter	Performance Range
Operating temperature	32 to 104 F (0 to 40 C)
Storage temperature	–4 to 149 F (–20 to 65 C)
Relative humidity	10 to 90%, noncondensing
Operating altitude	3000 meters
Mean time between failure (MTBF)	7 years for system configuration

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 675
3702
Doc:

17090

Regulatory Compliance

Safety

- UL 1950
- EN 60950
- CSA-C22.2 no. 950
- IEC 60950
- AS/NZA 3260
- 21 CFR 1040
- EN 60825-1
- IEC 60825-1
- TS 001

EMC

- FCC (CFR 47, Part 15) Class A
- VCCI
- CE Marking
- EN 55022
- EN 55024
- CISPR 22
- AS/NZS 3548
- NEBS Level 3 (GR-1089-CORE, GR-63-CORE)
- ETSI ETS-300386-2

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 676
3702
Doc:

17089

Specifications

Table 10 provides an overview of Catalyst 6500 Series switches specifications, additional information can be found in software release notes.

Table 10 Catalyst 6500 Series Specifications

Specification	Number	Description
IEEE Compliance		
802.1	802.1d 802.1p, q 802.1s 802.1w 802.1x	Bridging VLAN tagging Per-VLAN Group Spanning Tree Protocol Rapid Spanning Tree Protocol
802.1	802.3	10BASE-T, 10BASE-FL
	802.3ad 802.3ab 802.3ae 802.3u	Link aggregation 1000BASE-T 10 Gigabit Ethernet 100BASE-TX, 100BASE-FX
	802.3x	Flow control
	802.3z	1000BASE-SX, 1000BASE-LX
RFC Compliance		
ATM	1483, 2584	Protocol encapsulation over ATM AAL5
		ATM permanent virtual circuit (PVC) to 802.1q tagging
BGP4	1269	Definitions of Managed Objects for the Border Gateway Protocol (Version 3)
	1745	Border Gateway Protocol/Open Shortest Path First (BGP/OSPF) interactions
	1771	BGPv4
	1965	BGP4 autonomous system confederations
	1966	BGP4 route reflection
	1997	Communities attribute
	2385	Transmission Control Protocol (TCP) MD5 authentication for BGP
	2439	Route flap dampening
	2796	Route reflection
	2842	Capabilities advertisement
General routing protocols	768	User Datagram Protocol (UDP)
	783	Trivial File Transfer Protocol (TFTP)
	791	IP

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 677
3702
Doc:

17088
L

Table 10 Catalyst 6500 Series Specifications

Specification	Number	Description
	792	Internet Control Message Protocol (ICMP)
	793	TCP
	826	Address Resolution Protocol (ARP)
	854	Telnet
	894	IP over Ethernet
	903	Reverse Address Resolution Protocol (RARP)
	906	TFTP Bootstrap
	951, 1542	BootP, BootP extensions
	1027	Proxy ARP
	1122	Host requirements
	1256	ICMP Router Discovery Protocol (IRDP) IPv4 router discovery
	1519	Classless interdomain routing (CIDR)
	1541	Dynamic Host Control Protocol (DHCP)
	1591	Domain Name System (DNS) client
	1619	PPP over SONET
	1662	PPP HDLC-like framing
	1812	IPv4
	2131	BootP/DHCP
	2338	VRRP
		Internetwork Packet Exchange Routing Information Protocol/ Service Advertising Protocol (IPX RIP/SAP)
		Software-controlled redundant ports
IP multicast	1112	Internet Group Management Protocol (IGMP)
	1122	Host extensions, Distance Vector Multicast Routing Protocol (DVMRP)
	2236	IGMP v1, v2, v3 IGMP v1, v2, v3 Snooping
	2283	Multicast Border Gateway Protocol (MBGP)
	2362	Protocol-Independent Multicast (PIM)-SM
		DVMRP v3-07 Multicast Source Discovery Protocol (MSDP)
		PIM-Dense Mode (PIM-DM) v1

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 678
Doc: 3702

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

17087
2

Table 10 Catalyst 6500 Series Specifications

Specification	Number	Description
		PIM-DM v2 Bidirectional PIM (Supervisor Engine 720 only)
Intermediate system to Intermediate system (IS-IS)	1195	TCP
	1377	PPP
	2763	Dynamic host name exchange
	2966	Domain-wide prefixes
LSP tunnels	2211	Controlled load network element service
	2702	Traffic engineering over MPLS
MPLS	2547	MPLS VPN
	2961	Resource Reservation Protocol (RSVP) refresh
	3031	MPLS architecture
	3032	MPLS label stack encoding
	3036	Label Distribution Protocol (LDP)
OSPF	1583	OSPF v2
	1587	OSPF NSSA
	1745	OSPF interactions
	1765	OSPF database overflow
	1850	OSPF v2 Management Information Base (MIB), traps
	1997	Communities and attributes
	2154	OSPF digital signatures, MD5
	2178	OSPF v2 (superceded by RFC 2328)
	2328	OSPF v2
	2370	OSPF opaque link-state advertisement (LSA) option
	2385	TCP M5
	2439	Route flap damping
	2842	Capabilities advertisement
	2918	Route refresh capability
RIP	1058	RIP v1
	1723	RIP v2
	2453	RIP v2

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 679
Doc: 3702

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

17086

Table 10 Catalyst 6500 Series Specifications

Specification	Number	Description
Miscellaneous protocols	1866	HTML
	2030	Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI
	2068	HTTP
Denial of service (DoS) protection	2267	Network Ingress Filtering
		ACLs: wire-speed
		ICMP and IP-option control
		IP broadcast forwarding control
		Rate limiting using ACLs
		Unicast Reverse Path Forwarding (RPF)
		Server load balancing with Layer 3 and Layer 4 protection
		SYN attack protection
		Session control
Network management	782	VLAN Trunking Protocol (VTP)
	783	TFTP
	854	Telnet
	951	BOOTP
	1155	Structure of Management Information (SMIv1)
	1156	TCP/IP MIB
	1157	Simple Network Management Protocol (SNMP)v1
	1212	MIB definitions
	1213	SNMP MIB II
	1215	SNMP traps
	1256	ICMP router discovery
	1285	Station management (SMT) 7.3
	1354	IP forwarding table MIB
	1493	Bridge MIB
	1516	Ethernet repeater MIB
	1573	Interface table MIB
	1643	Ethernet MIB
	1650	Ether-like MIB

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 680
Doc: 3702

17085

Table 10 Catalyst 6500 Series Specifications

Specification	Number	Description
	1657	BGPv4 MIB
	1724	RIPv2 MIB
	1757	RMON MIB
	1850	OSPFv2 MIB
	1901, 1907	SNMPv2c
	1908	SNMPv1/v2 coexistence
	2021	RMON2 probes
	2037	ENTITY-MIB
	2096	IP forwarding
	2233	Interface MIB
	2613	RMON analysis for switched networks (SMON) MIB
	2668	802.3 media attachment unit (MAU) MIB
	2787	VRRP MIB
	2925	Ping/Traceroute/NS Lookup MIB
		Sampled Netflow
		999 local messages
		BSD Syslog with multiple servers
		Configuration logging
		CISCO-CDP-MIB
		CISCO-COPS-CLIENT-MIB
		Cisco Discovery Protocol
		CISCO-ENTITY-FRU-CONTROL-MIB
		CISCO-PAGP-MIB
		CISCO-STACK-MIB
		CISCO-STP-Extensions-MIB
		Cisco Traffic Director Software
		CISCO-UDLDP-MIB
		CiscoView
		CISCO-VLAN-Bridge-MIB
		Cisco VLAN Director Software
		CISCO-VLAN-Membership-MIB

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 681
Doc: 3702

17084
2

Table 10 Catalyst 6500 Series Specifications

Specification	Number	Description
		CISCO-VTP-MIB
		Cisco Workgroup MIB
		SPAN and Remote SPAN (RSPAN)
		Hot Standby Routing Protocol (HSRP)
		HC-RMON
		HTML/HTTP management
		NetFlow v1 export
		RMON HP Open View
		SMON-MIB
		Standard Cisco IOS Software security capabilities: passwords and TACACS+
		Telnet client
		Telnet management
		Text-based CLI
		Web-based GUI Management Tools (CiscoWorks)
Security	1492	Terminal Access Controller Access Control System Plus (TACACS+)
	2138	Remote Authentication Dial-In User Service (RADIUS) authentication
		ACLs for Layers 2, 3, 4, and 7
		Access profiles on all routing protocols
		Access profiles on all management methods
		Media Access Control (MAC) address security/lockdown
		Network Address Translation (NAT)
		Network login (including DHCP/RADIUS integration)
		RADIUS accounting
		RADIUS per-command authentication
		Secure Copy Protocol (secure file transfer)

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 682
Doc: 3702

17083
2

Technical Support Services

Whether your company is a large organization, a commercial business, or a service provider, Cisco is committed to maximizing the return on your network investment. Cisco offers a portfolio of technical support services to help ensure that your Cisco products operate efficiently, remain highly available, and benefit from the most up-to-date system software.

The Cisco Technical Support Services organization offers the following features, providing network investment protection and minimal downtime for systems running mission-critical applications:

- Provides Cisco networking expertise online and on the telephone
- Creates a proactive support environment with software updates and upgrades as an ongoing integral part of your network operations, not merely a remedy when a failure or problem occurs
- Makes Cisco technical knowledge and resources available to you on demand
- Augments the resources of your technical staff to increase productivity
- Complements remote technical support with onsite hardware replacement

Cisco Technical Support Services include:

- Cisco SMARTnet™ support
- Cisco SMARTnet Onsite support
- Cisco Software Application Services, including Software Application Support and Software Application Support plus Upgrades

For more information, visit:
http://www.cisco.com/en/US/products/svcs/ps3034/serv_category_home.html

Additional Cisco Catalyst 6500 Series Information

For additional information about the following data sheets that describe Cisco Catalyst 6500 Series, supervisor engines, interface modules, SFM, and services modules, visit:

http://www.cisco.com/en/US/products/hw/switches/ps708/products_data_sheets_list.html

- Cisco Catalyst 6500 Series Supervisor Engine 1A and Supervisor Engine 2 Data Sheet
- Cisco Catalyst 6500 Series Supervisor Engine 720 Data Sheet
- Cisco Catalyst 6500 Series 10/100 and 10/100/1000 Ethernet Interface Modules Data Sheet
- Cisco Catalyst 6500 Series Gigabit Ethernet Interface Modules Data Sheet
- Cisco Catalyst 6500 Series 10 Gigabit Ethernet Interface Modules Data Sheet
- Cisco Catalyst 6500 Series FlexWAN Interface Modules Data Sheet
- Cisco Catalyst 6500 Series Switch Fabric Interface Modules Data Sheet
- Cisco Catalyst 6500 Series Content Services Module Data Sheet
- Cisco Catalyst 6500 Series Firewall Services Module Data Sheet
- Cisco Catalyst 6500 Series Network Application Module (NAM) Data Sheet
- Cisco Catalyst 6500 Series Intrusion Detection (IDS) Module Data Sheet
- Cisco Catalyst 6500 Series IPSec VPN Services Module Data Sheet
- Cisco Catalyst 6500 Series SSL Services Module Data Sheet

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 683
Doc: 3702

17082
L

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the **Cisco Web site at www.cisco.com/go/offices**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Catalyst, Cisco, Cisco Systems, Cisco IOS, the Cisco Systems logo, EtherChannel, and SMARTnet are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0304R)

MH/LW4273 0403

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 684
Nº Doc: 3702

ANEXO 1A

17081

CHAPTER 1

Product Overview

This chapter describes the Catalyst 6500 series switches and contains these sections:

- Catalyst 6503 Switch, page 1-2
- Catalyst 6506 Switch, page 1-4
- Catalyst 6509 Switch, page 1-7
- Catalyst 6509-NEB Switch, page 1-11
- Catalyst 6513 Switch, page 1-14
- System Features, page 1-17
- Fan Assembly, page 1-19
- Power Supplies, page 1-24

The Catalyst 6500 series switch chassis are listed in Table 1-1.

Table 1-1 Catalyst 6500 Series Switches

Catalyst 6500 Series Switch	Orientation/Number of Slots
Catalyst 6503	Horizontal 3-slot
Catalyst 6506	Horizontal 6-slot
Catalyst 6509	Horizontal 9-slot
Catalyst 6509-NEB	Vertical 9-slot
Catalyst 6513	Horizontal 13-slot

RQS nº 03/2005 - CN - CPMI - CORREIOS

Fls Nº 685

3702

Doc:

1-1080
L

Note In this publication, the term Catalyst 6500 series refers only to the switch chassis listed in Table 1-2. The Catalyst 6000 series switches (Catalyst 6006 switch and Catalyst 6009 switch) are described in a separate publication, the *Catalyst 6000 Series Switches Installation Guide*.

Note Throughout this publication, except where noted, the term *supervisor engine* is used to refer to Supervisor Engine 1, Supervisor Engine 2, and Supervisor Engine 720.

Catalyst 6503 Switch

The Catalyst 6503 switch is a 3-slot horizontally-aligned switch. The Catalyst 6503 switch supports the following:

- A supervisor engine with two gigabit interface uplinks and an optional redundant supervisor engine in one of the following configurations:
  - Two supervisor engines, each with no Multilayer Switch Feature Card (MSFC) and no Policy Feature Card (PFC)
  - Two supervisor engines, each configured with a PFC daughter card
  - Two supervisor engines, each configured with both an MSFC and a PFC daughter card

Note The uplink ports are fully functional on the redundant supervisor engine in standby mode.

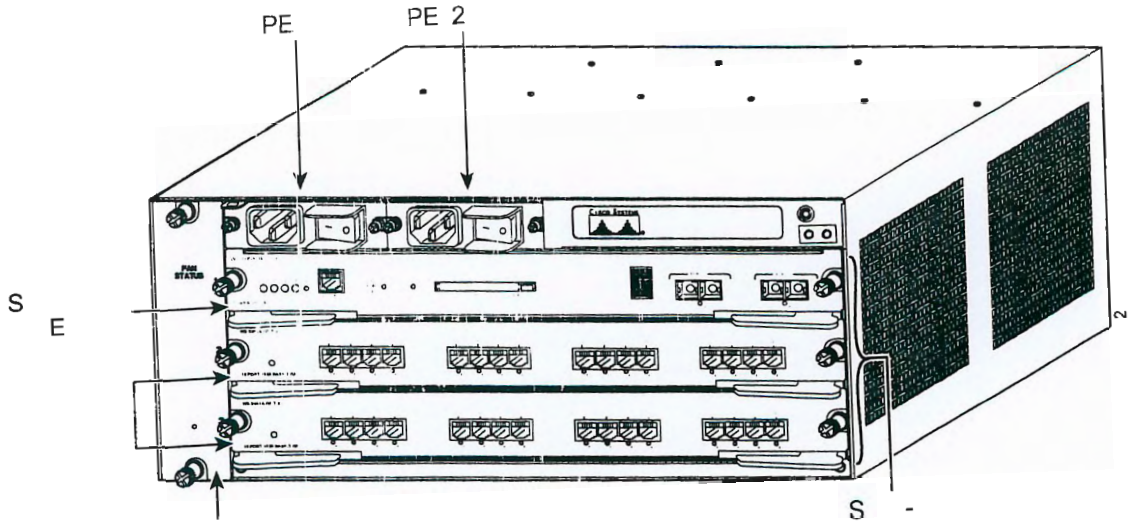
Note Both supervisor engines in a single chassis must be completely identical.

78-15722-01
RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 686
Nº 3702

17089

- Up to two hot-swappable Catalyst 6500 series modules:
  - The Switch Fabric Modules (WS-C6500-SFM and WS-X6500-SFM2) are not supported on the Catalyst 6503 switch.
  - The WS-X6816-GBIC 16-port Gigabit Ethernet fabric-enabled module is not supported on the Catalyst 6503 switch.
- Backplane bandwidth of 32 Gbps
- Hot-swappable fan assembly
- Two power entry modules (PEMs)
- Redundant AC-input or DC-input power supplies (950W power supply only)

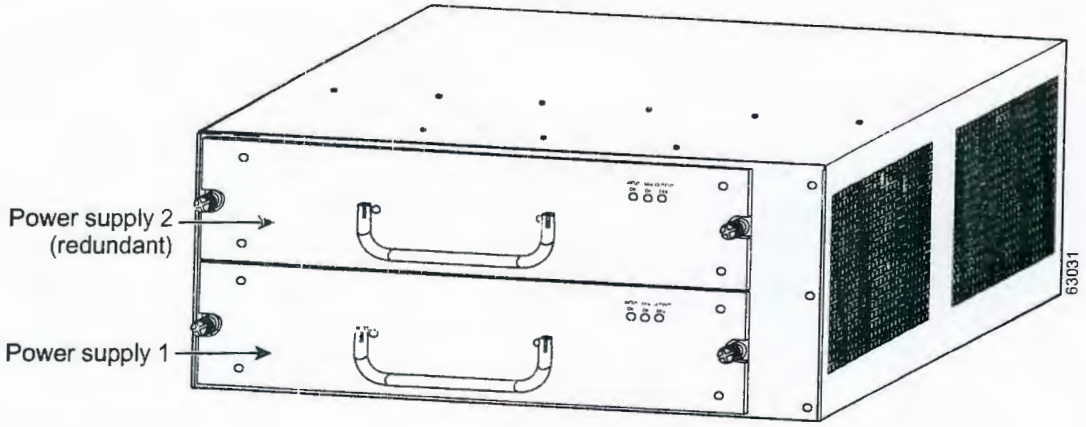
Figure 1-1 Catalyst 6503 Switch—Front View



R 1-3 /2005 - CN -
CPMI - CORREIOS
Fls Nº 687
Doc: 3702

12088

Figure 1-2 Catalyst 6503 Switch—Rear View



Catalyst 6506 Switch

The Catalyst 6506 switch chassis is a 6-slot horizontally-aligned chassis. The Catalyst 6506 switch supports the following:

- A supervisor engine with two Gigabit Ethernet uplink ports (slot 1)
- An optional redundant supervisor engine (slot 2)

Note Supervisor Engine 720 must be installed in chassis slots 5 or 6. Slots 1 and 2 are available for switching modules.

Note The uplink ports are fully functional on the redundant supervisor engine in standby mode.

10/03/2005 - CN -
CPMI - CORREIOS
Fls Nº 688
Doc: 3702

1708
2

Both supervisor engines in a single chassis must be completely identical. You can configure the redundant supervisor engines in a Catalyst 6506 switch in one of three configurations:

- Two supervisor engines, each with no Multilayer Switch Feature Card (MSFC) and no Policy Feature Card (PFC)
- Two supervisor engines, each configured with a PFC daughter card
- Two supervisor engines, each configured with both an MSFC and a PFC daughter card

- Up to five additional hot-swappable Catalyst 6500 series switching modules
  - Fabric-enabled module support provided in slots 2–6 (requires Switch Fabric Module)

Note Supervisor Engine 720 has built-in switching fabric and does not require that Switch Fabric Modules be installed in the chassis.

- Hot-swappable fan tray

Note The high capacity fan tray (WS-C6K-6SLOT-FAN2) must be installed when a Supervisor Engine 720 is installed in the chassis.

- Redundant AC-input or DC-input power supplies

Note When a Supervisor Engine 720 and the high capacity fan tray are installed, you must install 2500 W or higher capacity power supplies in the chassis.

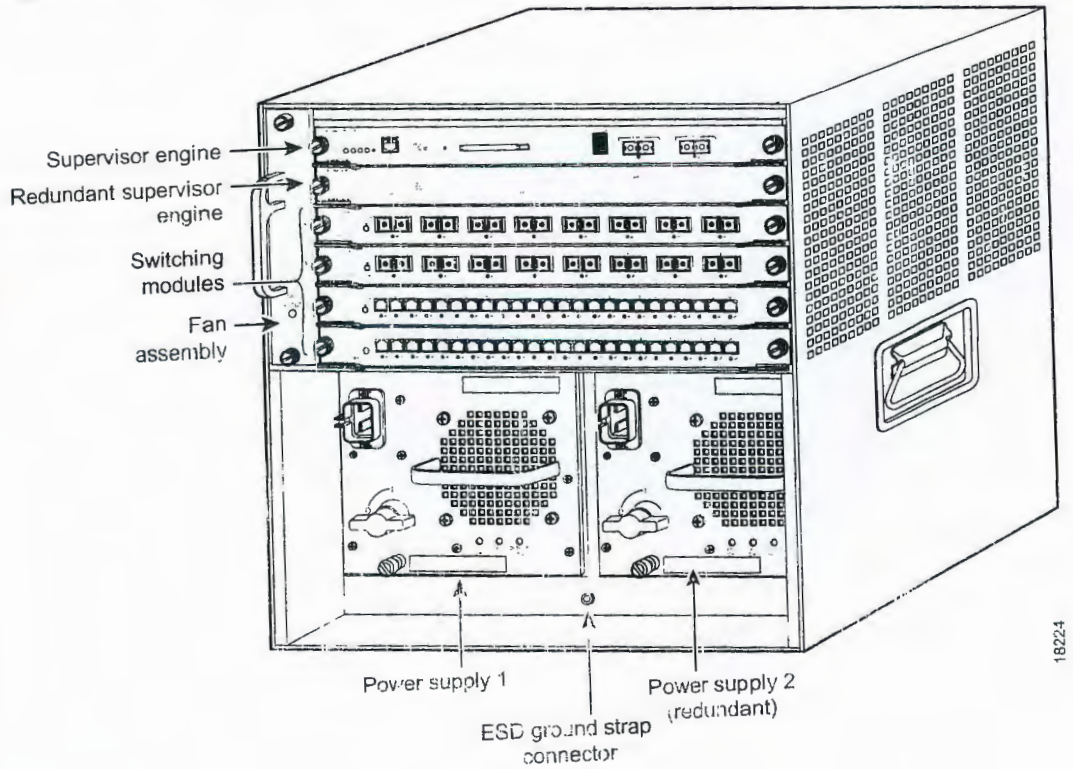
- Backplane bandwidth of 32 Gbps scalable up to 256 Gbps

Note Backplane bandwidth greater than 32 Gbps requires that you install either a Switch Fabric Module or a Supervisor Engine 720 in the switch chassis.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 689
Doc: 3702

17086
L

Figure 1-3 Catalyst 6506 Switch



ECT 08/2005 - CN - CPMI - CORREIOS
Fls Nº 690
Doc: 3702

17085
L

- A Switch Fabric Module (WS-C6500-SFM or WS-X6500-SFM2)
  - The Switch Fabric Module requires Supervisor Engine 2.

Note Switch Fabric Modules are not supported by Supervisor Engine 720.

  - You must install a Switch Fabric Module in either slot 5 or slot 6 of the Catalyst 6506 switch. For redundancy, you can install a standby Switch Fabric Module. The module first installed functions as the primary module. When you install two Switch Fabric Modules at the same time, the module in slot 5 acts as the primary module, and the module in slot 6 acts as the backup. If you reset the module in slot 5, the module in slot 6 becomes the primary module.
  - Mixing an SFM (WS-C6500-SFM) with an SFM2 (WS-X6500-SFM2) in the same Catalyst 6506, Catalyst 6509, or Catalyst 6509-NEB chassis is supported.
  - Fabric-enabled module support is provided in all slots. (A Switch Fabric Module is required.)

Catalyst 6509 Switch

The Catalyst 6509 switch chassis has nine horizontal slots that are numbered from top to bottom. (See Figure 1-4.) Slot 1 is reserved for the supervisor engine, which provides switching, local and remote management, and multiple gigabit uplink interfaces.

Slot 2 can contain an additional supervisor engine, which can act as a backup if the first supervisor engine fails. If a redundant supervisor engine is not required, slot 2 is available for a switching module.

For a detailed description of supervisor engine operation in a redundant configuration, refer to your software configuration guide.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 691
Doc 3702

17084
6

The Catalyst 6509 switch supports the following:

- A supervisor engine with two Gigabit Ethernet uplink ports and an optional redundant supervisor engine

Note Supervisor Engine 720 must be installed in chassis slots 5 or 6. Slots 1 and 2 are available for switching modules.

Note The uplink ports are fully functional on a redundant supervisor engine in standby mode.

Both supervisor engines in a single chassis must be completely identical. You can configure the redundant supervisor engines in a Catalyst 6500 series switch in one of three configurations:

  - Two supervisor engines, each with no MSFC and no PFC
  - Two supervisor engines, each configured with a PFC daughter card
  - Two supervisor engines, each configured with both an MSFC and a PFC daughter card

- Backplane bandwidth scalable up to 256 Gbps

Note Backplane bandwidth greater than 32 Gbps requires that you install a Switch Fabric Module or a Supervisor Engine 720 in the Catalyst 6509-NEB switch chassis.

- A Switch Fabric Module (WS-C6500-SFM or WS-X6500-SFM2)
  - The Switch Fabric Modules require Supervisor Engine 2.
  - You must install the Switch Fabric Module in either slot 5 or slot 6 of the Catalyst 6509-NEB switch. For redundancy, you can install a standby Switch Fabric Module. The module first installed functions as the primary module. When you install two Switch Fabric Modules at the same time, the module in slot 5 acts as the primary module, and the module in slot 6 acts as the backup. If you reset the module in slot 5, the module in slot 6 becomes the primary module.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 692
Nº 3702
Doc:

17083
2

- Mixing an SFM (WS-C6500-SFM) with an SFM2 (WS-X6500-SFM2) in the same Catalyst 6506, Catalyst 6509, or Catalyst 6509-NEB chassis is supported.

Note Supervisor Engine 720 has built-in switching fabric and does not require that Switch Fabric Modules be installed in the chassis.

- Up to eight additional Catalyst 6500 series modules
  - Fabric-enabled module support provided in all slots (requires Switch Fabric Module)
- Hot-swappable fan assembly

Note The high capacity fan tray (WS-C6K-9SLOT-FAN2) must be installed when a Supervisor Engine 720 is installed in the chassis.

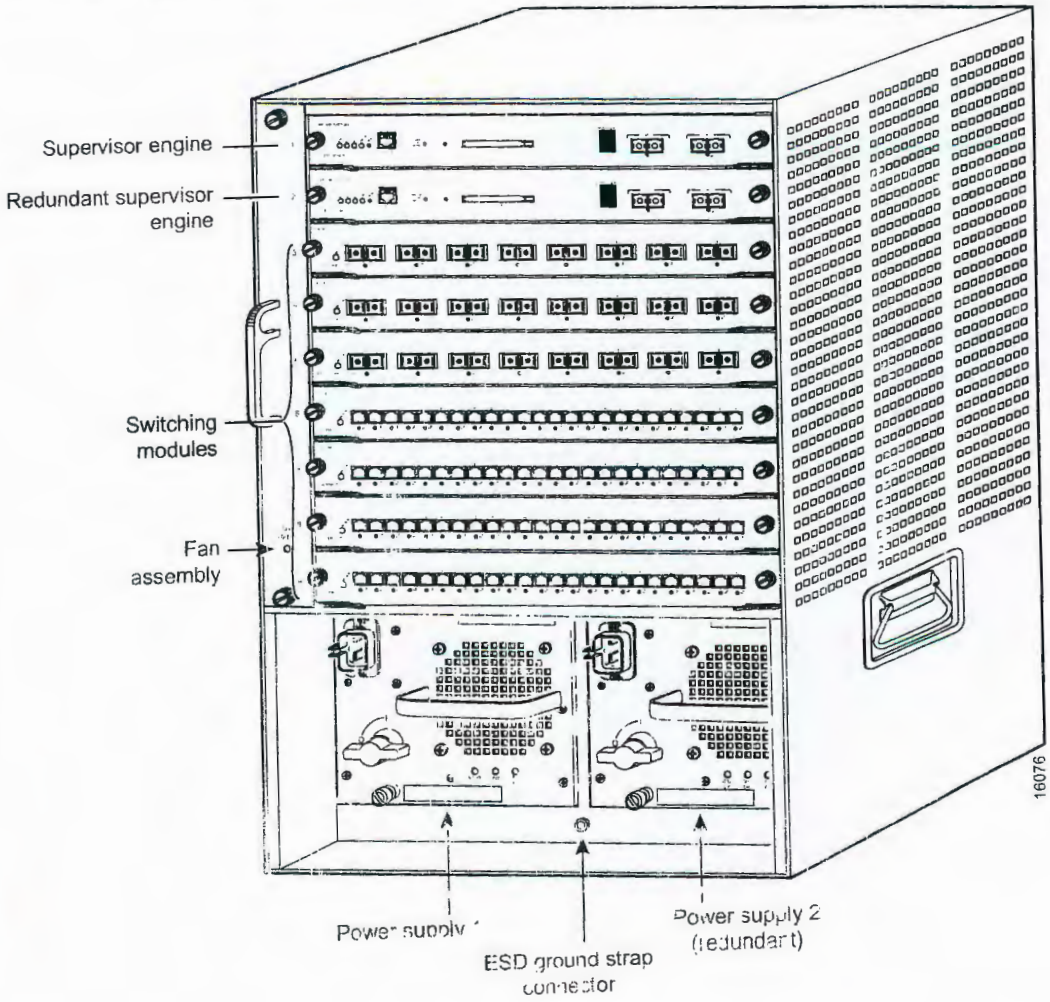
- Redundant AC-input or DC-input power supplies

Note When a Supervisor Engine 720 and the high capacity fan tray are installed, you must install 2500 W or higher capacity power supplies in the chassis.

3/2005 - CN -
CPMI - CORREIOS
Fls Nº 693
Nº Doc 3702

17082
2

Figure 1-4 Catalyst 6509 Switch



RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 694
Nº 3702
Doc:

17081

Catalyst 6509-NEB Switch

The Catalyst 6509-NEB switch chassis has nine vertical slots that are numbered from right to left. (See Figure 1-5.) Slot 1 is reserved for the supervisor engine, which provides switching, local and remote management, and multiple gigabit uplink interfaces.

Slot 2 can contain an additional supervisor engine, which can act as a backup if the first supervisor engine fails. If a redundant supervisor engine is not required, slot 2 is available for a switching module.

For a detailed description of supervisor engine operation in a redundant configuration, refer to your software configuration guide.

The Catalyst 6509-NEB switch supports the following:

- A supervisor engine with two Gigabit Ethernet uplink ports and an optional redundant supervisor engine

  Note Supervisor Engine 720 must be installed in slots 5 or 6. Slots 1 and 2 are available for switching modules.

  Note The uplink ports are fully functional on the redundant supervisor engine in standby mode.

  Both supervisor engines in a single chassis must be completely identical. You can configure the redundant supervisor engines in a Catalyst 6500 series switch in one of three configurations:

  - Two supervisor engines, each with no MSFC and no PFC
  - Two supervisor engines, each configured with a PFC daughter card
  - Two supervisor engines, each configured with both an MSFC and a PFC daughter card

- Backplane bandwidth scalable up to 256 Gbps

RC[redacted]2005 - CN - CPMI - CORREIOS
Fls Nº 695
Nº 3702
Doc:

17080
L

Note Backplane bandwidth greater than 32 Gbps requires that you install either a Switch Fabric Module or a Supervisor Engine 720 in the Catalyst 6509-NEB switch chassis.

- A Switch Fabric Module (WS-C6500-SFM or WS-X6500-SFM2)
  - The Switch Fabric Modules require Supervisor Engine 2.
  - You must install the Switch Fabric Module in either slot 5 or slot 6 of the Catalyst 6509-NEB switch. For redundancy, you can install a standby Switch Fabric Module. The module first installed functions as the primary module. When you install two Switch Fabric Modules at the same time, the module in slot 5 acts as the primary module, and the module in slot 6 acts as the backup. If you reset the module in slot 5, the module in slot 6 becomes the primary module.
  - Mixing an SFM (WS-C6500-SFM) with an SFM2 (WS-X6500-SFM2) in the same Catalyst 6506, Catalyst 6509, or Catalyst 6509-NEB chassis is supported.

Note The Supervisor Engine has built-in switching fabric and does not require that Switch Fabric Modules be installed in the chassis.

- Up to eight additional Catalyst 6500 series hot-swappable modules
  - Fabric-enabled module support provided in all slots (requires Switch Fabric Module or Supervisor Engine 720)
- Hot-swappable fan assembly

Note The high capacity fan tray (WS-C6509-NEB-FAN2) must be installed when a Supervisor Engine 720 is installed in the chassis.

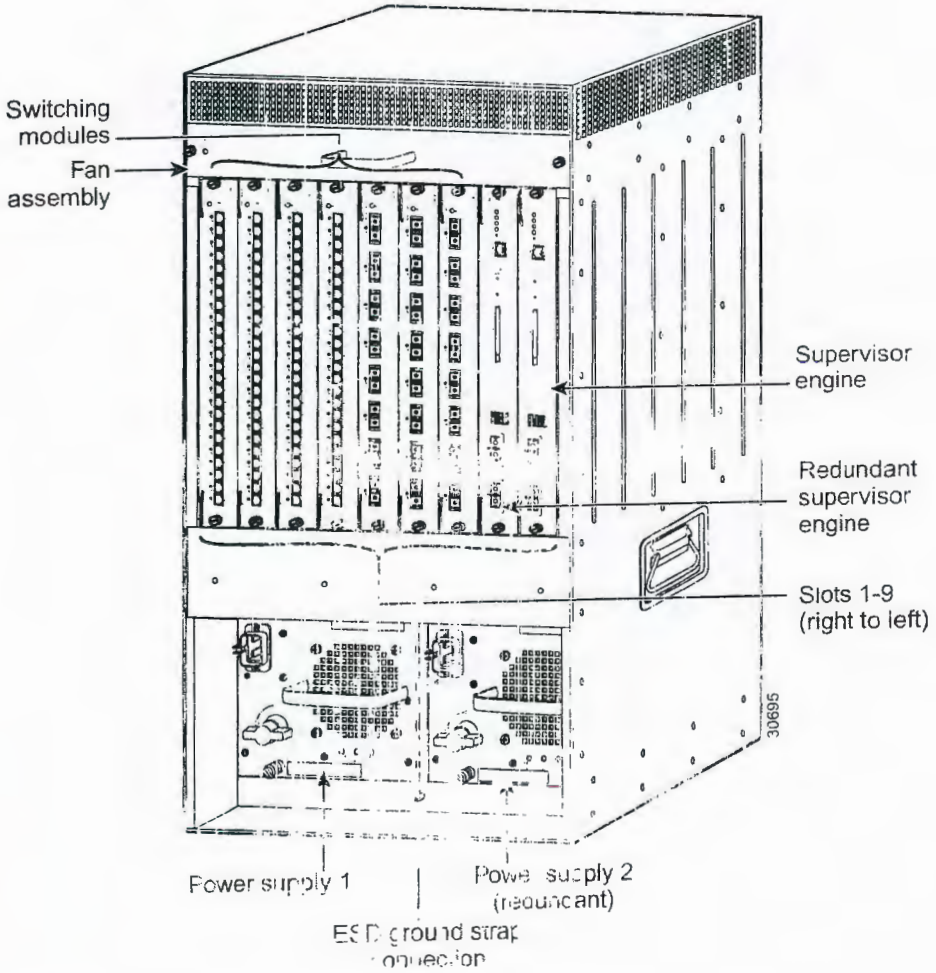
- Redundant AC-input or DC-input power supplies

Note When a Supervisor Engine 720 and the high capacity fan tray are installed, you must install 2500 W or larger capacity power supplies in the chassis.

ECT nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 696
Nº Doc: 3702

17079
L

Figure 1-5 Catalyst 6509-NEB Switch



RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 697
Doc 3702

17078
2

Catalyst 6513 Switch

The Catalyst 6513 switch chassis has 13 slots. (See Figure 1-6.) Slot 1 is reserved for a Supervisor Engine 2, which provides switching, local and remote management, and multiple gigabit uplink interfaces.

Note The Catalyst 6513 switch requires a Supervisor Engine 2 or Supervisor Engine 720.

Slot 2 can contain an additional Supervisor Engine 2, which can act as a backup if the primary supervisor engine fails. If a redundant supervisor engine is not required, slot 2 is available for a switching module.

Note Supervisor Engine 720 must be installed in slots 7 or 8.

For a detailed description of supervisor engine operation in a redundant configuration, refer to your software configuration guide

The Catalyst 6513 switch supports the following:

- A Supervisor Engine 2 with two Gigabit Ethernet uplink ports and an optional redundant Supervisor Engine 2

  Note The uplink ports are fully functional on the redundant Supervisor Engine 2 in standby mode.

  Both supervisor engines in a single chassis must be completely identical. You can configure the redundant supervisor engines in a Catalyst 6500 series switch in one of three configurations:

  - Two supervisor engines, each with no MSFC and no PFC
  - Two supervisor engines, each configured with a PFC daughter card
  - Two supervisor engines, each configured with both an MSFC and a PFC daughter card
- Backplane bandwidth scalable up to 256 Gbps

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 698
Nº 3702

17077
L

Note Backplane bandwidth greater than 32 Gbps requires that you install either a Switch Fabric Module or Supervisor Engine 720 in the Catalyst 6513 switch chassis.

- A Switch Fabric Module (supports WS-X6500-SFM2 only)
  - The Switch Fabric Module requires Supervisor Engine 2. Supervisor Engine 1A does not support the Switch Fabric Module.
  - You must install the Switch Fabric Module in slot 7 or slot 8 of the Catalyst 6513 switch. For redundancy, you can install a standby Switch Fabric Module. The module first installed functions as the primary module. When you install two Switch Fabric Modules at the same time, the module in slot 7 acts as the primary module, and the module in slot 8 acts as the backup. If you reset the module in slot 7, the module in slot 8 becomes the primary module.

Note Supervisor Engine 720 has built-in switching fabric and does not require that Switching Fabric Modules be installed in the chassis.

- Up to 12 additional hot-swappable switching modules
  - Fabric-enabled module support provided in all slots (requires a Switch Fabric Module (WS-X6500-SFM2) or Supervisor Engine 720 be installed)
  - Dual Fabric connectivity supported in slots 9–13 (requires a Switch Fabric Module (WS-X6500-SFM2) or Supervisor Engine 720 be installed)
- Hot-swappable fan assembly

Note The high capacity fan tray (WS-C6K-13SLT-FAN2) must be installed when a Supervisor Engine 720 is installed in the chassis.

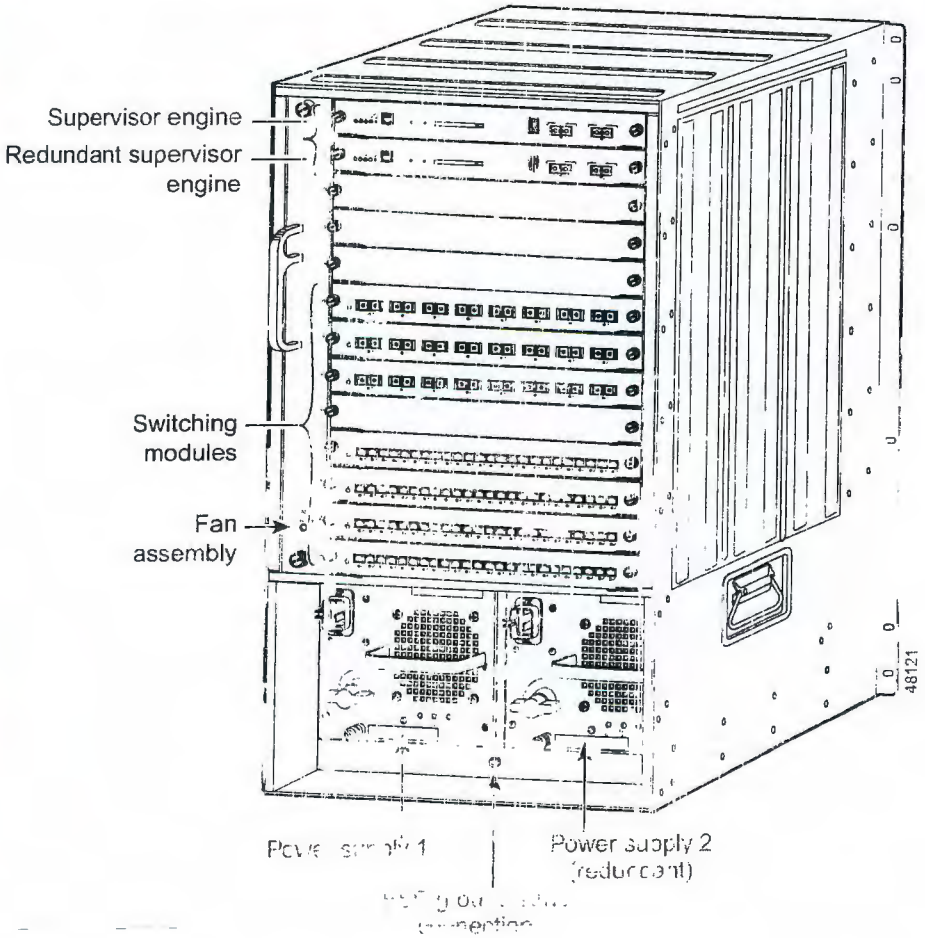
- Redundant AC-input or DC-input power supplies

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 699
Doc: 3702

17076

Note When a Supervisor Engine 720 and the higher capacity fan tray are installed, you must install 2500 W or higher capacity power supplies in the chassis.

Figure 1-6 Catalyst 6513 Switch



78-15722-01
RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 700
Doc: 3702

17075

System Features

This section describes the hardware features for the Catalyst 6500 series switches. For software descriptions, refer to your software configuration guide. For module descriptions and installation procedures, refer to the *Catalyst 6500 Series Switches Module Installation Guide*.

Port Density

Table 1-2 lists the port densities of the Catalyst 6500 series switches.

Table 1-2 Catalyst 6500 Series Port Density

Architecture	Catalyst 6500 Series Switches
Number of 10 Gigabit Ethernet Ports	2 (3 slots) Catalyst 6503 switch 5 (6 slots) Catalyst 6506 switch 8 (9 slots) Catalyst 6509 switch 12 (13 slots) Catalyst 6513 switch
Number of Gigabit Ethernet Ports	34 (3 slots) Catalyst 6503 switch 82 (6 slots) Catalyst 6506 switch 130 (9 slots) Catalyst 6509 switch 194 (13 slots) Catalyst 6513 switch
Number of 100BASE-FX Ethernet Ports	96 (3 slots) Catalyst 6503 switch 120 (6 slots) Catalyst 6506 switch 192 (9 slots) Catalyst 6509 switch 288 (13 slots) Catalyst 6513 switch
Number of 10/100 Ethernet Ports	96 (3 slots) Catalyst 6503 switch 240 (6 slots) Catalyst 6506 switch 384 (9 slots) Catalyst 6509 switch 576 (13 slots) Catalyst 6513 switch
Number of 10BASE-FL Ethernet Ports	48 (3 slots) Catalyst 6503 switch 120 (6 slots) Catalyst 6506 switch 192 (9 slots) Catalyst 6509 switch 288 (13 slots) Catalyst 6513 switch

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 701
Doc: 702

12074
L

Table 1-2 Catalyst 6500 Series Port Density (continued)

Architecture	Catalyst 6500 Series Switches
Number of ATM OC-12 Ports	2 (3 slots) Catalyst 6503 switch 5 (6 slots) Catalyst 6506 switch 8 (9 slots) Catalyst 6509 switch 12 (13 slots) Catalyst 6513 switch
Number of FlexWAN Modules	2 (3 slots) Catalyst 6503 switch 5 (6 slots) Catalyst 6506 switch 8 (9 slots) Catalyst 6509 switch 12 (13 slots) Catalyst 6513 switch

Redundancy

Catalyst 6500 series switches have these redundancy features:

- Ability to house two hot-swappable supervisor engines
- Ability to house two fully redundant, AC-input or DC-input, load-sharing power supplies

Note In certain configurations, the power supplies are not fully redundant. Refer to the "Power Supply Redundancy" section on page 1-29.

- A hot-swappable fan assembly containing multiple fans
- Redundant backplane-mounted clock modules
- Redundant backplane-mounted voltage termination (VTT) modules

Component Hot Swapping

You can hot swap all modules (including the supervisor engine if you have a redundant supervisor engine) and the fan assembly. You can add, replace, or remove modules without interrupting the system power or causing other software or interfaces to shut down.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 702
Nº 3702
Doc:

17073
2

Fan Assembly

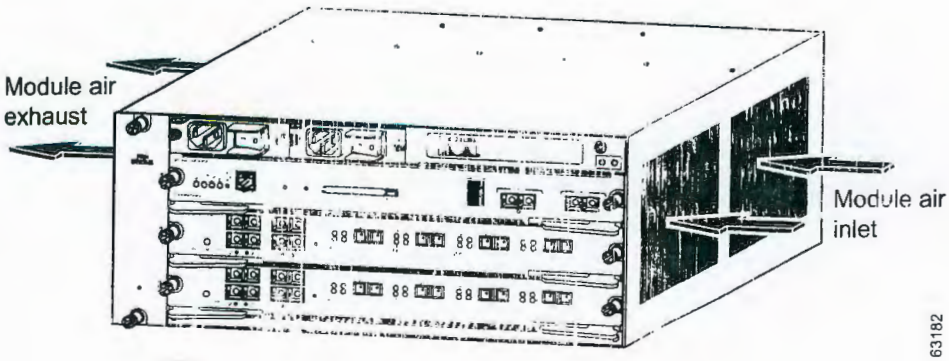
The system fan assembly is located in the chassis and provides cooling air for the supervisor engine and the switching modules. The following figures show the direction of airflow into and out of the switch: Figure 1-7 (Catalyst 6503 switch), Figure 1-8 (Catalyst 6506 switch), Figure 1-9 (Catalyst 6509 switch), Figure 1-10 (Catalyst 6509-NEB switch), and Figure 1-11 (Catalyst 6513 switch). Sensors on the supervisor engine monitor the internal air temperatures. If the air temperature exceeds a preset threshold, the environmental monitor displays warning messages.

Note We recommend that you maintain a minimum air space of 6 inches (15 cm) between walls and the chassis air vents and a minimum horizontal separation of 12 inches (30.5 cm) between two chassis to prevent overheating.

If an individual fan within the assembly fails, the FAN STATUS LED turns red. Individual fans cannot be replaced. To replace a fan assembly, see the "Removing and Replacing the Fan Assembly" section on page 5-35.

Refer to your software configuration guide for information on environmental monitoring.

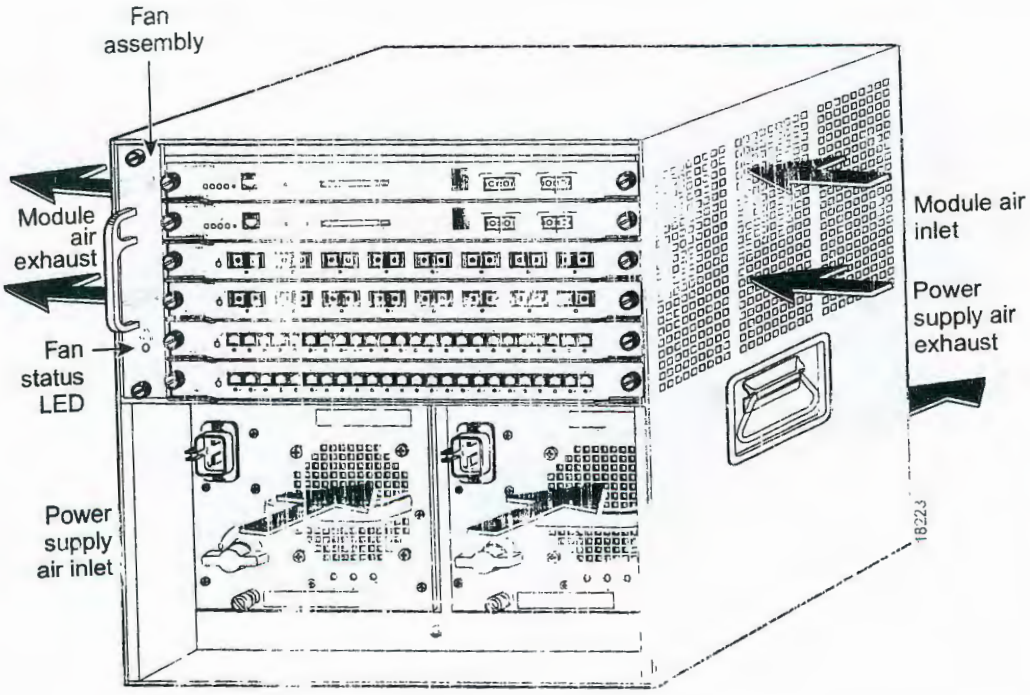
Figure 1-7 Catalyst 6503 Switch Internal Airflow



1-19
RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 703
Doc 3702

17072
L

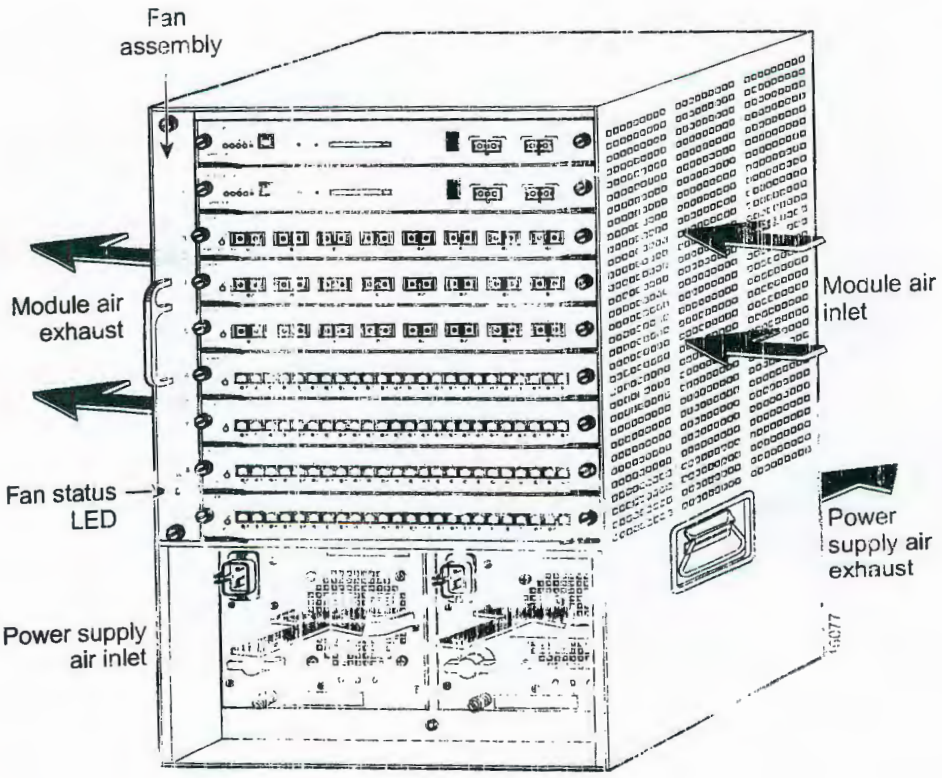
Figure 1-8 Catalyst 6[illegible] Switch Internal Airflow



RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 704
Doc: 3702

17071
L

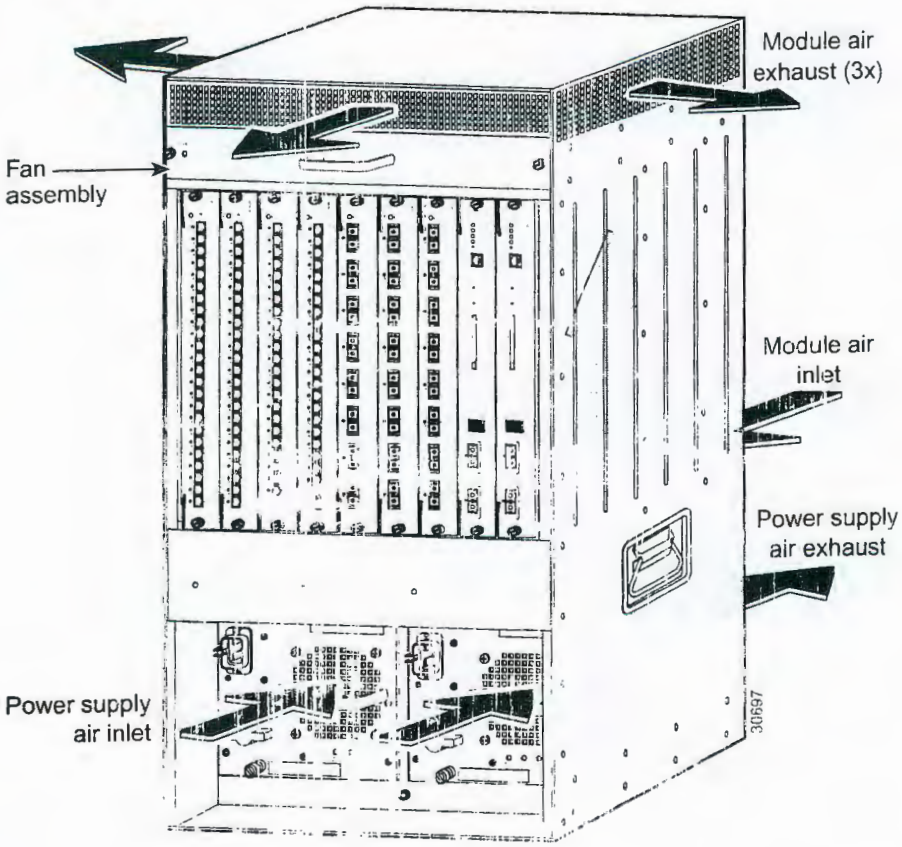
Figure 1-9 Catalyst 6500 Switch Internal Airflow



RQS 1-21 005 - CN -
CPMI - CORREIOS
Fls Nº 705
Doc: 3702

17070
L

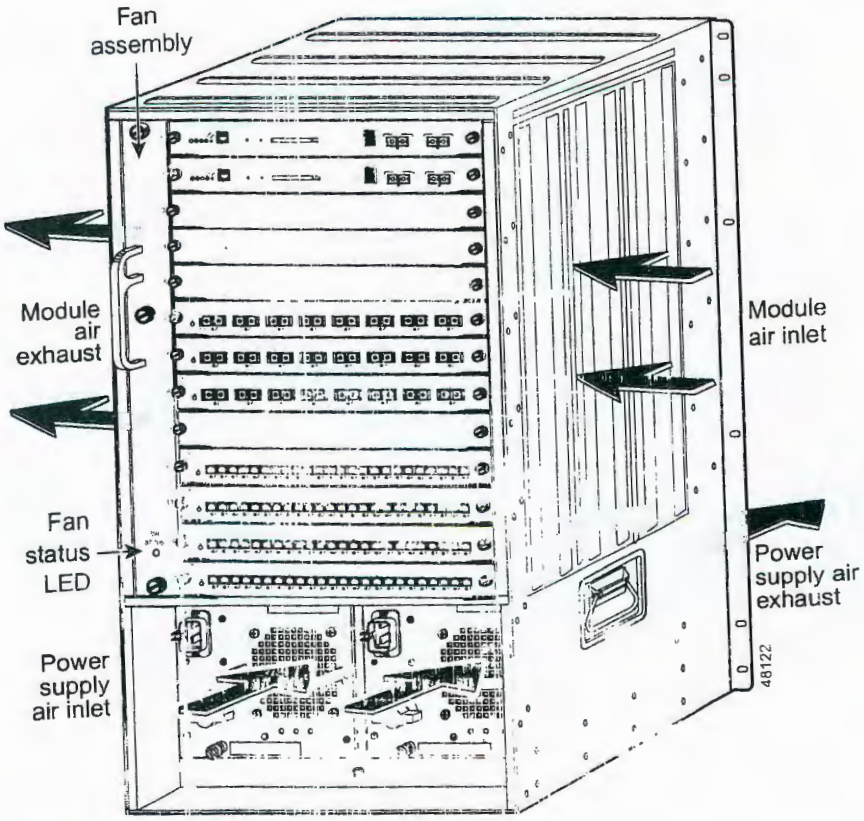
Figure 1-10 Catalyst 6509-NEB Switch Internal Airflow



RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 706
Doc: 3702

17069
L

Figure 1-11 Catalyst 6513 Switch Internal Airflow



RQS 05 - CN - CPMI - CORREIOS
Fls Nº 707
Doc 3702

17068

Power Supplies

Catalyst 6500 series switch power supplies are available in five power ratings:

- 950 W—AC and DC input (PWR-950-AC and PWR-950-DC) (for use with the Catalyst 6503 switch only)
- 1000 W—AC input only (WS-CAC-1000W)
- 1300 W—AC and DC input (WS-CAC-1300W and WS-CDC-1300W)
- 2500 W—AC and DC input (WS-CAC-2500W and WS-CDC-2500W)
- 4000 W—AC input only (WS-CAC-4000W-US1 or WS-CAC-4000W-INT)

950 W Power Supply (PWR-950-AC and PWR-950-DC)

Note The 950 W AC-input and DC-input power supplies can be installed in the Catalyst 6503 switch chassis only. They cannot be installed in any other Catalyst 6500 series switch chassis.

The 950 W power supplies (see Figure 1-12) do not connect directly to source AC or DC power. Use a power entry module (PEM), located on the front of the chassis, to connect the site power source to the power supply located in the back of the chassis.

The AC-input PEM (shown in Figure 1-13) and DC-input PEM (shown in Figure 1-14) provide an input power connection on the front of the router chassis to connect the site power source to the power supply. You can connect the DC-input power supply to the power source with heavy gauge wiring connected to a terminal block. The wire gauge size is determined by local electrical codes and restrictions.

Note The power cord is not shown in Figure 1-13.

The PEMs have an illuminated power switch (AC-input only), current protection, surge and EMI suppression, and filtering functions.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 708
Doc: 3702

17067
L

Figure 1-12 Catalyst 6503 950 W AC- and DC-Input Power Supplies

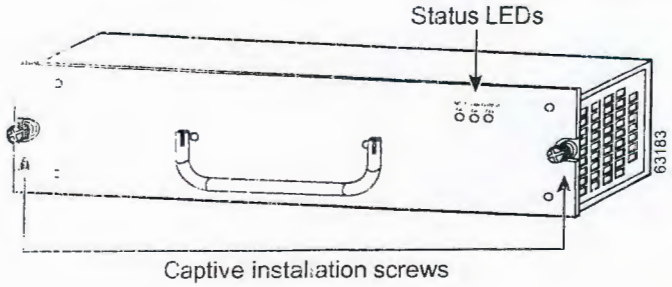


Figure 1-13 Catalyst 6503 AC Power Entry Module (PEM)

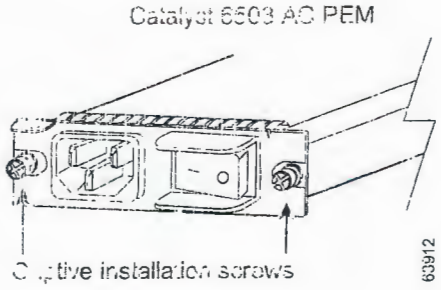
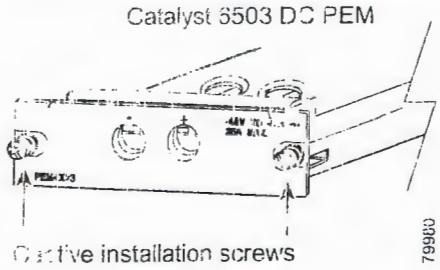


Figure 1-14 Catalyst 6503 DC Power Entry Module (PEM)



RQS nº 03/2005 - CN -
CPMI 1-25 RREIOS
Fls Nº 709
Doc. 3702

17066
L

1000 W, 1300 W, 2500 W, and 4000 W Power Supplies

The 1000 W, 1300 W, 2500 W, and 4000 W AC-input and DC-input power supplies have the same form factor and designed for use in the Catalyst 6500 series switches

Note The 1000 W, 1300 W, 2500 W, and 4000 W power supplies have a different form factor and cannot be used in the Catalyst 6503 series switch.

Catalyst 6500 series chassis power supply configurations for the 1000 W, 1300 W, 2500 W and 4000 W power supplies are shown in Table 1-3.

Table 1-7 Catalyst 6500 Series Power Supply Configurations

Catalyst 6500 Series Switch	Power Supply Configurations
Catalyst 6506	1000 W AC-input
	1300 W AC- and DC-input
	2500 W AC- and DC-input
Catalyst 6509	1300 W AC- and DC-input
	2500 W AC- and DC-input
	4000 W AC-input
Catalyst 6509-NEB	1300 W AC- and DC-input
	2500 W AC- and DC-input
	4000 W AC-input
Catalyst 6513	2500 W AC- and DC-input
	4000 W AC-input

Catalyst 6500 series switches support redundant AC-input and DC-input power supplies. Unlike the Catalyst 4000 family and Catalyst 5000 family switches, the Catalyst 6500 series switches allow you to mix AC-input and DC-input power supplies in the same chassis

0012005 - CN - CPMI - CORREIOS
Fls Nº 710
Doc: 3702

Many telco organizations require a -48 VDC power supply to accommodate their power distribution systems. From an operational perspective, the DC-input power supply has the same characteristics as the AC-input version.

The AC-input power supply (see Figure 1-15) has a detachable power cord (except for the WS-CAC-4000W) that allows you to connect each power supply to the site power source. You can connect the DC-input power supply (see Figure 1-16) to the power source with heavy gauge wiring connected to a terminal block. The wire gauge size is determined by local electrical codes and restrictions.

Note The power cord is not shown in Figure 1-15.

Note With a fully populated Catalyst 6513 switch, two 2500 W power supplies are not fully redundant. If you run the 2500 W power supply at the low range input (100 to 120 VAC), it is not redundant in a fully populated Catalyst 6509 or Catalyst 6509-NEB switch.

Note The 2500 W AC-input power supply needs 220 VAC to deliver 2500 W of power. When powered with 110 VAC, it delivers only 1300 W. In addition, the power supply needs 16 A, regardless of whether it is plugged into 110 VAC or 220 VAC.

For complete power specifications, see Appendix A, "Technical Specifications."

03/2005 - CN - CPMI - CORREIOS
Fls Nº 711
Doc: 3702

17069
L

Figure 1-15 AC-Input Power Supply

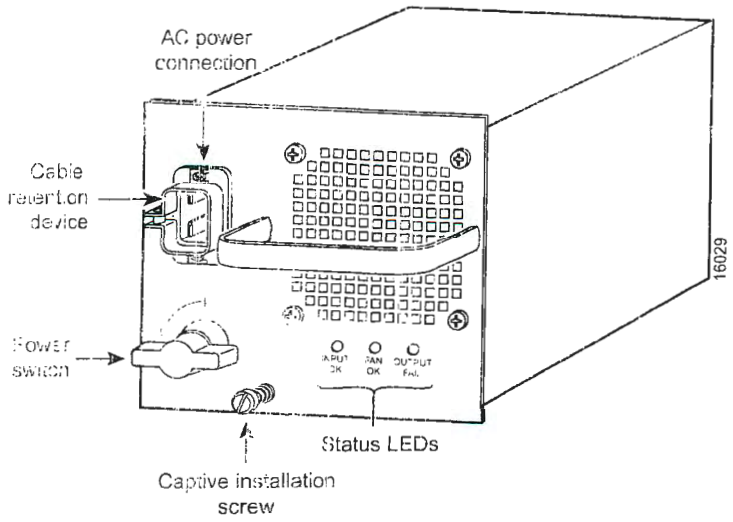
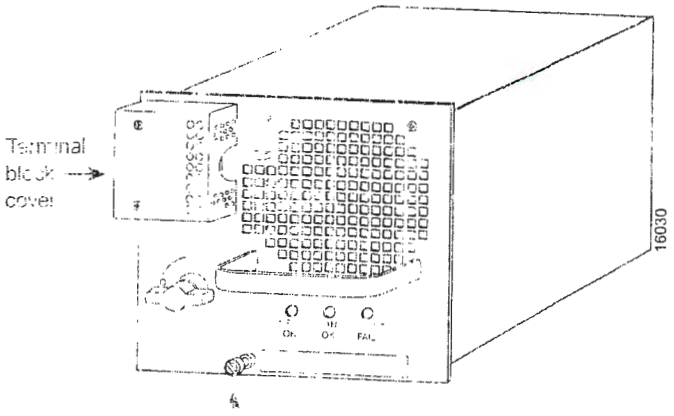


Figure 1-16 DC-Input Power Supply



Captive installation screw

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 712
Doc: 3702

17063
L

Power Supply Redundancy

Catalyst 6500 series modules have different power requirements. Depending upon the wattage of the power supply, certain switch configurations might require more power than a single power supply can provide. Although the power management feature allows you to power all installed modules with two power supplies, redundancy is not supported in this configuration. Redundant and nonredundant power configurations are summarized in Table 1-4. The effects of changing the power supply configurations are summarized in Table 1-5.

Note For proper load sharing operation in a redundant power supply configuration, you must install two modules in the chassis. If you fail to install two modules, you might receive spurious OUTPUT FAIL indications on the power supply.

B/2005 - CN -
CPMI - CORREIOS
Fls Nº 713
Doc: 3702

17062
L

Table 1-4 Power Supply Redundancy

If you have two power supplies of	and redundancy is	Then
Equal wattage	Enabled	The total power drawn from both supplies is never greater than the capability of one supply. If one supply malfunctions, the other supply can take over the entire system load. Each power supply provides approximately half of the required power to the system. Load sharing and redundancy are enabled automatically; no software configuration is required.
Unequal wattage	Enabled	Both power supplies come online, but a syslog message displays that the lower wattage power supply will be disabled. If the active power supply fails, the system shuts down. The lower wattage power supply must then be manually turned on. The lower wattage power supply selectively powers up the modules so that the capacity of the power supply is not exceeded.
Equal or unequal wattage	Disabled	The total power available to the system is approximately 167 percent of the lower wattage power supply. The system powers up as many modules as the combined capacity allows. If the higher wattage power supply fails, the lower wattage supply might also shut down due to overcurrent protection, thus preventing damage to the lower wattage power supply.

ROS A° 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 714
Doc: 3702

12061
L

Table 1-5 Effects of Power Supply Configuration Changes

Configuration Change	Effect
Redundant to nonredundant	• System log and syslog messages are generated. • System power is increased to approximately 167 percent of the lower wattage power supply. • The modules marked as *power-deny* in the **show module** Status field are brought up if there is sufficient power.
Nonredundant to redundant	• System log and syslog messages are generated. • System power is the power capability of the larger wattage supply. • If there is not enough power for all previously powered-up modules, some modules are powered down and marked as *power-deny* in the **show module** Status field.
Equal wattage power supply is inserted with redundancy enabled	• System log and syslog messages are generated. • System power equals the power capability of one supply (both supplies provide approximately one half of the total current). • No change in the module status because the power capability is unchanged.
Equal wattage power supply is inserted with redundancy disabled	• System log and syslog messages are generated. • System power is the combined power capability of both supplies. • The modules marked as *power-deny* in the **show module** Status field are brought up if there is sufficient power.
Higher wattage power supply is inserted with redundancy enabled	• System log and syslog messages are generated. • The system disables the lower wattage power supply; the higher wattage supply powers the system.
Lower wattage power supply is inserted with redundancy enabled	• System log and syslog messages are generated. • The system disables the lower wattage power supply; the higher wattage supply powers the system..

1-31 03/2005 - CN - CPMI - CORREIOS
Fls Nº 715
Doc 3702

17060

Table 1-5 Effects of Power Supply Configuration Changes (continued)

Higher or lower wattage power supply is inserted with redundancy disabled	• System log and syslog messages are generated. • System power is increased to the combined power capability of both supplies. • The modules marked as *power-deny* in the **show module** Status field are brought up if there is sufficient power.
Power supply is removed with redundancy enabled	• System log and syslog messages are generated. • If the power supplies are of equal wattage, there is no change in the module status because the power capability is unchanged. If the power supplies are of unequal wattage and the lower wattage supply is removed, there is no change in the module status. If the power supplies are of unequal wattage and the higher wattage supply is removed, the lower wattage power supply must be manually turned on. (The system had previously turned off the lower wattage power supply.)
Power supply is removed with redundancy disabled	• System log and syslog messages are generated. • System power is decreased to the power capability of one supply. • If there is not enough power for all previously powered-up modules, some modules are powered down and marked as *power-deny* in the **show module** Status field.
System is booted with power supplies of different wattage installed and redundancy enabled	• System log and syslog messages are generated. • The lower wattage supply is disabled.
System is booted with power supplies of equal or different wattage installed and redundancy disabled	• System log and syslog messages are generated. • System power equals the combined power capability of both supplies. • The system powers up as many modules as the combined capacity allows.

You can change the configuration of the power supplies to redundant or nonredundant at any time. If you switch from a redundant to a nonredundant configuration, both power supplies are enabled (even a power supply that was disabled because it was of a lower wattage than the other power supply). If you

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 716
Nº 3702
Doc:

17059
L

change from a nonredundant to a redundant configuration, both power supplies are initially enabled, and if they are of the same wattage, remain enabled. If they are of different wattage, a syslog message displays and the lower wattage supply is disabled.

For additional information about the power management feature and individual module power consumption, refer to your software configuration guide.

Environmental Monitoring of the Power Supply

The environmental monitoring and reporting functions allow you to maintain normal system operation by resolving adverse environmental conditions prior to loss of operation.

The power supplies monitor their own internal temperature and voltages. In the event of excessive internal temperature, the power supply will shut down to prevent damage. When the power supply returns to a safe operating temperature, it will restart. In the event of an abnormal voltage on one or more outputs of the power supplies the OUTPUT FAIL LED will light. Substantial overvoltage conditions can lead to a power supply shutdown.

The power supply front panel LEDs are described in Table 1-6.

For more information about the environmental monitoring feature, refer to your software configuration guide.

ROS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 717
Doc: 3702

17058
L

Table 1-6 Power Supply Front Panel LEDs

LED	Description
INPUT OK	AC-input power supplies: • Green when the input voltage is OK (85 VAC or greater) • Off when the input voltage falls below 70 VAC or if the power supply shuts down DC-input power supplies: • Green when the input voltage is OK (–40.5 VDC or greater) • Off when the input voltage falls below –33 VDC or if the power supply shuts down
FAN OK	Green when the power supply fan is operating properly. Red when a power supply fan failure is detected.
OUTPUT FAIL	Red when there is a problem with one or more of the DC-output voltages of the power supply

Power Supply Fan Assembly

The power supplies have a built-in fan; air enters the front of the fan (power-input end) and exits through the back. An air dam keeps the airflow separate from the rest of the chassis, which is cooled by the system fan assembly.

Power supply fans are not field-replaceable; the power supply must be replaced. To replace a power supply, see the "Removing and Replacing the 1000 W, 1300 W, 2500 W, and 4000 W Power Supplies" section on page 5-20.

ECT 08/2005 - CN -
78-16722-01
CPMI - CORREIOS
Fls Nº 718
Doc: 3702

ANEXO (2)

17057
L

Cisco Systems

Data Sheet

Cisco Catalyst 6500 **Supervisor** Engines 1A and 2

As Cisco's premier modular multilayer switch, the Catalyst® 6500 Series delivers secure, converged services from the wiring closet to the core, to the data center to the WAN edge.

The supervisor engines for the Catalyst 6500 Series deliver the latest advanced switching technology with proven Cisco software to power a new generation of scalable and intelligent multilayer switching solutions for both enterprise and service provider environments. Designed to integrate data, voice, and video into a single platform for fully integrated IP communications, the Catalyst 6500 Series supervisor engines enable intelligent, resilient, scalable, and secure high performance multilayer switching solutions.

The widely deployed Supervisor Engine 1A and Supervisor Engine 2 are used in wiring closets, distribution/core, data center and WAN edge configurations enabling the seamless integration of advanced services such as security, voice and content into a converged network that reduces the total cost of ownership. And the new Supervisor Engine 720 is ideally suited for high performance core, data center and metro Ethernet deployments with its scalable performance of up to 400 million packets per second using a 720Gbps switch fabric.

By sharing a common set of interfaces, operating system and management tools, the Catalyst 6500 Series supervisors provide operational consistency—enabling common sparing and minimizing training requirements; all modules feature predictable performance and a broad range of capabilities. Supervisor Engine 1A and Supervisor Engine 2 highlights include:

- *Feature-rich and wire-rate intelligent network services*—Support and complement comprehensive security and granular Quality of Service mechanisms, including identity-based networking capabilities based on IEEE 802.1x extensions and simplified configuration using two AutoQoS commands
- *End-to-end flexible deployments*—Position anywhere in the network from the wiring closet to the distribution/core, and from the data center to the WAN edge and the MAN
- *Scaleable and predictable performance*—Feature a flexible switch fabric and forwarding architecture delivering throughput from 15Mpps/32Gbps (Classic interface modules), to 30Mpps/256Gbps (CEF256 interface modules), to 210Mpps/256Gbps (dCEF256 interface modules) for network cores supporting multi-gigabit trunks
- *Flexible multilayer switching support and forwarding architectures*—Select basic Layer 2 forwarding or feature-rich Cisco Express Forwarding (CEF) using the same supervisor

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 719
Doc: 3702

Cisco Systems, Inc.
All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

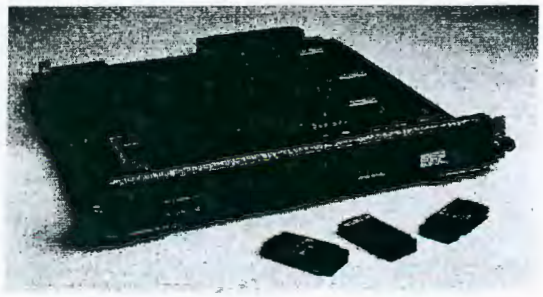
17056
L

- *Choice of operating system support*—Support both Cisco IOS® Software, Catalyst OS software, and Hybrid (Catalyst OS software and Cisco IOS Software for the MSFC)
- *Operational consistency*— Support all 3 generations of Catalyst 6500 Series interface and services modules in all Catalyst 6500 3-, 6-, 9- and 13-slot chassis running Cisco IOS® Software and Cisco Catalyst Operating System Software and a common set of Cisco network management tools that support the Catalyst 6500 Supervisor Engine 1A and 2 as well as many other Cisco Systems product lines
- *Maximum network uptime and user productivity*—Provide fault-tolerant network resilience and high availability features including fast 1- to 3-second stateful fail-over between redundant Catalyst 6500 supervisor engines enabling near-hitless software upgrades for business critical network environments, including IP-telephony enabled wiring closets
- *Extensive management tools*—Support CiscoWorks network management platform, Simple Network Management Protocol (SNMP) versions 1, 2, and 3 and four RMON groups (statistics, history, alarms, and events)

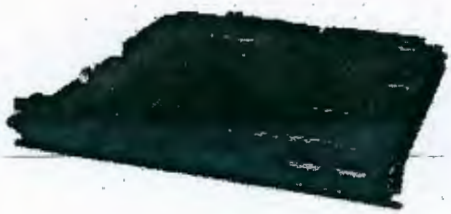
As part of the Catalyst 6500 Series of modular products, Supervisor Engines 1A and 2 share a common operating system and CLI—encouraging an end-to-end Catalyst 6500 Series solution for maximum operational consistency, common sparing, and minimized training requirements (Figure 1).

Figure 1 Supervisor Engines 1A and Supervisor Engine 2

Supervisor Engine 1-PFC



Supervisor Engine 2-MSFC2



All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

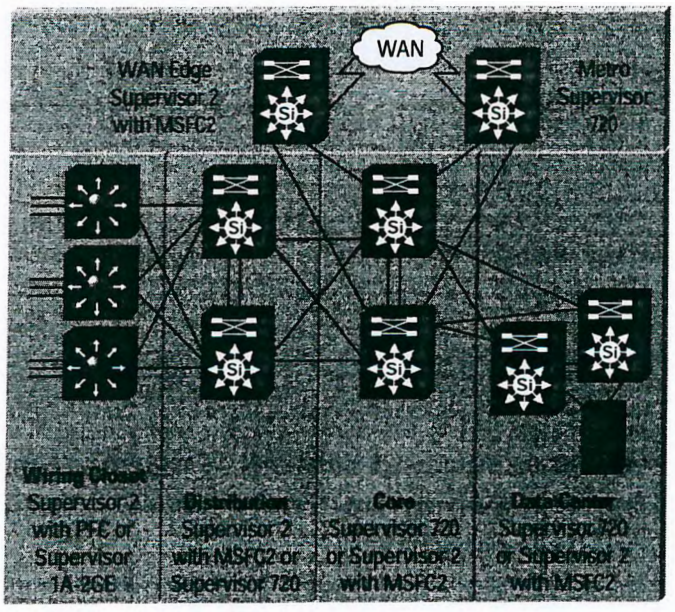
RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 720
Doc: 3702

17055
L

Supervisor Engine 1A and Supervisor Engine 2 Deployment Scenarios

With a broad range of interfaces, and services modules, chassis / slot configurations as well as a scalable set of Supervisor Engines, the Catalyst 6500 can be deployed anywhere in the network. The figure below depicts the Catalyst 6500 deployed in the wiring closet, distribution, core, data center, WAN edge and Metro and provides recommended supervisor engines for each part of the network.

Figure 2
Cisco Supervisor Engine 1A and Supervisor Engine 2 Deployment Scenarios



All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 721
Nº 3702
Doc:

17054
L

The following table outlines the primary deployment scenarios for Cisco Catalyst 6500 Series supervisor engines.

Table 1 Deployment Scenarios for Cisco Catalyst 6500 Series Supervisor Engines

Supervisor Engine	Performance/Features	Recommended Deployments
Supervisor Engine 720	400 Mpps, 720 Gbps Layer 2–4 distributed Cisco Express Forwarding Supports new accelerated Cisco Express Forwarding 720 and distributed Cisco Express Forwarding 720 interface modules	Enterprise core, distribution, and data centers
Supervisor Engine 2 **Policy Feature Card 2 (PFC2)** **Multilayer Switch Feature Card 2 (MSFC2)**	210 Mpps, 256 Gbps Layer 2–4 distributed Cisco Express Forwarding Supports distributed Cisco Express Forwarding 256 interface modules	Enterprise distribution, data centers, and WAN edge
Supervisor Engine 1A **PFC** **MSFC2**	15 Mpps, 32 Gbps Centralized Layer 2–4 forwarding Enhanced security and quality of service (QoS)	Distribution and core
Supervisor Engine 2 **PFC2**	30 Mpps, 256 Gbps Centralized Layer 2 forwarding and Layer 3–4 services Enhanced security and QoS	Premium wiring closet and data center access
Supervisor Engine 1A **PFC**	15 Mpps, 32Gbps Centralized Layer 2 forwarding and Layer 3–4 services Enhanced security and QoS	Enterprise wiring closets
Supervisor Engine 1A **2GE**	15 Mpps, 32 Gbps Centralized Layer 2 forwarding	Value wiring closet

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 722
Doc: 3702

17053
1

Supervisor Engine 1A and 2 Features

The Supervisor Engine 1A and 2 provide the following features:

- High availability
- Scalable performance
- Wire-rate traffic management
- End-to-end management tools
- Comprehensive security
- Advanced Layer 2, Layer 3, and Layer 4 forwarding

High Availability

Supervisor Engines 1A and 2 can be deployed in dual-supervisor engine configurations in all Cisco Catalyst 6500 Series chassis (6503, 6506, 6509, and 6513). The dual-supervisor engine configuration synchronizes protocol states between the primary and the redundant supervisor engine, provides industry-leading network availability with sub-3-second failover, and maximizes network uptime by allowing hot swapping of standby supervisor engines. Important high-availability features include:

- *Supervisor engine redundancy*—With synchronization of protocol states and support for HSRP and Uplink Fast
- *Rapid failover rates*—Sub-3-second stateful failover and Layer 3 IP Unicast and Multicast failover
- *Hot swapping*—Hot swapping of standby supervisors

Scalable Performance

Supervisor Engines 1A and 2 provide scalable performance, from 15 Mpps to 210 Mpps with bandwidth scaling from 32 Gbps to 256 Gbps, that densely populated wiring closets and high-throughput network cores with multigigabit trunks require.

Supervisor Engine 2 uses the Cisco Express Forwarding routing architecture that performs high-speed lookups even with advanced Layer 3 services enabled, and independent of the number of flows through the switch, while maintaining 30 Mpps of centralized performance and 210 Mpps of distributed performance.

- *Supervisor Engine 1A*—Provides 15-Mpps performance with 32-Gbps bandwidth
- *Supervisor Engine 2*—Provides 30 Mpps of centralized performance and 210 Mpps of distributed performance with 256-Gbps bandwidth

For details see Table 2—Cisco Catalyst 6500 Supervisor Engine Feature Comparison.

Wire-Rate Traffic Management

Supervisor Engines 1A and 2 provide wire-rate traffic management using Layer 2, 3, and 4 QoS and security checks, including ACL policy enforcement, as part of their forwarding process to protect and secure content. These traffic management features enable efficient handling of converged networks that carry a mix of mission-critical, time-sensitive, and bandwidth-intensive multimedia applications.

- Advanced QoS tools such as packet classification and marking and congestion avoidance based on Layer 2, Layer 3, and Layer 4 header information.
- QoS scheduling rules with thresholds can be configured in the switch for multiple receive and transmit queues.
- Rate limiting can be used to police traffic on a per-flow or aggregate basis with a very fine granularity.

For details see Table 3—QoS Features Comparison.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 723
Nº 3702 Doc.

1705
L

End-to-End Management Tools

Managed with CiscoWorks2000, Cisco Catalyst 6500 Series switches can be configured and managed to deliver end-to-end device, VLAN, traffic, and policy management. Cisco Resource Manager, a Web-based management tool that works with CiscoWorks2000, provides: automated inventory collection, software deployment, easy tracking of network changes, views into device availability, and quick isolation of error conditions.

Supervisor Engines 1A and 2 provide a comprehensive set of management tools to provide the required visibility and control in the network.

- *Console management*—Provide shared interface to the Supervisor Engine 2 and the Multilayer Switch Feature Card 2 (MSFC2) available out-of-band from a local terminal or remote terminal connected through a modem to the console or auxiliary interface
- *In-band management*—Provide shared interface to the Supervisor Engine 2 and the MSFC2 available in-band through SNMP, Telnet client, Bootstrap Protocol (BOOTP), and Trivial File Transfer Protocol (TFTP)
- *SPAN*—Allow management and monitoring of switch traffic
- *RSPAN*—Allow centralized management and monitoring by aggregating and directing traffic from multiple distributed hosts and switches to a remotely located switch through a trunk link
- *VACL Capture*—Direct traffic to a network analysis port using an ACL

For details see Table 4—Management Tools Comparison.

Comprehensive Security

The advanced security capabilities of Supervisor Engines 1A and 2 can reduce the threats of malicious attacks while enabling authentication, authorization, and accounting. With support for up to 32K ACL entries, IP/IPX security ACLs in hardware, and advanced features such as port security, Supervisor Engines 1A and 2 offer a superior set of Layer 2–4 network traffic security capabilities:

- *Layer 2 security features*—Include private VLANs and port security, to help the network architect properly partition and control the utilization of the switch resources.
- *Layer 2, 3, and 4 hardware filters*—Can work on the forwarding engine and in conjunction with optional integrated services modules to inspect each forwarded packet and permit or deny all the streams of traffic according to the network administrator's rules.

For details see Table 5—PFC and PFC2 Security Features Comparison.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 724
Doc: 3702

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

1705
2

Supervisor Engine 1A and 2 Architecture

Catalyst 6500 Series Supervisor Engines 1A and 2 manage the system by storing and running the system software, controlling the various modules in the chassis, performing basic forwarding, and providing the Gigabit uplinks that allow redundant supervisor engine connections.

Supervisor Engine 2 offers an improved forwarding design. The Supervisor Engine 1A CPU performs Layer 2 forwarding, but Supervisor Engine 2 performs Cisco Express Forwarding (CEF) and distributed CEF, doubling the forwarding performance. As shown in Table 2, Supervisor Engines 1A and 2 offer choices in operating characteristics, including forwarding architecture, performance, bandwidth, DRAM and boot Flash sizes, and support for chassis, Policy Feature Card/Policy Feature Card 2 (PFC/PFC2), MSFC2, and Switch Fabric Module (SFM).

Table 2 Cisco Catalyst 6500 Supervisor Engine Feature Comparison

Feature	Supervisor Engine 2 *Supervisor Engine-PFC2* *Supervisor Engine-MSFC2*	Supervisor Engine 1A *Supervisor Engine 1A-2GE* *Supervisor Engine 1A-PFC* *Supervisor Engine 1A-/MSF*
Cisco Express Forwarding (CEF)	Yes	No
Performance	30 Mpps—*Supervisor Engine 2- PFC2 and Supervisor Engine 2-MSFC2* up to 210 Mpps—*Supervisor Engine 2- MSFC2 with SFM and DFCs*	15 Mpps
Maximum bandwidth	256 Gbps (with distributed forwarding)	32 Gbps
DRAM	128 MB, 256 MB, 512 MB	128 MB
Onboard Flash (BootFlash)	32 MB	16 MB
Chassis supported	6006, 6009, 6503, 6506, 6509, 6509-NEB, 6509-NEB-A, 6513; 7603, 7606, 7609, OSR-7609, 7613	6006, 6009, 6503, 6506, 6509, 6509-NEB, 6509-NEB-A; 7603, 7606, 7609, OSR-7609
PFC daughter card available	Yes (PFC2); Standard with Supervisor Engine 2	Yes (PFC); Not field upgradable
MSFC2 daughter card available	Yes, and field upgradable	Yes, not field upgradable
SFM supported	Yes	No

The PFC/PFC2 and MSFC2 daughter cards and the SFM increase Supervisor Engines 1A and 2 functions:

- *PFC and PFC2*—Perform hardware-based Layer 2, Layer 3, and Layer 4 packet forwarding as well as packet classification, traffic management, and policy enforcement
- *MSFC2*—Performs Layer 3 control plane functions including address resolution and routing protocols
- *SFM 2*—Provides 256 Gbps dedicated bandwidth to all slots in the chassis and requires Supervisor Engine 2-MSFC2. The SFM 2 will not operate in the same chassis with Supervisor Engine 720.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 725
Doc: 3702

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

17050
L

Policy Feature Card (PFC and PFC2)

The Policy Feature Card provides quality of service (QoS) and policy based intelligent networking capabilities to the Catalyst 6500 Series. Recommended for premier wiring closets, backbone, data center and WAN edge deployments, the PFC identifies and classifies traffic applying the appropriate QoS priority level and Security Policies as defined by the network administrator configured ACLs. The PFC also helps to prevent unauthorized applications from being allowed on the network.

The Supervisor Engine PFC daughter card makes the packet forwarding decision in its application-specific integrated circuit (ASIC) complex. In distributed forwarding implementations, an identical ASIC complex located on an interface module's DFC daughter card allows the interface module to make packet-forwarding decisions locally. After the PFC or DFC makes the forwarding decision for the interface module, it sends the forwarding result to the interface module that does all packet buffering, queuing, and delivery.

In addition to packet forwarding, the PFC performs the following major functions at wire-rate:

- *Layer 3 packet classification*—Using QoS access-control entries
- *Traffic management (rate limiting)*—Using ingress and egress policing
- *Security policy enforcement*—Within subnets or VLANs
- *Intelligent multicast forwarding*—Efficient replication of multicast streams, supplied to appropriate end-user stations
- *NetFlow data export*—Collecting IP flow statistics for inter-subnet flows

QoS

The following table shows the PFC and PFC2 QoS features.

Table 3 QoS Features Comparison

Feature	PFC2 *Supervisor Engine 2* *PFC2* *Supervisor Engine 2* *MSFC2*	PFC *Supervisor Engine* *1A PFC* *Supervisor Engine* *1A PFC/MSFC2*	No PFC *Supervisor Engine* *1A-2GE*
Layer 2 classification and marking	Yes	Yes	Yes
Layer 3 classification and marking/ Access Control Entries (ACEs)	Yes 32K	Yes 16K	None
Rate limiting location (port)	Ingress port, VLAN	Ingress port, VLAN	None
Rate Limiting Level Types ***CIR = Committed Information Rate*** ***PIR = Peak Information Rate***	CIR, PIR	CIR	None
Aggregate traffic rate limiting/ number of policers	Yes 1023 policers	Yes 1023 policers	None
Flow-based rate limiting method/ number of rates	Full flow; 64 rates	Full flow; 64 rates	None

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 726
Doc: 3702

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

17049
L

Management Tools

The following table compares the management tools that are available with Supervisor Engines 1A and 2.

Table 4 Management Tools Comparison

Feature	PFC *Supervisor Engine 1A PFC* *Supervisor Engine 1A PFC/MSFC2* *Supervisor Engine 2 PFC2* *Supervisor Engine 2 MSFC2*	No PFC *Supervisor Engine 1A-2GE*
SPAN	Yes	Yes
RSPAN	Yes	No
ERSPAN	No	No
VACL Capture	Yes	No

Security

Table 5 shows the PFC and PFC2 security features.

Table 5 PFC and PFC2 Security Features Comparison

Feature	With PFC2 *Supervisor Engine 2 PFC2* *Supervisor Engine 2 MSFC2*	With PFC *Supervisor Engine 1A PFC* *Supervisor Engine 1A PFC/MSFC2*	Without PFC *Supervisor Engine 1A-2GE*
Port security	Yes	Yes	Yes
TCP intercept hardware acceleration	Yes	Yes	No
IEEE 802.1X and 802.1X extensions	Yes	Yes	No
IP security ACLs in hardware	Yes	Yes	No
IPX security ACLs in hardware	Yes	Yes	No
Security ACL entries	32K	16K	No
Reflexive ACLs	128K	512K	No
Unicast Reverse Path Forwarding (uRPF) check-in hardware	Yes	No	No
CPU rate limiters	1	None	None

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 727
3702
Doc:

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

12048

Multi-layer Switch Fabric Card2 (MSFC2)

Supported on both Supervisor 1A and Supervisor 2 as an option the MSFC2 acts as the Layer 3 forwarding routing engine. On its Layer 3 forwarding routing engine, the MSFC2 builds the CEF Forwarding Information Base (FIB) table in software and then downloads this table to the ASICs on the PFC or DFC that make the forwarding decisions for IP Unicast and Multicast traffic. For more information see How Cisco Express Forwarding Works.

Layer 3 Switching

Table 6 shows the MSFC2 Layer 3 switching features.

Table 6 Layer 3 Switching Feature Comparisons

Feature	MSFC2 *Supervisor Engine 1A-PFC/MSFC2* *Supervisor Engine 2-MSFC2*	No MSFC2 *Supervisor Engine 2-PFC2*	No MSFC2 *Supervisor Engine 1A-2GE* *Supervisor Engine 1A-PFC*
IPv4 routing	Yes	Yes, with MSFC2 upgrade	No, not upgradable
MPLS	Yes, through OSM	Yes, through OSM	No
IPv6	Yes, in software (only on Supervisor Engine 2-MSFC2	No, requires MSFC2 upgrade	No

Note: Refer to the release notes for up-to-date software version information.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 728
Nº Doc: 3702

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

17047
L

Switch Fabric Modules (SFM and SFM2)

Designed to support distributed forwarding, the Cisco Catalyst 6500 Series SFM (WS-X6500-SFM) and SFM2 (WS-X6500-SFM2) provide dedicated bandwidth to each slot up to 256 Gbps per system.

For distributed forwarding to work, an interface module must have a Distributed Forwarding Card (DFC) and must be installed in the chassis with either a Supervisor Engine 2-MSFC2 and an SFM or SFM2, or a Supervisor Engine 720. The SFM works with Cisco Catalyst 6506, 6509, 6509-NEB, and 6509-NEB-A chassis and can occupy any slot. The SFM2 works with 6506, 6509, 6509-NEB, 6509-NEB-A, 6513, 7603, 7606, 7609, OSR-7609, and 7613 chassis; and it can occupy any slot, except in the 6513 and 7613 where it must occupy slot 7 or 8.

The Catalyst 6503 does not currently support the SFM modules as this would leave one slot open after configuring the supervisor and SFM in two of the three available slots. However, the Supervisor 720 provides full CEF256, dCEF256, aCEF720 and dCEF720 capabilities to the Catalyst 6503 chassis with its slot-efficient integration of the supervisor engine and switch fabric in a single module.

Switch Fabric Module Architecture

Providing access to the switch fabric through dual 8-Gbps serial channels, the SFM or SFM2 performs all switching on the module independent of the passive backplane. For more information see How Distributed Cisco Express Forwarding (dCEF) Works.

High Availability

Two SFM and SFM2 modules can be configured in a system for high availability with 1-to-1 redundancy, where one SFM or SFM2 is operational and one serves as a backup.

Note: The SFM and SFM2 cannot operate in the same chassis with a Supervisor Engine 720.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 729
Doc: 3702

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

17046
2

Supervisor Engine 2-MSFC2

Suited for deployment in the distribution/core with Classic interface modules, CEF256 interface modules and dCEF256 interface modules, Supervisor 1A-2GE provides Layer 2/3/4 forwarding with the following operational advantages:

- *Layer 2–4 forwarding*—Performs Layer 2 – 4 forwarding with Layer2, 3, 4 features; supports dCEF256 interface modules
- *Media Access Control (MAC) addresses*—128K
- *Forwarding rate*—Up to 30 Mpps per system
- *Bandwidth*—32 Gbps per system; 256 Gbps with SFM in chassis
- *Layer 2, 3 traffic classification and marking*—Layer 2 and Layer 3 (See Table 3—QoS Features Comparison for details)
- *Multilayer (Layer 3) switching*—IPv4 supported (See Table 6 for details)
- Distributed forwarding—Requires Switch Fabric Module and interface modules with Distributed Forwarding Cards (DFCs); for details, see section titled How Distributed Cisco Express Forwarding (dCEF) Works
- *Operating system*—Cisco Catalyst OS with Cisco IOS on the MSFC and Cisco IOS Software
- *Management tools*—SPAN, RSPAN, VACL capture
- *DRAM*—128, 256, 512 MB
- *Onboard flash (BootFlash)*—32 MB
- *Chassis supported*—Cisco Catalyst 6006, 6009, 6503, 6506, 6509, 6509-NEB, 6509-NEB-A, and 6513; 7603, 7606, 7609, OSR-7609, and 7613
- *Slot requirements*—Slots 1 or 2 of any chassis
- *Upgrade support*—None required

Figure 3
Cisco Catalyst 6500 Series Supervisor Engine 2-MSFC2

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 730
Doc: 3702

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

17045
L

Supervisor Engine 2-PFC2

Suited for deployment in wiring closets with Classic and CEF256 interface modules, Supervisor Engine 1A-2GE provides basic Layer 2 forwarding with the following operational advantages:

- *Layer 2 forwarding*—Performs Layer 2 forwarding with Layer2, 3, 4 features; requires MSFC2 upgrade to support Layer 3, 4 forwarding
- *MAC addresses*—128K
- *Forwarding rate*—Up to 30 Mpps per system
- *Bandwidth*—32 Gbps per system; 256 Gbps with SFM in chassis
- *Layer 2, 3 traffic classification and marking*—Layer 2 and Layer 3 (See Table 3—QoS Features Comparison for details)
- *Multilayer (Layer 3) switching*—Requires MSFC2 upgrade (See Table 6 for details)
- *Distributed forwarding*—Requires MSFC2 upgrade, SFM, and interface modules with DFCs (for details, see section titled How Distributed Cisco Express Forwarding (dCEF) Works).
- *Operating system*—Cisco Catalyst OS only (Cisco IOS Software supported with MSFC2 upgrade)
- *Management tools*—SPAN, RSPAN, VACL capture
- *DRAM*—128, 256, 512 MB
- *Onboard flash (BootFlash)*—32 MB
- *Chassis supported*—Cisco Catalyst 6006, 6009, 6503, 6506, 6509, 6509-NEB, 6509-NEB-A, and 6513; 7603, 7606, 7609, OSR-7609, and 7613
- *Slot requirements*—Slots 1 or 2 of any chassis
- *Upgrade support*—MSFC2 upgrade

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 731
Doc: 3702

17044
L

Supervisor Engine 1A-PFC/MSFC2

Suited for deployment in the distribution/core with Classic interface modules, Supervisor Engine 1A-2GE provides Layer 2–4 forwarding with the following operational advantages:

- *Layer 2–4 forwarding*—Performs Layer 2–4 forwarding with Layer 2–4 features
- *MAC addresses*—128K
- *Forwarding rate*—Up to 15 Mpps per system
- *Bandwidth*—32 Gbps per system
- *Layer 2, 3 traffic classification and marking*—Layer 2 and Layer 3 (see Table 3—QoS Features Comparison for details)
- *Multilayer (Layer 3) switching*—IPv4 supported (See Table 6 for details)
- *Distributed forwarding*—Unsupported
- *Operating system*—Cisco Catalyst OS with Cisco IOS on the MSFC and Cisco IOS Software
- *Management tools*—SPAN, RSPAN, VACL capture
- *DRAM*—128 MB
- *Onboard flash (BootFlash)*—16 MB
- *Chassis supported*—Cisco Catalyst 6006, 6009, 6503, 6506, 6509, and 6509-NEB, 6509-NEB-A (6513 not supported); 7603, 7606, 7609, and OSR-7609 (7613 not supported)
- *Slot requirements*—Slots 1 or 2 of any chassis
- *Upgrade support*—None

Figure 4
Cisco Catalyst 6500 Supervisor Engine 1A-PFC/MSFC2

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 732
Doc: 3702

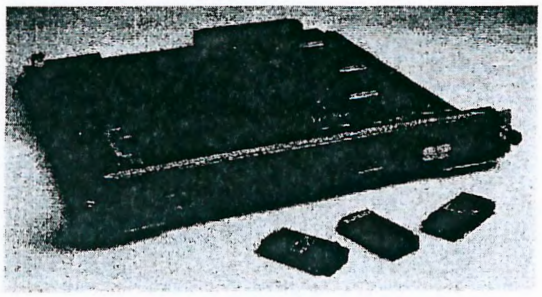
17043
L

Supervisor Engine 1A-PFC

Suited for deployment in wiring closets with Classic interface modules, Supervisor Engine 1A-2GE provides basic Layer 2 forwarding with the following operational advantages:

- *Layer 2 forwarding*—Performs basic Layer 2 forwarding with no Layer 2–4 features
- *MAC addresses*—128K
- *Forwarding rate*—Up to 15 Mpps per system
- *Bandwidth*—32 Gbps per system
- *Layer 2, 3 traffic classification and marking*—Layer 2 and Layer 3 (See Table 3—QoS Features Comparison for details)
- *Multilayer (Layer 3) switching*—Unsupported
- *Distributed forwarding*—Unsupported
- *Operating system*—Cisco Catalyst OS only
- *Management tools*—SPAN, RSPAN, VACL capture
- *DRAM*—128 MB
- *Onboard flash (BootFlash)*—16 MB
- *Chassis supported*—Cisco Catalyst 6006, 6009, 6503, 6506, 6509, and 6509-NEB, 6509-NEB-A (6513 not supported); 7603, 7606, 7609, and OSR-7609 (7613 not supported)
- *Slot requirements*—Slots 1 or 2 of any chassis
- *Upgrades*—None

Figure 5
Cisco Catalyst 6500 Supervisor Engine 1A-PFC



All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 733
3702
Doc:

170912

Supervisor Engine 1A-2GE

Suited for deployment in wiring closets with Classic interface modules, Supervisor Engine 1A–2GE provides basic Layer 2 forwarding with the following operational advantages:

- *Layer 2 forwarding*—Performs Layer 2 forwarding with Layer 4 features
- *MAC addresses*—128K
- *Forwarding rate*—Up to 15 Mpps per system
- *Bandwidth*—32 Gbps per system
- *Layer 2, 3 traffic classification and marking*—Layer 2 only, not upgradable to support Layer 3 (for details, see Table 3—QoS Features Comparison)
- *Multilayer (Layer 3) switching*—Unsupported
- *Distributed forwarding*—Unsupported
- *Operating system*—Cisco Catalyst OS only
- *Management tools*—SPAN only
- *DRAM*—64 MB
- *Onboard flash (BootFlash)*—16 MB
- *Chassis supported*—Cisco Catalyst 6006, 6009, 6503, 6506, 6509, and 6509-NEB, 6509-NEB-A (6513 not supported); 7603, 7606, 7609, and OSR-7609 (7613 not supported)
- *Slot requirements*—Slots 1 or 2 of any chassis
- *Upgrade support*—None

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 734
Nº 3702
Doc:

17041
L

How Cisco Express Forwarding Works

Cisco Express Forwarding (CEF) is a Layer 3 technology that provides increased forwarding scalability and performance to handle many short-duration traffic flows common in today's enterprise and service provider networks. To meet the needs of environments handling large amounts of short-flow, Web-based, or highly interactive types of traffic, CEF forwards all packets in hardware, and maintains its forwarding rate completely independent of the number of flows going though the switch.

On the Cisco Catalyst 6500 Series, the CEF Layer 3 forwarding engine is located centrally on the supervisor engine's PFC2 or PFC3—the same device that performs hardware-based Layer 2 and 3 forwarding, ACL checking, QoS policing and marking, and NetFlow statistics gathering.

Using the routing table that Cisco IOS Software builds to define configured interfaces and routing protocols, the CEF architecture creates CEF tables and downloads them into the hardware-forwarding engine before any user traffic is sent through the switch. The CEF architecture places only the routing prefixes in its CEF tables—the only information it requires to make the Layer 3 forwarding decisions—relying on the routing protocols to do route selection. By performing a simple CEF table lookup, the switch forwards packets at wire-rate, independent of the number of flows transiting the switch.

CEF-based forwarding requirements: Requires a Cisco Catalyst Supervisor Engine 2 or Catalyst Supervisor Engine 720.

How Distributed Cisco Express Forwarding (dCEF) Works

With Distributed Cisco Express Forwarding (dCEF), forwarding engines located on the interface modules make forwarding decisions locally and in parallel, allowing the Cisco Catalyst 6500 Series to achieve the highest forwarding rates in the industry. With dCEF, forwarding occurs on the interface modules in parallel and system performance scales up to 400 Mpps—the aggregate of all forwarding engines working together.

Using the same ASIC engine design as the central PFCx, DFCs located on the interface modules forward packets between two ports, directly or across the switch fabric, without involving the supervisor engine. With the DFC, each interface module has a dedicated forwarding engine complete with the full forwarding tables. dCEF forwarding works like this:

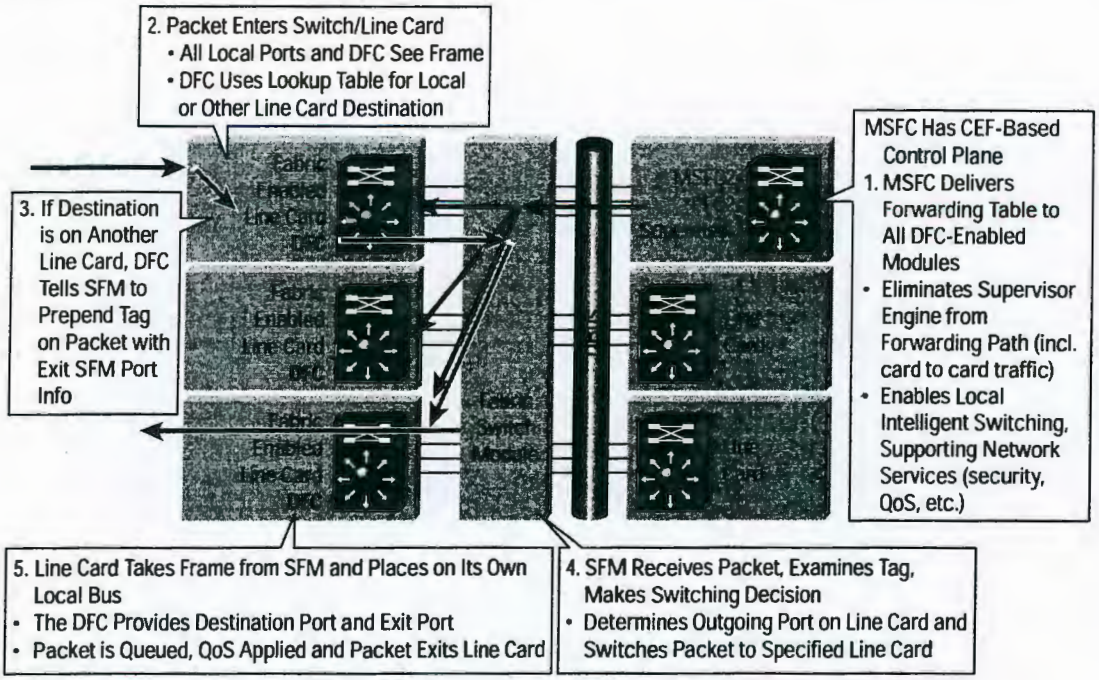
- As in standard CEF forwarding, the central PFC3 located on the supervisor engine and the DFC engines located on the interface modules are loaded with the same CEF information derived from the forwarding table before any user traffic arrives at the switch.
- As a packet arrives at an interface module, its DFC engine inspects the packet and uses the information in the CEF table (including Layer 2, Layer 3, ACLs, and QoS) to make a completely hardware-based forwarding decision for that packet.
- The dCEF engine handles all hardware-based forwarding for traffic on that module, including Layer 2 and Layer 3 forwarding, ACLs, QoS policing and marking, and NetFlow.
- Because the DFCs make all the switching decisions locally, the supervisor engine is freed from all forwarding responsibilities and can perform other software-based functions, including routing, management, and network services.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 735
Doc: 3702

17040
2

Figure 5
Distributed Cisco Express Forwarding Packet Flow



dCEF-based forwarding requirements: Requires a Cisco Catalyst Supervisor Engine 720 for dCEF720 interface modules; requires either a Catalyst Supervisor Engine 720 or a Catalyst Supervisor Engine 2-MSFC2 and a SFM for dCEF256 interface modules.

Software Requirements

Depending on its configuration, a supervisor engine will operate with one or more of the following operating systems:

- Cisco IOS Software for the supervisor engine (native Cisco IOS Software)
- Cisco Catalyst OS software
- Hybrid, Catalyst OS software and Cisco IOS Software for the MSFC

Notes: Refer to the release notes for up-to-date software version information.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 736
3702
Doc:

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

17034

Ordering Information

Table 7 lists the ordering information for the Supervisor Engines 1A and 2.

Table 7 Product Numbers for Ordering

Product Number	Description
WS-X6K-SUP1A-2GE	Catalyst 6500 Supervisor Engine1A, 2GE
WS-X6K-SUP1A-PFC	Catalyst 6500 Supervisor Engine1A, 2GE, plus PFC
WS-X6K-S1A-MSFC2	Catalyst 6500 Supervisor Engine1A, 2GE, plus MSFC-2 and PFC
WS-X6K-S2-PFC2	Catalyst 6500 Supervisor Engine 2, 2GE, plus PFC-2
WS-X6K-S2-MSFC2	Catalyst 6500 Supervisor Engine 2, 2GE, plus MSFC-2/PFC-2
WS-X6K-S1A-MSFC2	Supervisor Engine 1A with PFC+MSFC2
WS-X6K-S1A-MSFC2=	Supervisor Engine 1A with PFC+MSFC2=
WS-X6K-S1A-MSFC2/2	Supervisor Engine 1A with PFC+MSFC2/2
WS-F6K-MSFC2	Catalyst 6500 Multilayer Switch Feature Card 2
MEM-MSFC2-128MB=	Catalyst 6500 MSFC2 Memory, 128 MB DRAM Spare
MEM-MSFC2-256MB	Catalyst 6500 MSFC2 Memory, 256 MB DRAM Option
MEM-MSFC2-256MB=	Catalyst 6500 MSFC2 Memory, 256 MB DRAM Spare
MEM-MSFC2-512MB	Catalyst 6500 MSFC2 Memory, 512 MB DRAM Option
MEM-MSFC2-512MB=	Catalyst 6500 MSFC2 Memory, 512 MB DRAM Spare
WS-X6500-SFM	Catalyst 6500 Switch Fabric Module
WS-X6500-SFM2	Catalyst 6500 Switch Fabric Module2

Dimensions

- (H x W x D): 1.6 x 15.3 x 16.3 in. (4.0 x 37.9 x 40.3 cm)

Environmental Conditions

- Operating temperature: 32 to 104 F (0 to 40 C)
- Storage temperature: –40 to 167 F (–40 to 75 C)
- Relative humidity: 10 to 90%, noncondensing
- Regulatory compliance

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 737
Doc: 3702

170-58

Safety Certifications

- UL 1950
- EN 60950
- CSA-0C22.2 No. 950
- IEC 950

Electromagnetic Emissions Certifications

- FCC 15J Class A
- VCCI CE II
- CE mark
- EN 55022 Class B
- CISPR 22 Class B

Technical Support Services

Whether your company is a large organization, a commercial business, or a service provider, Cisco Systems is committed to maximizing the return on your network investment. Cisco offers a portfolio of Technical Support Services to ensure that your Cisco products operate efficiently, remain highly available, and benefit from the most up-to-date system software.

Cisco Technical Support Services offers the following features, which help enable network investment protection and minimal downtime for systems running mission-critical applications:

- Provides Cisco networking expertise online and on the telephone
- Creates a proactive support environment with software updates and upgrades as an ongoing integral part of your network operations, not merely a remedy when a failure or problem occurs
- Makes Cisco technical knowledge and resources available to you on demand
- Augments the resources of your operations technical staff to increase productivity
- Complements remote technical support with onsite hardware replacement
- The Cisco portfolio of Technical Support Services includes:
- Cisco SMARTnet™ support
- Cisco SMARTnet Onsite support
- Cisco Software Application Services, including Software Application Support and Software Application Support plus Upgrades

For more information visit:

http://www.cisco.com/en/US/products/svcs/ps3034/serv_category_home.html

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
738
Fls Nº
3702
Doc:

17026

Additional Cisco Catalyst 6500 Series Information

For additional information about the Cisco Catalyst 6500 Series, supervisor engines, interface modules, SFM, and services modules, visit:

http://www.cisco.com/en/US/products/hw/switches/ps708/products_data_sheets_list.html

- Catalyst 6500 Series Data Sheet
- Catalyst 6500 Supervisor Engine 720 Data Sheet
- Catalyst 10/100 and 10/100/1000 Ethernet Data Sheet
- Catalyst 6500 Gigabit Ethernet Interface Modules Data Sheet
- Catalyst 6500 10 Gigabit Ethernet Interface Modules Data Sheet
- Catalyst 6500 FlexWAN Interface Modules Data Sheet
- Catalyst 6500 Switch Fabric Interface Modules Data Sheet
- Catalyst 6500 Content Services Module (CSM) Data Sheet
- Catalyst 6500 Firewall Services Module Data Sheet
- Catalyst 6500 Network Application Module (NAM) Data Sheet
- Catalyst 6500 Intrusion Detection (IDS) Module Data Sheet
- Catalyst 6500 IP Sec/VPN Services Module Data Sheet
- Catalyst 6500 SSL Services Module Data Sheet

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the
Cisco Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland
Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland
Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. CCIP, CCSP, the Cisco Arrow logo, the Cisco *Powered* Network mark, Cisco Unity, Follow Me Browsing, FormShare, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, Fast Step, GigaStack, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, MGX, MICA, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, ScriptShare, SlideCast, SMARTnet, StrataView Plus, Stratm, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0304R)

203070/ETMG_07/03

SCDC - RJ 13/2005 - CN -
CORREIOS
Fls Nº 739
Doc: 3702

ANEXO (3)

17035
2

CISCO SYSTEMS

Data Sheet

Cisco Catalyst 6500 Series **Gigabit** Ethernet Modules

The Cisco Catalyst® 6500 Series Switch—the premier modular multilayer switch—delivers secure converged services from the wiring closet to the core, to the data center, to the WAN edge.

Designed to complement the many roles that the Cisco Catalyst 6500 Series plays in a network, Cisco Catalyst 6500 Series Gigabit Ethernet modules offer the broadest selection of media, densities, performance, interoperability, and chassis deployments for enterprises and service providers. *These modules are ideal for* gigabit to the desktop, gigabit uplinks, aggregation of high-density 10/100 interfaces, Metro Ethernet links; and backbone and high-speed server farm or data center connections. The Cisco Catalyst 6500 Series Gigabit Ethernet modules offer the following features:

- Flexible configurations for any deployment—Provide flexible port densities, media choices, and performance speeds for any deployment requirement
- Choice of media and connector type—Available in multimode fiber or single-mode fiber using MT-RJ and modular GBIC and SFP optics supporting station-to-station distances up to 100 km

Note: For information about 10/100/1000 copper interface modules with auto-negotiation, see the Cisco Catalyst 6500 Series 10/100 and 10/100/1000 Ethernet Data Sheet

- High port densities—From 8 up to 16 ports per module, up to 256 ports per system
- Scalable and predictable performance—Provide a selection of switch fabric connections and throughput: 32 Gbps bandwidth/15 Mpps (Classic interface modules), 256 Gbps bandwidth/30 Mpps (CEF256 interface modules), and 256 Gbps bandwidth/210 Mpps (dCEF256 interface modules)
- Operational consistency—Supported in all Catalyst 6500 3-, 6-, 9-, and 13-slot chassis running Cisco IOS® Software and Cisco Catalyst Operating System Software; interoperable with all other interfaces and services modules; and forward-compatible with all Catalyst 6500 supervisor engines
- Maximum network uptime and resiliency—Support Cisco enhanced Per-Virtual LAN (VLAN) Spanning Tree Plus (PVST+) protocol, IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) and IEEE 802.1s Multiple Spanning Tree (MST) protocol, Per-VLAN Rapid Spanning Tree (PVRST) protocol, Hot Standby Router Protocol (HSRP), Virtual Router Redundancy Protocol (VRRP), Cisco EtherChannel®, and IEEE 802.3ad link aggregation for fault-tolerant connectivity

RQS nº 03/2005 - CN - CPMI - CORREIOS
740
Fls Nº
3702
Doc:

Cisco Systems, Inc.
All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

17034
L

- Superior traffic management—Available with large per-interface buffers and multiple-priority queues for traffic prioritization and policing, allowing for tight service-level agreement (SLA) enforcement
- Extensive management tools—Support CiscoWorks network management platform, Simple Network Management Protocol (SNMP) versions 1, 2, and 3 and four RMON groups (statistics, history, alarms, and events)

Figure 1
Cisco Catalyst 6500 Series Gigabit Ethernet Interface Modules
WS-X6816-GBIC

WS-X6516A-GBIC

Cisco Systems, Inc.
All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 741
3702
Doc:

17033

Gigabit Ethernet Applications

Gigabit Ethernet interface modules are used in distribution and core layers, and in data-center applications (Table 1).

Table 1 Cisco Catalyst 6500 Series Gigabit Interface Module Applications

Primary Applications	Product Number	Interface Module Class	Ports/ Connector/ Interface	Queues per Port (Tx = Transmit, Rx = Receive)[1]	Buffer Size
Data center and server farm	WS-X6816-GBIC	dCEF256	16, GBIC	Tx–1p2q2t Rx–1p1q4t	512 KB per port
Data center and server farm	WS-X6516A-GBIC	CEF256	16, GBIC	Tx–1p2q2t Rx–1p1q4t	1 MB per port
Base server farm	WS-X6408A-GBIC	Classic	8, GBIC	Tx–1p2q2t Rx–1p1q4t	512 KB per port
Base server farm	WS-X6316-GE-TX	Classic	16, RJ-45, 1000	Tx–1p2q2t Rx–1p1q4t	512 KB per port
Base server farm	WS-X6516-GBIC[1]	CEF256	16, GBIC	Tx–1p2q2t Rx–1p1q4t	512 KB per port
Base server farm	WS-X6416-GBIC	Classic	16, GBIC	Tx–1p2q2t Rx–1p1q4t	512 KB per port
Base server farm	WS-X6416-GE-MT	Classic	16, MT-RJ, MM	Tx–1p2q2t Rx–1p1q4t	512 KB per port

1. **Queues Legend:** 1p2q2t = 1 priority queue, 2 round robin queues, 2 thresholds

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 742
Doc: 3702

17032
L

Gigabit Ethernet Interface Modules

The Cisco Catalyst 6500 Classic, CEF256, and dCEF26 interface modules provide Gigabit Ethernet with a choice of speeds and forwarding rates.

Classic Interface Modules

Suited for wiring closet applications, Classic interface modules use the supervisor engine for centralized Layer 2 and Layer 3 forwarding, and forward packets up to 15 Mpps over a 32-Gbps shared bus.

Capable of operating in the same chassis with the Cisco Catalyst 6500 Series Supervisor Engine 1A, Supervisor Engine 2, and Supervisor Engine 720, Catalyst Classic interface modules do not support distributed forwarding and cannot be upgraded with a Distributed Forwarding Card (DFC).

Table 2 provides more information about Catalyst Classic interface modules.

CEF256 Interface Modules

Suited for distribution and core layers and for data-center and Web-hosting applications, CEF256 interface modules use the centralized CEF engine located on the supervisor engine's policy feature card (PFC) and forward packets up to 30 Mpps over a dedicated 8-Gbps full-duplex switch fabric connection.

Capable of operating in the same chassis with the Cisco Catalyst 6500 Series Supervisor Engine 1A, Supervisor Engine 2, and Supervisor Engine 720, CEF256 interface modules support distributed forwarding when upgraded with a DFC (Table 2).

Table 2 CEF256 Interface Module Distributed Forwarding Upgrade Requirements

Supervisor Engine	Switch Fabric	Distributed Forwarding Card
Supervisor Engine 2 MSFC2/PFC2	Separate switch fabric module (SFM)	Requires WS-F6K-DFC upgrade
Supervisor Engine 720	Supervisor Engine 720 integrates a 720 Gbps switch fabric *Note:* A Supervisor Engine 720 and an SFM cannot occupy the same chassis	Requires WS-F6K-DFC3 upgrade; will not interoperate with WS-F6K-DFC

dCEF256 Interface Modules

Suited for distribution and core layers, for data-center and Web-hosting applications, and for several high-performance service provider applications, the dCEF256 interface modules use the dCEF engine and tables located on the interface module to perform all forwarding.

dCEF256 interface modules require a Cisco Catalyst 6500 Series Supervisor Engine 720 or a Supervisor Engine 2 with a Multilayer Switch Feature Card 2 (MFSC2) and SFM. Supervisor Engine 720 requires a WS-F6K-DFC3 upgrade; and Supervisor Engine 2-MFSC2 operates with the WS-F6K-DFC supplied with the dCEF256 interface module.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 743
Nº 3702

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

17 031
L

Table 3 Interface Module Class Comparison: Classic, CEF256, and dCEF256

Feature	Classic	CEF256	dCEF256
Performance maximum (Mpps)	15	30	210
Forwarding engine/ location	Centralized CEF Engine; located on supervisor engine's PFCx	Centralized CEF Engine; located on supervisor engine's PFCx	Distributed CEF Engine; located on interface module's DFCx
Supervisor engine supported	Supervisor Engine 1A; Supervisor Engine 2; Supervisor Engine 720	Supervisor Engine 1A (15 Mpps maximum); Supervisor Engine 2; Supervisor Engine 720	Supervisor Engine 2; Supervisor Engine 720
DFC modules integrated/ upgrade requirements	Not supported	None integrated; upgrade with WS-F6K-DFC3 for Supervisor Engine 720 *or* upgrade with WS-F6K-DFC for Supervisor Engine 2-MSFC2	DFC integrated; DFC3 field upgrade (requires Supervisor Engine 720)
Fabric connections	32 Gbps shared bus connection (on Supervisor Engine 1A, Supervisor Engine 2, and Supervisor Engine 720)	Single 8-Gbps channel connection to switch fabric (on Supervisor Engine 720 or Supervisor Engine 2-MSFC2 with SFM) *and* 32-Gbps shared bus connection	Dual 8-Gbps full-duplex serial channel connections to switch fabric (on Supervisor Engine 720 or Supervisor Engine 2-MSFC2 with SFM)
Slot requirements	Can occupy any slot in any chassis	Can occupy any slot in any chassis	Can occupy any slot in any Cisco Catalyst 6503, 6506, 6509, 6509-NEB, or 6509-NEB-A chassis, or any Cisco 7603, 7606, 7609, or OSR-7609 chassis; can only occupy slots 9 through 13 in a 6513, or 7613 chassis
Receive queue structure	1p1q4t	1p1q4t	1p1q4t
Transmit queue structure	1p2q2t	1p2q2t	1p2q2t
Scheduler	Weighted Round Robin (WRR)	WRR	WRR
Buffer size	512 KB	512 KB or 1 MB (WS-X6516a)	512 KB

Legend: 1p2q2t = one strict priority queue, two round-robin queues, and two different thresholds

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 744
Doc: 3702

17030
2

Cisco Catalyst Classic Gigabit Ethernet Copper Interface Modules

Designed for distribution and core layers and for data-center and Web-hosting applications, Cisco Catalyst Classic copper interface modules provide line-rate Gigabit Ethernet forwarding with the following operational advantages:

Forwarding architecture—Use centralized CEF forwarding

Forwarding performance—Forward packets up to 15 Mpps per system

Fabric connection—Provide a 32-Gbps shared bus connection

Supervisor engine—Work with Supervisor Engine 1A, Supervisor Engine 2, or Supervisor Engine 720

Distributed forwarding upgrade—None; Classic interface modules cannot be upgraded for distributed forwarding

Slot requirements—None; can occupy any slot in any Cisco Catalyst 6500 Series chassis

Table 4 Classic Gigabit Ethernet Copper Interface Modules

Product	Ports/Interface/ Connectors	Port Density/ Chassis Model	Maximum Distance/ Cable Type
WS-X6316-GE-TX	16 ports; 1000BASE-T; RJ-45	192 ports (Cisco Catalyst 6513); 128 ports (Cisco Catalyst 6509)	100 meters; Category 5 cable

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 745
Doc: 3702

17029

Cisco Catalyst Classic Gigabit Ethernet Optical Interface Modules

Designed for distribution and core layers and for data-center and Web-hosting applications, Cisco Catalyst Classic optical interface modules provide line-rate Gigabit Ethernet forwarding with the following operational advantages:

Forwarding architecture—Use centralized CEF forwarding

Forwarding performance—Forward packets up to 15 Mpps per system

Optics—Supports hot-pluggable gigabit interface converters (GBICs)

Fabric connection—Provide a 32-Gbps shared bus connection

Supervisor engine—Work with Supervisor Engine 1A, Supervisor Engine 2, or Supervisor Engine 720

Distributed forwarding upgrade—None; Classic interface modules cannot be upgraded for distributed forwarding

Slot requirements—Can occupy any slot in any Cisco Catalyst 6500 Series chassis

Table 5 Classic Gigabit Ethernet Optical Interface Modules

Product	Transceiver Type	Ports/Interface/ Connectors	Port Density/ Chassis Model	Maximum Distance/ Cable Type
WS-X6408A-GBIC	GBIC	8 ports; 1000BASE-SX, -LX/LH, -ZX; SC	96 ports (Cisco Catalyst 6513); 64 ports (Cisco Catalyst 6509)	550 m: 1000BASE-SX 10 km: LX/LH 100 km: ZX
WS-X6416-GBIC	GBIC	16 ports; 1000BASE-SX, -LX/LH, -ZX; SC	192 ports (Cisco Catalyst 6513); 128 ports (Cisco Catalyst 6509)	550 m: 1000BASE-SX 10 km: LX/LH 100 km: ZX
WS-X6416-GE-MT	MT-RJ	16 ports; 1000BASE-SX; MT-RJ	192 ports (Cisco Catalyst 6513); 128 ports (Cisco Catalyst 6509)	550 m: 1000BASE-SX

Figure 2
Classic Gigabit Ethernet Optical Interface Modules
WS-X6416-GE-MT

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 746
Doc: 3702

17028

Cisco Catalyst CEF256 Gigabit Ethernet Optical Interface Modules

Designed for data center and server farm applications, Cisco Catalyst CEF256 optical interface modules provide line-rate Gigabit Ethernet forwarding with the following operational advantages:

Forwarding architecture—Uses the central CEF engine located on the supervisor engine

Forwarding performance—Forwards packets up to 30 Mpps per system and up to 15 Mpps per slot if upgraded to support distributed forwarding

Optics—Supports hot-pluggable GBICs

Fabric connection—Connects to the switch fabric using one 8-Gbps full-duplex connection and the 32-Gbps shared bus

Supervisor engine—Works with Supervisor Engine 1A, Supervisor Engine 2, or Supervisor Engine 720

Distributed forwarding upgrade—Optional; upgrade is required only to perform distributed forwarding; requires a WS-F6K-DFC3 upgrade to operate with Supervisor Engine 720; requires a WS-F6K-DFC upgrade and an SFM to operate with Supervisor Engine 2-MFSC2

Slot requirements—Can occupy any slot in any Catalyst 6500 Series chassis

Port densities—192 ports: Catalyst 6513 chassis; 128 ports: Catalyst 6509 chassis

Note: Supervisor Engine 720 communicates with a CEF256 interface module in 256-Gbps mode. Supervisor Engine 720 and SFM cannot operate in the same chassis.

Table 6 CEF256 Gigabit Ethernet Optical Interface Modules

Product	Transceiver Type	Ports/Interface/ Connectors	Port Density/ Chassis Model	Maximum Distance/ Cable Type
WS-X6516-GBIC	GBIC	16 ports; 1000BASE-SX, -LX/LH, -ZX; SC	192 ports (Cisco Catalyst 6513); 128 ports (Cisco Catalyst 6509)	550 m: 1000BASE-SX 10 km: LX/LH 100 km: ZX
WS-X6516A-GBIC	GBIC	16 ports; 1000BASE-SX, -LX/LH, -ZX; SC	192 ports (Cisco Catalyst 6513); 128 ports (Cisco Catalyst 6509)	550 m: 1000BASE-SX 10 km: LX/LH 100 km: ZX

Figure 3
CEF256 Gigabit Ethernet Optical Interface Modules
WS-X6516A-GBIC

Cisco Systems, Inc.
All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 747
Doc: 3702

17027
L

Cisco Catalyst dCEF256 Gigabit Ethernet Optical Interface Modules

Designed for distribution and core layers and for data-center and Web-hosting applications, Cisco Catalyst dCEF256 optical interface modules provide line-rate Gigabit Ethernet forwarding with the following operational advantages:

Forwarding architecture—Use the dCEF engine and dCEF tables located on the interface module

Forwarding performance—Forward packets up to 24 Mpps per slot when interface modules have dual-fabric connections

Optics—Support hot-pluggable GBICs over single-mode fiber

Fabric connection—Connect using dual 8-Gbps full-duplex serial channel connections to fabric on a Supervisor Engine 720 or a SFM

Supervisor engine—Work with Supervisor Engine 2 with a SFM or Supervisor Engine 720

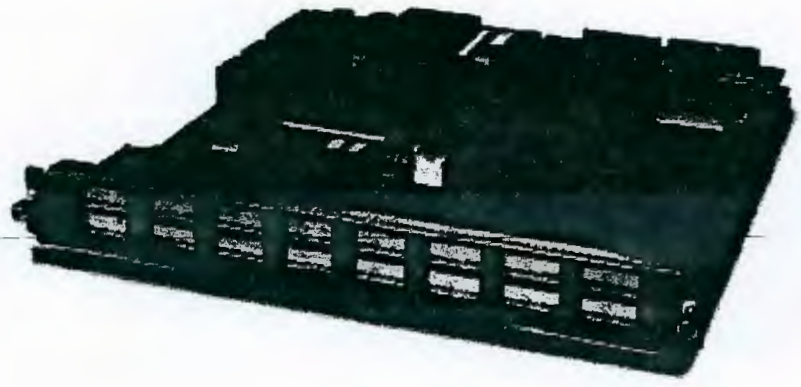
Distributed forwarding—Include a DFC when operating with Supervisor Engine 2 or a DFC3 when operating with Supervisor Engine 720

Slot requirements—Can occupy any slot in any Cisco Catalyst 6500 Series chassis except the 6513 chassis where they must be installed in slots 9 through 13 (the only slots on the chassis with dual fabric connections)

Table 7 dCEF256 Gigabit Ethernet Optical Interface Modules

Product	Transceiver Type	Ports/Interface/ Connectors	Port Density/ Chassis Model	Maximum Distance/ Cable Type
WS-X6816-GBIC	GBIC	16 ports; 1000BASE-SX,- LX/LH, -ZX; SC	90 ports (Cisco Catalyst 6513); 128 ports (Cisco Catalyst 6509)	550 m: 1000BASE-SX 10 km: LX/LH 100 km: ZX

Figure 4
dCEF256 Gigabit Ethernet Optical Interface Modules
WS-X6816-GBIC



RQS nº 03/2005 - CN -
CPMI - CORREIOS
748
Fls Nº
Doc: 3702

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

17026
L

Interface Distances

Table 8 summarizes the interfaces and distances supported by all the Gigabit Ethernet modules in the Cisco Catalyst 6500 Series.

Table 8 Interfaces and Distances Supported by Gigabit Ethernet Modules in the Cisco Catalyst 6500 Series

Module	Interface/Fiber Core	62.5	62.5 um MM 160/500 MHz-km	62.5 um MM 200/500 MHz-km	50 um MM 400/400 MHz-km	50 um MM 500/500 MHz-km	9/10 um Single Mode	Dispersion Shifted	Category 5 UTP
WS-X6416-GE-MT	MT-RJ	220 m	275 m	500 m	550 m				
WS-X6408-GBIC	1000BASE-SX	220 m	275 m	500 m	550 m				
WS-X6408A-GBIC	1000BASE-SX	220 m	275 m	500 m	550 m				
WS-X6416-GBIC	1000BASE-SX	220 m	275 m	500 m	550 m				
WS-X6516-GBIC	1000BASE-SX	220 m	275 m	500 m	550 m				
WS-X6816-GBIC	1000BASE-SX	220 m	275 m	500 m	550 m				
WS-X6408A-GBIC	1000BASE-LX/LH	550 m	550 m	550 m	550 m		10 km		
WS-X6416-GBIC	1000BASE-LX/LH	550 m	550 m	550 m	550 m		10 km		
WS-X6516-GBIC	1000BASE-LX/LH	550 m	550 m	550 m	550 m		10 km		
WS-X6816-GBIC	1000BASE-LX/LH	550 m	550 m	550 m	550 m		10 km		
WS-X6408-GBIC	1000BASE-ZX						70 km	100 km	
WS-X6408A-GBIC	1000BASE-ZX						70 km	100 km	
WS-X6416-GBIC	1000BASE-ZX						70 km	100 km	
WS-X6516-GBIC	1000BASE-ZX						70 km	100 km	
WS-X6816-GBIC	1000BASE-ZX						70 km	100 km	
WS-X6316-GE-TX	RJ-45								100 m

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 749
3702
Doc:

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

17025
2

Ordering Information

Table 9 provides part number information for Catalyst 6500 Series chassis.

Table 9 Catalyst 6500 Series Chassis Part Numbers

Product Number	Description
WS-X6316-GE-TX	16-port Classic Gigabit Ethernet interface module for the Cisco Catalyst 6000 Series switches; RJ-45
WS-X6408-GBIC	8-port Classic Gigabit Ethernet interface module for the Cisco Catalyst 6000 Series switches; requires GBICs
WS-X6408A-GBIC	8-port Classic Gigabit Ethernet interface module for the Cisco Catalyst 6000 Series switches with enhanced QoS; requires GBICs
WS-X6416-GBIC	16-port Classic Gigabit Ethernet interface module for the Cisco Catalyst 6000 Series switches; requires GBICs
WS-X6416-GE-MT	16-port Classic Gigabit Ethernet interface module for the Cisco Catalyst 6000 Series switches; MT-RJ
WS-X6516-GBIC	16-port CEF256 Gigabit Ethernet interface module for the Cisco Catalyst 6500 Series switches with single fabric channel interface; requires GBICs; upgradable to support distributed forwarding through the addition of the distributed forwarding daughter card (WS-F6K-DFC)
WS-F6K-DFC	Distributed forwarding daughter card for CEF26 interface modules
WS-X6816-GBIC	16-port dCEF256 Gigabit Ethernet interface module for the Cisco Catalyst 6500 Series switches with dual fabric channel interfaces and distributed forwarding; requires GBICs
WS-X6816A-GBIC	16-port dCEF256 Gigabit Ethernet interface module for the Cisco Catalyst 6500 Series switches with dual fabric channel interfaces and distributed forwarding; requires GBICs
GLC-SX-MM	1000BASE-SX SFP (multimode only) Dual LC connector
GLC-SX-MM=	1000BASE-SX SFP (multimode only) spare Dual LC connector
GLC-LH-SM	1000BASE-LX SFP (single mode only) Dual LC connector
GLC-ZX-SM	1000BASE-ZX SFP (single mode only) Dual LC connector
WS-G5484	1000BASE-SX SX GBIC (multimode only)
WS-G5485	1000BASE-LX/LH LH GBIC (single mode or multimode)
WS-G5487	1000BASE-ZX ZX GBIC (single mode only)

Specifications

Standard Protocols

- IEEE 802.1d, IEEE 802.1p, IEEE 802.1q, IEEE 802.1s, IEEE 802.1w, IEEE 802.3x, IEEE 802.3z, IEEE 802.3ab, and IEEE 802.3ad,
- 1000BASE-X (GBIC), 1000BASE-SX, 1000BASE-LX/LH, 1000BASE-ZX, CWDM

Physical Specification

- Occupies one slot in the Cisco Catalyst 6500 Series chassis
- Dimensions (H x W x D): 1.2 x 14.4 x 16 in. (3.0 x 35.6 x 40.6 cm)

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 750
Doc: 3702

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

1702/24

Environmental Conditions

- Operating temperature: 32 to 104 F (0 to 40 C)
- Storage temperature: –40 to 167 F (–40 to 75 C)
- Relative humidity: 10 to 90%, noncondensing
- Operating altitude: –60 to 4000 m
- Mean time between failure (MTBF): seven years for system configuration

Safety Compliance

Cisco Catalyst 6500 Series Gigabit Ethernet interface modules, when installed in a system, comply with the following compliance and safety standards:

- UL 1950
- CSA C22.2 No.950
- EN 60950
- EN 60825-1
- IEC 60950
- IEC 60825-1
- TS 001
- CE marking
- AS/NZS 3260
- 21CFR1040

EMC Compliance

Cisco Catalyst 6500 Series Gigabit Ethernet modules, when installed in a system, comply with the following EMI standards:

- FCC Part 15 (CFR 47) Class A
- VCCI
- EN55022
- EN55024
- CISPR 22
- CE marking
- AS/NZS 3548

Network Management

- ETHERLIKE-MIB (RFC 1643)
- IF-MIB (RFC 1573)
- Bridge MIB (RFC 1493)
- CISCO-STACK-MIB
- CISCO-VTP-MIB
- CISCO-CDP-MIB

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 751
Doc: 3702

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

17023
L

- RMON MIB (RFC 1757)
- CISCO-PAGP-MIB
- CISCO-STP-EXTENSIONS-MIB
- CISCO-VLAN-BRIDGE-MIB
- CISCO-VLAN-MEMBERSHIP-MIB
- ENTITY-MIB (RFC 2037)
- HC-RMON
- RFC1213-MIB (MIB-II)
- SMON-MIB

Maximum Station-to-Station Cabling Distance

- 1000BASE-SX: 62.5 um multimode fiber: up to 275 m
- 1000BASE-SX: 50 um multimode fiber: up to 550 m
- 1000BASE-LX: 62.5 um multimode fiber: up to 550 m
- 1000BASE-LX: 50 um multimode fiber: up to 550 m
- 1000BASE-LX: 9/10 um single-mode fiber: up to 5 km[1]
- 1000BASE-LH: 62.5 um multimode fiber: up to 550 m
- 1000BASE-LH: 50 um multimode fiber: up to 550 m
- 1000BASE-LH: 9/10 um single-mode fiber: up to 10 km
- 1000BASE-ZX: 9/10 um single-mode fiber: up to 70 km
- 1000BASE-ZX: disposition shifted fiber: up to 100 km
- 1000BASE-T: Category 5 cable: up to 100 m
- 10/100/1000BASE-T: Category 5 cable: up to 100 m

Indicators and Interfaces

- Status: green (operational); red (faulty); orange (module booting or running diagnostics)
- Link good: green (port active); orange (disabled); off (not active or not connected); blinking orange (failed diagnostic and disabled)
- 1000BASE-SX: GBIC (female, multimode)
- 1000BASE-LX/LH: GBIC (female, multimode)
- 1000BASE-LX/LH: GBIC (female, single mode)
- 1000BASE-ZX: GBIC (female, single mode)
- 1000BASE-ZX: GBIC (female, dispersion shifted)
- 1000BASE-SX: MT-RJ (female, multimode)
- 1000BASE-T: RJ-45
- 10/100/100BASE-T: RJ-45

1. Cisco 1000BASE-LX/LH interfaces fully comply with the IEEE 802.3z 1000BASE-LX standard. However, their higher quality allows them to reach 10 km over single-mode fiber versus the 5 km specified in the standard.

ROS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 752
Doc: 3702

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Technical Support Services

Whether your company is a large organization, a commercial business, or a service provider, Cisco is committed to maximizing the return on your network investment. Cisco offers a portfolio of technical support services to help ensure that your Cisco products operate efficiently, remain highly available, and benefit from the most up-to-date system software.

The Cisco Technical Support Services organization offers the following features, providing network investment protection and minimal downtime for systems running mission-critical applications:

- Provides Cisco networking expertise online and on the telephone
- Creates a proactive support environment with software updates and upgrades as an ongoing integral part of your network operations, not merely a remedy when a failure or problem occurs
- Makes Cisco technical knowledge and resources available to you on demand
- Augments the resources of your technical staff to increase productivity
- Complements remote technical support with onsite hardware replacement

Cisco Technical Support Services include:

- Cisco SMARTnet™ support
- Cisco SMARTnet Onsite support
- Cisco Software Application Services, including Software Application Support and Software Application Support plus Upgrades

For more information, visit:
http://www.cisco.com/en/US/products/svcs/ps3034/serv_category_home.html

Additional Cisco Catalyst 6500 Series Information

Visit this link for to view the following data sheets:
http://www.cisco.com/en/US/products/hw/switches/ps708/products_data_sheets_list.html

- Cisco Catalyst 6500 Series Data Sheet
- Cisco Catalyst 6500 Series Supervisor Engine 1A/Supervisor Engine 2 Data Sheet
- Cisco Catalyst 6500 Series Supervisor Engine 720 Data Sheet
- Cisco Catalyst 6500 Series 10/100 and 10/100/1000 Ethernet Data Sheet
- Cisco Catalyst 6500 Series 10-Gigabit Ethernet Interface Modules Data Sheet
- Cisco Catalyst 6500 Series FlexWAN Interface Modules Data Sheet
- Cisco Catalyst 6500 Series Switch Fabric Interface Modules Data Sheet
- Cisco Catalyst 6500 Series Content Services Module (CSM) Data Sheet
- Cisco Catalyst 6500 Series Firewall Services Module Data Sheet
- Cisco Catalyst 6500 Series Network Application Module (NAM) Data Sheet
- Cisco Catalyst 6500 Series Intrusion Detection (IDS) Module Data Sheet
- Cisco Catalyst 6500 Series IPsec/VPN Services Module Data Sheet
- Cisco Catalyst 6500 Series SSL Services Module Data Sheet

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the **Cisco Web site at www.cisco.com/go/offices**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain, Sweden Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Catalyst, Cisco, Cisco IOS, Cisco Systems, the Cisco Systems logo, EtherChannel, and SMARTnet are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0304R)

MH/LW4273 0403

ROS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 753
Doc 3702

ANEXO (4)

17021
2

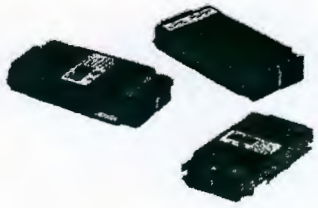
Data Sheet

Cisco **Gigabit** Interface Converter

The industry-standard Cisco Gigabit Interface Converter (GBIC) is a hot-swappable input/output device that plugs into a Gigabit Ethernet port or slot, linking the port with the network. Cisco GBICs can be interchanged on a wide variety of Cisco products and can be intermixed in combinations of 1000BASE-T, 1000BASE-SX, 1000BASE-LX/LH, 1000BASE-ZX, or 1000BASE-CWDM interfaces on a port-by-port basis.

As additional capabilities are developed, these modules make it easy to upgrade to the latest interface technology, maximizing investment protection. Figure 1 shows three Cisco GBIC models.

Figure 1
Cisco Gigabit Interface Converters]



Cisco 1000BASE-T GBIC

The Cisco 1000BASE-T GBIC (product number WS-G5483) connects a GBIC port to Category 5 wiring via a standard RJ-45 interface. The maximum Category 5 wiring distance is 328 feet (100 meters). For details, see the *Cisco 1000BASE-T Gigabit Interface Converter Data Sheet.*

Cisco 1000BASE-SX GBIC

The Cisco 1000BASE-SX GBIC (WS-G5484) operates on ordinary multimode fiber (MMF) optic link spans up to 1815 feet (550 m) long.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 754
Doc: 3702

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

17020
L

Cisco 1000BASE-LX/LH GBIC

The Cisco 1000BASE-LX/LH GBIC (WS-G5486) fully complies with the IEEE 802.3z 1000BASE-LX standard. However, its higher optical quality allows it to reach 6.2 miles (10 kilometers) over single-mode fiber (SMF), compared with the 3.1 miles (5 km) specified in the standard.

Cisco 1000BASE-ZX GBIC

The Cisco 1000BASE-ZX GBIC (WS-G5487) operates on ordinary single-mode fiber optic link spans up to 43.4 miles (70 km) long. Link spans of up to 62 miles (100 km) are possible using premium single-mode fiber or dispersion shifted single-mode fiber. The GBIC provides an optical link budget of 23 dB—the precise link span length will depend on multiple factors such as fiber quality, number of splices, and connectors.

When shorter distances of single-mode fiber are used, it might be necessary to insert an in-line optical attenuator in the link to avoid overloading the receiver:

- A 5-dB or 10-dB inline optical attenuator should be inserted between the fiber-optic cable plant and the receiving port on the Cisco 1000BASE-ZX GBIC at each end of the link whenever the fiber-optic cable span is less than 15.5 miles (25 km).

Technical Specifications

This section covers the Cisco 1000BASE-SX GBIC, Cisco 1000BASE-LX/LH GBIC, and the Cisco 1000BASE-ZX GBIC, unless otherwise specified. Technical specifications for the Cisco 1000BASE-T GBIC can be found in a separate document, *Cisco 1000BASE-T Gigabit Interface Converter Data Sheet*.

Platform Support

Cisco GBICs are supported across a variety Cisco switches, routers, and optical transport devices. For more details, see the document *GBIC Compatibility Matrix*.

Connectors and Cabling

Connectors: Dual SC connector

Table 1 provides cabling specifications for the Cisco GBICs that you install in the Gigabit Ethernet port. Note that all Cisco GBICs have SC-type connectors, and the minimum cable distance for all GBICs listed (multimode fiber [MMF] and single-mode fiber [SMF]) is 6.5 feet (2 m).

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 755
Doc: 3702

17019
L

Table 1 Cisco GBIC Port Cabling Specifications

GBIC	Wavelength (nm)	Fiber type	Coresize (micron)	Modal bandwidth (MHz/km)	Cable distance
Cisco 1000BASE-SX	850	MMF	62.5	160	722 ft (220 m)
			62.5	200	902 ft (275 m)
			50.0	400	1640 ft (500 m)
			50.0	500	1804 ft (550 m)
Cisco 1000BASE-LX/LH	1300	MMF[1]	62.5	500	1804 ft (550 m)
			50.0	400	1804 ft (550 m)
		SMF	50.0	500	1804 ft (550 m)
			9/10	N/A	6.2 miles (10 km)
Cisco 1000BASE-ZX	1550	SMF	9/10	N/A	43.4 to 62 miles (70 to 100 km)[2]

1. Mode-conditioning patch cord (CAB-GELX-625 or equivalent) is required. Using an ordinary patch cord with MMF, 1000BASE-LX/LH GBICs, and a short link distance (10s of meters) can cause transceiver saturation resulting in an elevated bit error rate (BER). In addition, when using the Cisco 1000BASE-LX/LH GBIC with 62.5-micron diameter MMF, you must install a mode-conditioning patch cord between the GBIC and the MMF cable on both the transmit and receive ends of the link. The mode-conditioning patch cord is required for link distances greater than 984 feet (300 m).

2. Cisco 1000BASE-ZX GBIC can reach up to 62 miles (100 km) by using dispersion shifted SMF or low-attenuation SMF; the distance depends on fiber quality, number of splices, and connectors.

Note: A mode-conditioning patch cord (product number CAB-GELX-625 or equivalent) is required to comply with IEEE standards. The IEEE found that link distances could not be met with certain types of fiber-optic cable cores. The solution is to launch light from the laser at a precise offset from the center, which is accomplished by using the mode-conditioning patch cord. At the output of the patch cord, the Cisco 1000BASE-LX/LH GBIC is compliant with the IEEE 802.3z standard for 1000BASE-LX.

Standards

Compatible with GBIC standard as specified in IEEE 802.3z

Compliant with GBIC Specification Revision 5.4

Table 2 Fiber Loss Budgets for 1000BASE-SX, 1000BASE-LX, and 1000BASE-ZX

Device	Type	Transmit (dBm)		Receive (dBm)	
		Max	Min	Max	Min
WS-G5484	1000BASE-SX	–4	–9.5	0	–17
WS-G5486	1000BASE-LX/LH	–3	–9.5	–3	–19
WS-G5487	1000BASE-ZX	5	0	–3	–23[1]

1. The WS-G5487 1000BASE-ZX GBIC provides a minimum optical power budget of 23 dB. To determine the supported link distance you should measure your cable plant with an optical loss test set to verify that the optical loss of the cable plant (including connectors and splices) is less than or equal to this figure. The optical loss measurement must be performed with a 1550-nanometer light source.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 756
Doc: 3702

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

17018
L

Dimensions

Dimensions (H x W x D): 8.5 mm x 13.4 mm x 56.5 mm

Environmental Conditions and Power Requirements

The operating temperature range is 32 to 122 F (0 to 50 C)

Storage temperature range is –40 to 185 F (–40 to 85 C).

Table 3 Electrical Power Interface

Parameter	Symbol	Minimum	Typical	Maximum	Units
Supply current	I_S	—	200	300	mA
Supply voltage	I_{max}	—	—	6	—
Surge current	I_{SURGE}	—	—	30	mA
Input voltage	V_{CC}	4.75	5	5.25	V

Warranty

- Standard warranty: 90 days
- Extended warranty (option): Available under a Cisco SMARTnet™ support contract for the Cisco switch or router chassis

Ordering Information

Table 4 lists product numbers to use when ordering Cisco GBICs.

Table 4 Cisco GBIC Product Numbers

GBIC	Product number
Copper (Cisco 1000BASE-T)	WS-G5483
Short wavelength (1000BASE-SX)	WS-G5484
Long wavelength/long haul (1000BASE-LX/LH)	WS-G5486
Extended distance (1000BASE-ZX)	WS-G5487

Regulatory and Standards Compliance

Safety—Laser Class I 21CFR1040

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
757
Fls Nº 3702
Doc:

17077
L

For More Information

For additional information about the Cisco Coarse Wavelength-Division Multiplexing (CWDM) GBIC Solution contact:

- United States and Canada: 800 553-NETS (6387)
- Europe: 32 2 778 4242
- Australia: 612 9935 4107
- Other: 408 526-7209
- http://www.cisco.com

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems Europe
11 Rue Camille Desmoulins
92782 Issy-les-Moulineaux
Cedex 9
France
www-europe.cisco.com
Tel: 33 1 58 04 60 00
Fax: 33 1 58 04 61 00

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 317 7777
Fax: +65 317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the **Cisco Web site at www.cisco.com/go/offices**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

All contents are Copyright © 1992–2003, Cisco Systems, Inc. All rights reserved. Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems, Cisco IOS, the Cisco Systems logo, and SMARTnet are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0301R)

KCJLW4171 02/03

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 758
3702
Doc:

ANEXO (5)

17016
L

Data Sheet

Cisco Catalyst 6500 Series 10/100 and 10/100/1000 **Ethernet** Interface Modules

As Cisco's premier modular multilayer switch, the Catalyst® 6500 Series delivers secure, converged services from the wiring closet to the core, to the data center, to the WAN edge.

The Cisco Catalyst® 6500 Series provides the broadest selection of 10/100 and 10/100/1000 Ethernet media, inline power options, densities, performance, interoperability, and chassis deployments. Equally suited for basic wiring closets, small campus distribution/core layers, and high performance data centers, Catalyst 6500 10/100 and 10/100/1000Mbps modules scale from 16-ports up to 576-ports in a single Catalyst 6500 chassis. Catalyst 6500 10/100 and 10/100/1000Mbps modules feature:

- Proven and widely deployed Cisco AVVID wiring closet solution—Cisco's most widely deployed IP telephony port-enabled campus switch
- Choice of media and connector types—Available in copper unshielded twisted-pair (UTP), shielded twisted-pair (STP) using RJ-45 or RJ-21, multimode fiber (62.5/125 micron), and single-mode fiber using MT-RJ 100FX and 10FL
- IP phone and wireless access point support—Support inline power field upgrade (copper only), NIC/Phone auto-detection (phone discovery), and voice VLANs
- Simplified network operation with cable fault detection—Test cabling using Time Domain Reflectometer (TDR) that sends signals down the cable to identify faults in each twisted pair (available for 10/100/1000 copper
- Range of port densities—Available with 16 to 48 ports per module; enabling up to 576 10/100/1000Base-TX ports, 288 ports of 100-Base-FX, or 10BASE-FL per 13-slot chassis (configured with 12 interface modules)
- Scalable and predictable performance—Provide a selection of switch fabric connections and throughput: 32 Gbps bandwidth/15 Mpps (Classic interface modules), 256 Gbps bandwidth/30 Mpps (CEF256 interface modules) and 256 Gbps bandwidth/210 Mpps(dCEF256 interface modules)
- IEEE 802.3 triple-speed autonegotiation—Allow switches to negotiate speed (10, 100, and now 1000 Mbps) and duplex mode (half or full) with attached devices
- Superior traffic management—Available with large 1-MB-per-interface buffers and up to 8 transmit queues for traffic prioritization and policing

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 759
Nº Doc 3702

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

17015
L

- Operational consistency—Supported in all Catalyst 6500 3-, 6-, 9-, and 13-slot chassis running Cisco IOS® Software and Cisco Catalyst Operating System Software; interoperable with all other interfaces and services modules; and forward-compatible with all Catalyst 6500 supervisor engines
- Maximum network uptime and resiliency—Support Cisco enhanced Per-Virtual LAN (VLAN) Spanning Tree Plus (PVST+) protocol, IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) and IEEE 802.1s Multiple Spanning Tree (MST) protocol, Per-VLAN Rapid Spanning Tree (PVRST) protocol, Hot Standby Router Protocol (HSRP), Virtual Router Redundancy Protocol (VRRP), Cisco EtherChannel®, and IEEE 802.3ad link aggregation for fault-tolerant connectivity
- Extensive management tools—Support CiscoWorks network management platform; Simple Network Management Protocol (SNMP) versions 1, 2, and 3; and four Remote Monitoring (RMON) groups (statistics, history, alarms, and events)

The newest members of the Cisco Catalyst 6500 Series 10/100/1000 product family—the Classic interface module WS-X6148-GE-TX and the CEF256 interface module WS-X6548-GE-TX—provide 10/100/1000 Gigabit Ethernet over copper network access using standard RJ-45 connectors (Figure 1).

Figure 1
Cisco Catalyst 6500 Series 48-Port RJ-45 10/100/1000 Ethernet Interface Modules
WS-X6148-GE-TX

WS-X6548-GE-TX

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 760
Doc: 3702

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

1701 14

Cisco Catalyst 6500 Series 10/100 and 10/100/1000 Ethernet Applications

Ethernet and Fast Ethernet 10/100 and 10/100/1000 interface modules are used in both wiring closet and data center applications (Figure 2; Table 1).

Table 1 Cisco Catalyst 6500 Series 10/100 and 10/100/1000 Copper Interface Module Applications

Primary Applications	Product Number	Interface Module Class	Ports/ Connector/ Interface	Inline Power Support[1]	Queues per Port (Tx = Transmit, Rx = Receive)[2]	Buffer Size
Data Center and Server Farm	WS-X6516-GE-TX	CEF256	16, RJ-45, 10/100/1000	No	Tx–1p2q2T, Rx–1p1q4T	512 KB per port
Server Farm	WS-X6548-RJ-45	CEF256	48, RJ-45, 10/100	No	Tx–1p3q1t, Rx–1p1q0t	1 MB per port
Server Farm	WS-X6548-RJ-21	CEF256	48, RJ-21, 10/100	No	Tx–1p3q1t, Rx–1p1q0t	1 MB per port
Premier Wiring Closet	WS-X6548V-GE-TX	CEF256, No upgrade to dCEF	48, RJ-45, 10/100/1000	Both	Tx–1p2q2t (per 8 ports), Rx–1p2t (per port)	1 MB per 8 ports
Premier Wiring Closet	WS-X6548-GE-TX	CEF256, No upgrade to dCEF	48, RJ-45, 10/100/1000	Both, Upgr	Tx–1p3q1t, Rx–1p1q4t	1 MB per 8 ports
Wiring Closet	WS-X6148V-GE-TX	Classic	48, RJ-45, 10/100/1000	Both	Tx–1p2q2t, Rx–1q2t	1 MB per 8 ports
Wiring Closet	WS-X6148-GE-TX	Classic	48, RJ-45, 10/100/1000	Both, Upgr	Tx–1p2q2t, Rx–1q2t	1 MB per 8 ports
Base Wiring Closet	WS-X6148-RJ45V	Classic	48, RJ-45, 10/100/1000	Both	Tx–2q2t, Rx–1q4t	128 KB per port
Base Wiring Closet	WS-X6148-RJ21V	Classic	48, RJ-21, 10/100	Both	Tx–2q2t, Rx–1q4t	128 KB per port
Base Wiring Closet	WS-X6148-RJ-45	Classic	48, RJ-45, 10/100	Both, Upgr	Tx–2q2t, Rx–1q4t	128 KB per port
Base Wiring Closet	WS-X6148-RJ-21	Classic	48, RJ-21, 10/100	Both, Upgr	Tx–2q2t, Rx–1q4t	128 KB per port
Base Wiring Closet	WS-X6348-RJ45V	Classic	48, RJ-45, 10/100	Cisco	Tx 2q2t, Rx 1q4t	128 KB per port
Base Wiring Closet	WS-X6348-RJ21V	Classic	48, RJ-21, 10/100	Cisco	Tx 2q2t, Rx 1q4t	128 KB per port

1. Inline Power Legend:
Both = Cisco inline power (available now) and IEEE 802.3af (via future field upgradable daughter card)
Cisco = Cisco inline power only
Upgr = shipped as data only but upgradable to the inline power type specified
No = inline power not supported

2. Queues Legend: 1p7q8t = 1 priority queue, 7 round robin queues, 8 thresholds

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 761
Doc: 3702

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

17013

Table 2 Cisco Catalyst 6500 Series 100FX and 10FL Fiber Interface Module Applications

Primary Applications	Product Number	Interface Module Class	Ports/ Connectors/ Interface Media	Queues per Port (Tx = Transmit, Rx = Receive)[1]	Buffers
Access, Server Farm	WS-X6524-100FX-MM	CEF256, Upgradable to dCEF	24, MM MT-RJ, 100FX	Tx 1p3q1t, Rx 1p1q0t	1 MB per port
Access, Server Farm	WS-X6324-100FX-MM	Classic	24, MM, MT-RJ, 100FX	Tx 2q2t, Rx 1q4t	128 KB per port
Access, Server Farm	WS-X6324-100FX-SM	Classic	24, SM MT-RJ, 100FX	Tx 2q2t, Rx 1q4t	128 KB per port
Access	WS-X6024-10FL-MT	Classic	24, MM MT-RJ, 10FL	Tx 2q2t, Rx 1q4t	64 KB per port

1. **Queues Legend:** 1p3q1t = 1 priority queue, 3 round robin queues, 1 threshold

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 762
Doc: 3702

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

17042

Cisco Catalyst 6500 Series 10/100 and 10/100/1000 Ethernet Interface Modules with Cisco Inline Power

The Cisco Catalyst 6500 Series delivered the first 10/100BASE-T Ethernet switching modules that provided inline power for converged data and voice traffic as well as other inline powered devices, such as wireless access points. Several Catalyst 6500 series interface modules support inline power or "power over Ethernet" on each interface port, allowing customers to build campus multiservice data and voice networks for wiring closets with the following features:

- Inline power—Provides 48-volt DC power (for Cisco Inline Power and IEEE 802.3af standard inline power when it becomes available) over standard Category 5 unshielded twisted-pair (UTP) cable up to 100 meters for IP phones and wireless access points
- Phone discovery—Detects the presence of an IP phone and supplies inline power automatically
- Auxiliary VLAN using 802.1Q—Segments IP phones and data endpoints into separate logical networks automatically
- AutoQoS—Simplifies the task of configuring QoS mechanisms for IP telephony and more

Cisco Catalyst Inline Power and IEEE 802.3af Inline Power

The Inline Power feature gives network administrators centralized power control. It works over existing Category 5 UTP installations and helps to ensure that building power outages will not affect network telephony connections, providing greater network availability—when Cisco Catalyst 6500 Series switches are configured with uninterruptible power supply (UPS) systems.

Several 10/100 and 10/100/1000 Ethernet interface modules support the Cisco Inline Power feature today, enabled by a daughter card for "pay as grow" flexibility. Once ratified, some of these interface modules will also support the IEEE 802.3af standard as an additional upgrade option. The Cisco Catalyst Inline Power feature implementation passes the required domestic and international safety regulations and compliance measures.

Phone Discovery

The Cisco phone discovery feature eases network management burdens by automating the Inline Power feature. With phone discovery, the Cisco Catalyst switch detects the presence of an IP phone and supplies inline power automatically, eliminating the need to manually enable ports for inline power. The phone discovery mechanism is intelligent enough to differentiate between an IP phone and a network interface card (NIC), and will not supply inline power to NICs or other devices not designed to use inline power. With this feature, network administrators can depend on automatic and centralized control of inline power that is safe to deploy and maintain.

Auxiliary VLAN

The unique Auxiliary VLAN feature offered by Cisco provides automatic VLAN configuration for IP phones. It places phones into their own VLANs automatically, simplifying the task of overlaying a voice topology onto a data network. It allows network administrators to easily segment phones into separate logical networks, even though the data and voice infrastructure is physically the same—greatly simplifying the task of managing a multiservice network and identifying and troubleshooting network problems.

The Auxiliary VLAN feature maintains VLAN assignments, even when phones are moved to new locations. When a user plugs a phone into the switch, the switch provides the phone with the necessary VLAN information.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 763
Doc 3702

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

17011

AutoQoS

Network administrators can assign IP phones to separate IP subnets and VLANs to allow separate quality of service (QoS) or security policies for IP phones. By deploying AutoQoS that configures QoS on voice ports automatically, the administrative task of configuring QoS to establish end-to-end traffic prioritization is greatly simplified.

Cisco Catalyst 6500 Series 10/100 and 10/100/1000 Modules

Two classes of Cisco Catalyst 6500 Series 10/100 and 10/100/1000 Ethernet interface modules—Classic and CEF256—provide a choice of speeds and forwarding rates (Table 4).

Classic 10/100 and 10/100/1000 Interface Modules

Suited for wiring closet applications, Classic 10/100 and 10/100/1000 modules use the supervisor's centralized forwarding engine for Layer 3 forwarding, and forward packets up to 15 Mpps.

Capable of operating in the same chassis with Supervisor Engine 1A, Supervisor Engine 2, and Supervisor Engine 720, Classic interface modules do not support distributed forwarding and cannot be upgraded with a Distributed Forwarding Card (DFC).

CEF256 10/100 and 10/100/1000 Interface Modules

Suited for premier wiring closet, distribution and core layers, data-center, and Web-hosting applications, CEF256 10/100 and 10/100/1000 interface modules use the centralized CEF engine located on the supervisor engine's policy feature card (PFC) and forward packets up to 30 Mpps.

Capable of operating in the same chassis with Supervisor Engine 1A, Supervisor Engine 2, and Supervisor Engine 720, CEF256 interface modules can also support distributed forwarding, with the following noteable exceptions: the WS-6548-GE-TX and WS-6548V-GE-TX do not support distributed forwarding.

Table 3 CEF256 10/100 and 10/100/1000 Switch Fabric DFC Upgrade Requirements

Supervisor Engine	Switch Fabric	DFC
Supervisor Engine 2 MSFC2/PFC2	Separate switch fabric module (SFM)	Requires WS-F6K-DFC upgrade
Supervisor Engine 720	Supervisor Engine 720 contains a switch fabric	Requires WS-F6K-DFC3 upgrade; will not work with WS-F6K-DFC3, or WS-F6K-DFC

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 764
Nº Doc: 3702

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

1701C

Table 4 provides a comparison of the interface module classes available for 10/100 and 10/100/1000 Ethernet interface modules.

Table 4 Classic and CEF256 10/100 and 10/100/1000 Interface Module Comparison

Feature	Classic Interface Modules	CEF256 Interface Modules
Performance/ Forwarding Rate (Mpps)	32 Gbps; 15 Mpps per system	256 Gbps; Up to 30 Mpps per system (15 Mpps per slot for slots upgraded with DFC to support distributed forwarding)
Forwarding Engine Architecture	Supervisor engine CPU makes forwarding decision	Centralized CEF engine located on supervisor's PFCx daughter card makes forwarding decision upgradeable to dCEF switching[1] with optional WS-F6K-DFC or WS-F6K-DFC3
Supervisor Engine Supported	Supervisor Engine 1A, Supervisor Engine 2, Supervisor Engine 720	Supervisor Engine 1A, Supervisor Engine 2, Supervisor Engine 720
DFC Upgrade Requirements	Not supported	None integrated; Supervisor Engine 2—WS-F6K-DFC upgrade; SupervisorEngine 720—WS-F6K-DFC3 upgrade
Fabric Connections	32 Gbps shared bus connection (on Supervisor Engine1A, Supervisor Engine 2, and Supervisor Engine 720)	Single 8-Gbps channel connection to switch fabric [on Supervisor Engine 720 or Supervisor Engine 2-MSFC2 with Switch Fabric Module (SFM)] and 32-Gbps shared bus connection
Slot Requirements	Can occupy any slot in any chassis	Can occupy any slot in any chassis
Scheduler	Weighted Round Robin (WRR)	WRR

[1] The WS-X6548-GE-TX and WS-X6548V-GE-TX do not support distributed forwarding; a DFCx can not be installed on these interface modules.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 765
Doc: 3702

1709
C

Cisco Catalyst Classic 10/100/1000 Voice Interface Modules

Suited for wiring closet applications, Cisco Catalyst Classic 10/100/1000 voice interface modules (Table 5) provide access to the desktop through standard RJ-45 connectors with the following operational advantages:

Forwarding architecture—Centralized CEF forwarding

Forwarding performance—Forward packets up to 15 Mpps per system

Fabric connection—Provide a 32-Gbps shared bus connection

Supervisor engine—Work with Supervisor Engine 1A, Supervisor Engine 2, or Supervisor Engine 720

Distributed forwarding upgrade—None; Classic interface modules cannot be upgraded for distributed forwarding

Slot requirements—Can occupy any slot in any Cisco Catalyst 6500 Series chassis

Maximum Port Density / Chassis— up to 576 ports / Cisco Catalyst 6513; up to 384 ports / Cisco Catalyst 6509

Time Domain Reflectometer (TDR)—Tests cabling by sending signals down the cable to identify faults in each twisted pair

Transmit queue structure—1p2q2t = 1 strict priority queue, 2 round robin queues, 2 thresholds

Receive queue structure—1q2t = 1 round robin queue, 2 thresholds

Table 5 Classic 10/100/1000 Voice Interface Modules

Product	Ports/ Interface/ Connectors	Maximum Distance/ Cable Type	Maximum Frame Size (Jumbo Frame) Support	Inline Power for Voice Availability/ Upgrade Capability
WS-X6148-GE-TX	48-port;10/100/ 1000BASE-TX; RJ-45	100 meters; Category 5 cable	up to 1518 bytes	Cisco Inline Power; upgradable to 802.3af
WS-X6148V-GE-TX	48-port; 10/100/ 1000BASE-TX; RJ-45	100 meters; Category 5 cable	up to 1518 bytes	Cisco Inline Power; upgradable to 802.3af

Figure 2
Classic 10/100/1000 Voice Interface Modules
WS-X6148V-GE-TX

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 766
Doc 3702

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

17.003
2

Cisco Catalyst CEF256 10/100/1000 Voice Interface Modules

Suited for wiring closet applications, Cisco Catalyst CEF256 10/100/1000 voice interface modules provide access to the desktop through standard RJ-45 connectors and line-rate 10/100/1000 Ethernet forwarding (Table 6) with the following operational advantages:

Forwarding architecture—Use the central CEF engine located on the supervisor engine

Forwarding performance—Forward packets up to 30 Mpps per system and up to 15 Mpps per slot if upgraded to support distributed forwarding

Fabric connection—Connect to the switch fabric through one 8-Gbps connection and the 32-Gbps shared bus

Supervisor engine—Work with Supervisor Engine 1A, Supervisor Engine 2, or Supervisor Engine720

Distributed forwarding upgrade—Not Supported. The WS-X6548-GE-TX and WS-X6548V-GE-TX do not support distributed forwarding or any DFCx.

Slot requirements—Can occupy any slot in any Cisco Catalyst 6500 Series chassis

Maximum Port Density / Chassis—up to 576 ports / Cisco Catalyst 6513; up to 384 ports / Cisco Catalyst 6509

Time Domain Reflectometer (TDR)—Tests cabling by sending signals down the cable to identify faults in each twisted pair

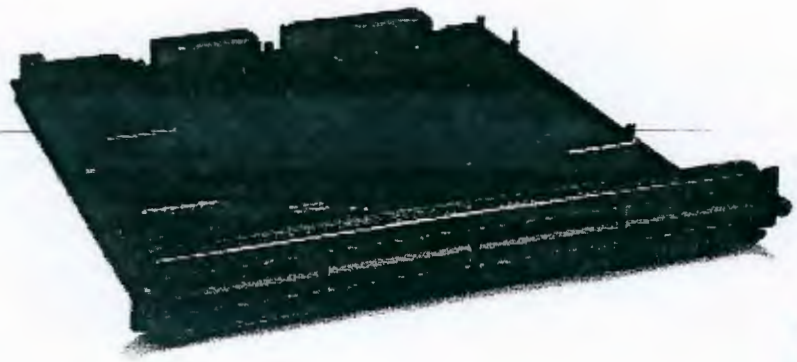
Transmit queue structure—1p2q2t = 1 priority queue, 2 round robin queues, 1 threshold

Receive queue structure—1q2t = 1 round robin queue, 2 thresholds

Table 6 CEF256 10/100/1000 Voice Interface Modules

Product	Ports/ Interface/ Connectors	Maximum Distance/ Cable Type	Maximum Frame Size (Jumbo Frame) Support	Inline Power for Voice Availability/ Upgrade Capability
WS-X6548-GE-TX	48-port; 10/100/ 1000BASE-TX; RJ-45	100 meters; Category 5 cable	up to 1518 bytes	Cisco Inline Power; upgradable to 802.3af

Figure 3
CEF256 10/100/1000 Voice Interface Modules
WS-X6548-GE-TX



RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 767
Doc: 3702

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

1700

Cisco Catalyst Classic 10/100 Copper Voice Modules

Designed for deployment in wiring closets, high-density Cisco Catalyst Classic 10/100 interface modules come with a selection of inline power capabilities and provide line-rate 10/100 Ethernet forwarding with the following operational advantages:

- Voice-ready modules with Cisco Inline Power and upgradable to 802.3af—Available in 48-port RJ-45 and RJ-21 configurations (WS-X6148-RJ45V and WS-X6148-RJ21V)
- Voice-ready modules with Cisco Inline Power and not upgradable to 802.3af—Available in 48-port RJ-45 and RJ-21 configurations (WS-X6348-RJ45V and WS-X6348-RJ21V)
- Voice-capable modules upgradable to Cisco Inline Power or 802.3af—Available in 48-port RJ-45 and RJ-21 configurations (WS-X6148-RJ-45 and WS-X6148-RJ-21)

Note: These modules are designed to fully support future upgrades to the IEEE 802.3af inline power standard currently underway, providing maximum investment protection, a new daughter card will be offered once the standard is ratified.

Forwarding architecture—Use centralized CEF forwarding

Forwarding performance—Forwards packets up to 15 Mpps per system

Fabric connection—Connect to the switch fabric using a 32-Gbps shared bus connection

Supervisor engine—Work with Supervisor Engine 1A, Supervisor Engine 2, or Supervisor Engine 720

Distributed forwarding upgrade—None; Classic interface modules cannot be upgraded for distributed forwarding

Slot requirements—Can occupy any slot in any Cisco Catalyst 6500 Series chassis

Maximum Port Density / Chassis—up to 576 ports / Cisco Catalyst 6513; up to 384 ports / Cisco Catalyst 6509

Transmit queue structure—2q2t = two round robin queues and two thresholds

Receive queue structure—1q4t = one round robin queue and four thresholds

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 768
Doc: 3702

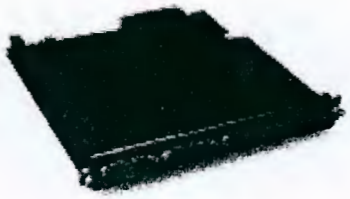
All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

17006
C

Table 7 Classic 10/100 Copper Voice Interface Modules

Product	Ports/ Interface/ Connectors	Maximum Distance/Cable Type	Maximum Frame Size (Jumbo Frame) Support	Inline Power for Voice Availability/ Capability
WS-X6148-RJ45	48-port; 10/100BASE-TX; RJ-45	100 meters; Category 5 cable	up to 9216 bytes	Cisco Inline Power; upgradable to 802.3af
WS-X6148-RJ21V	48-port; 10/100BASE-TX; RJ-21	100 meters; Category 5 cable	up to 9216 bytes	Cisco Inline Power; upgradable to 802.3af
WS-X6348-RJ45V	48-port; 10/100BASE-TX; RJ-45	100 meters; Category 5 cable	up to 8092 bytes	Cisco Inline Power; cannot upgrade to 802.3af
WS-X6348-RJ21V	48-port; 10/100BASE-TX; RJ-21	100 meters; Category 5 cable	up to 8092 bytes	Cisco Inline Power; cannot upgrade to 802.3af
WS-X6148-RJ-45	48-port; 10/100BASE-TX; RJ-45	100 meters; Category 5 cable	up to 9216 bytes	None provided; can upgrade to Cisco Inline Power or 802.3af
WS-X6148-RJ-21	48-port; 10/100BASE-TX; RJ-21	100 meters; Category 5 cable	up to 9216 bytes	None provided; can upgrade to Cisco Inline Power or 802.3af

Figure 4
Classic 10/100 Copper Voice Interface Modules
WS-X6148-RJ45



VWS-X6148-RJ21V

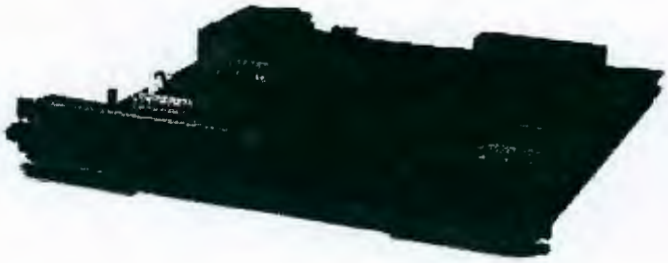
RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 769
Doc 3702

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

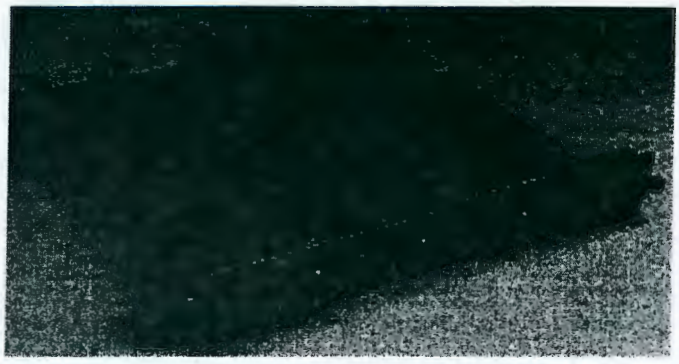
17005
L.

WS-X6348-RJ21V

WS-X6148-RJ-45



WS-X6148-RJ-21



Cisco Systems, Inc.
All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 770
Doc: 3702

17009
L

Cisco Catalyst CEF256 10/100 Copper Modules

Designed for small campus distribution and core layers and for data-center and Web-hosting applications where voice capability is not required, Cisco Catalyst CEF256 twisted-pair interface modules provide line-rate 10/100 Ethernet forwarding with the following operational advantages:

Forwarding architecture—Use the central CEF engine located on the supervisor engine

Forwarding performance—Forward packets up to 30 Mpps per system and up to 15 Mpps per slot for slots upgraded to support distributed forwarding

Fabric connection—Connect to the switch fabric using a single 8-Gbps switch fabric channel and a 32-Gbps shared bus

Supervisor engine—Work with Supervisor Engine 1A, Supervisor Engine 2, or Supervisor Engine 720

Distributed forwarding upgrade—Only required to perform distributed forwarding; require a WS-F6K-DFC3 upgrade to operate with Supervisor Engine 720; require a WS-F6K-DFC upgrade to operate with Supervisor Engine 2/ MFSC2 and an SFM

Slot requirements—Can occupy any slot in any Cisco Catalyst 6500 Series chassis

Maximum Port Density / Chassis—up to 576 ports / Cisco Catalyst 6513; up to 384 ports / Cisco Catalyst 6509

Transmit queue structure—1p3q1t = 1 priority queue, 3 round robin queues, 1 threshold

Receive queue structure—1p1q4t = 1 priority queue, 1 round robin queue, 4 thresholdse

Table 8 CEF256 Copper 10/100 Interface Modules

Product	Ports/Interface/ Connectors	Maximum Distance/Cable Type	Maximum Frame Size (Jumbo Frame) Support
WS-X6548-RJ-45	48-port; 10/100BASE-TX; RJ-45	100 meters; Category 5 cable	up to 9216 bytes / frame
WS-X6548-RJ-21	48-port; 10/100BASE-TX; RJ-21	100 meters; Category 5 cable	up to 9216 bytes / frame

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

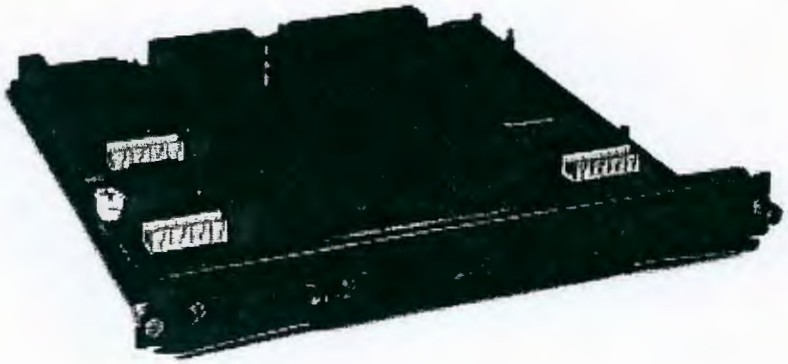
RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 771
3702
Doc:

17.005

Figure 5 shows high-density Cisco Catalyst CEF256 copper interface modules designed for distribution and core layers.

Figure 5
CEF256 Copper 10/100 Interface Modules
WS-X6548-RJ-45

WS-X6548-RJ-21



RQS nº 03/2005 - CN - CPMI - CORREIOS
772
Fls Nº
Doc: 3702

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

17002

Catalyst Classic 100FX and 10FL Fiber Interface Modules

Designed for deployment in wiring closets where optical interfaces are required, the Cisco Catalyst Classic fiber interface modules provide 10/100 Ethernet forwarding with the following operational advantages:

Forwarding architecture—Use centralized CEF forwarding

Forwarding performance—Forward packets up to 15 Mpps per system

Fabric connection—Connect to the switch fabric using a 32-Gbps shared bus connection

Supervisor engine—Work with Supervisor Engine 1A, Supervisor Engine 2, or Supervisor Engine 720

Distributed forwarding upgrade—None; Classic interface modules cannot be upgraded for distributed forwarding

Slot requirements—Can occupy any slot in any Cisco Catalyst 6500 Series chassis

Maximum Port Density / Chassis—up to 288 ports / Cisco Catalyst 6513; up to 192 ports / Cisco Catalyst 6509

Transmit queue structure—2q2t = 2 round robin queues, 2 thresholds

Receive queue structure—1q4t = 1 round robin queue, 4 thresholds

Note: No inline power support for voice is available for 100FX/10FL fiber modules.

Table 9 Classic 100FX/10FL Fiber Interface Modules

Product	Ports/ Interface/ Connectors	Maximum Distance/Cable Type	Maximum Frame Size (Jumbo Frame) Support
WS-X6324-100FX-MM	24-port; 100BASE-FX; MT-RJ	2 km; –62.5/125-micron multimode fiber; full or half duplex	up to 9216 bytes / frame
WS-X6324-100FX-SM	24-port; 100BASE-FX; MT-RJ	2 km; –62.5/125-micron multimode fiber; full or half duplex	up to 9216 bytes / frame
WS-X6024-10FL-MT	24-port; 10FL; MT-RJ	2 km; –62.5/125-micron multimode fiber; full or half duplex	up to 9216 bytes / frame

Figure 6
Classic 100FX/10FLFiber Interface Modules
WS-X6024-10FL-MT

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 773
Nº 3702
Doc:

17002
L

Cisco Catalyst CEF256 100FX Fiber Modules

Designed for small campus distribution and core layers and for data-center and Web-hosting applications, Cisco Catalyst dCEF256 fiber interface modules provide line-rate 100FX Ethernet forwarding with the following operational advantages:

Forwarding architecture—Use the central CEF engine located on the supervisor engine

Forwarding performance—Forward packets up to 30 Mpps per system and up to 15 Mpps per slot for slots upgraded to support distributed forwarding

Fabric connection—Connect to the switch fabric using one 8-Gbps connection and the 32-Gbps shared bus

Supervisor engine—Work with Supervisor Engine 1A, Supervisor Engine 2, or Supervisor Engine 720

Distributed forwarding upgrade—Only required to perform distributed forwarding; require a WS-F6K-DFC3 upgrade to operate with Supervisor Engine 720; require a WS-F6K-DFC upgrade to operate with Supervisor Engine 2/MFSC2 and a Switch Fabric Module

Slot requirements—Can occupy any slot in any Cisco Catalyst 6500 Series chassis

Maximum Port Density / Chassis—up to 288 ports / Cisco Catalyst 6513; up to 192 ports / Cisco Catalyst 6509

Transmit queue structure—1p3q1t = 1 priority queue, 3 round robin queues, 1 threshold

Receive queue structure—1p1q2t = 1 priority queue, 1 round robin queue, 2 thresholds

Note: No inline power support for voice is available for 100FX fiber modules.

Table 10 CEF256 100FX Fiber Interface Modules

Product	Ports/Interface/ Connectors	Maximum Distance/Cable Type	Maximum Frame Size (Jumbo Frame) Support
WS-X6524-100FX-MM	24-port; 100BASE-FX; MT- RJ	2 km; –62.5/125-micron multimode fiber; full or half duplex	up to 9216 bytes

Figure 7
CEF256 100FX Fiber Interface Modules
WS-X6524-100FX-MM

Cisco Systems, Inc.
All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 774
3702
Doc:

17.000
L

Ordering Information

Table 11 provides part number information for Catalyst 6500 Series 10/100 and 100/1000 Ethernet interface modules.

Table 11 Catalyst 6500 Series 10/100 and 100/1000 Ethernet Interface Modules

Product Number	Description
WS-X6024-10FL-MT	Catalyst 6500 24-port 10FL Classic interface module, multimode fiber, MT-RJ
WS-X6148-GE-TX	Catalyst 6500 48-port 10/100/1000 RJ-45 Classic interface module; field-upgradable to support Cisco Inline Power through voice daughter card (WS-F6K-VPWR=)
WS-X6148-VGE-TX	Catalyst 6500 48-port 10/100/1000 RJ-45 Classic interface module; with Cisco Inline Power through voice daughter card
WS-F6K-VPWR-GE=	Catalyst 6500 Inline power daughter card (WS-X6148-GE-TX, WS-X6548-GE-TX)
WS-X6148-RJ-21	Catalyst 6500 48-port 10/100 RJ-21 Classic interface module; field-upgradable to support Cisco Inline Power through voice daughter card (WS-F6K-VPWR=)
WS-X6148-RJ21V	Catalyst 6500 48-port 10/100 Telco RJ-21 Classic interface module with Cisco Inline Power
WS-X6148-RJ-45	Catalyst 6500 48-port 10/100 RJ-45 Classic interface module; field-upgradable to support Cisco Inline Power through voice daughter card (WS-F6K-VPWR=)
WS-X6148-RJ45V	Catalyst 6500 48-port 10/100 RJ-45 Classic interface module with Cisco Inline Power
WS-X6348-RJ21V	Catalyst 6500 48-port 10/100 Telco RJ-21 Classic interface module with Cisco Inline Power
WS-X6348-RJ45	Catalyst 6500 48-port 10/100 RJ-45 Classic interface module; field-upgradable to provide Cisco Inline Power through voice daughter card (WS-F6K-VPWR=)
WS-X6348-RJ45V	Catalyst 6500 48-port 10/100 RJ-45 Classic interface module with Cisco Inline Power
WS-F6K-VPWR=	Inline power daughter card to support Cisco Inline Power for Cisco Catalyst 6500 Series switches
WS-X6324-100FX-MM	Catalyst 6500 24-port 100FX Classic interface module, multimode fiber, MT-RJ
WS-X6324-100FX-SM	Catalyst 6500 24-port, 100FX Classic interface module, single-mode fiber, MT-RJ, with enhanced QoS
WS-X6548-RJ-45	Catalyst 6500 48-port, CEF256 10/100 RJ-45 interface module; field-upgradable to support distributed forwarding with the addition of the Distributed Forwarding daughter card (WS-F6K-DFC= or DFC3)
WS-X6548-RJ-21	Catalyst 6500 48-port, CEF256 10/100 RJ-21 interface module; field-upgradable to support distributed forwarding with the addition of the Distributed Forwarding daughter card (WS-F6K-DFC= or DFC3)
WS-X6516-GE-TX	Catalyst 6500 16-port 10/100/1000 RJ-45 CEF256 interface module; field-upgradable to support distributed forwarding with the addition of the Distributed Forwarding daughter card (WS-F6K-DFC= or DFC3)
WS-X6548-GE-TX	Catalyst 6500 48-port 10/100/1000 RJ-45 CEF256 interface module; field-upgradable to support Cisco Inline Power through voice daughter card (WS-F6K-VPWR-GE=)
WS-X6548-VGE-TX	Catalyst 6500 48-port 10/100/1000 RJ-45 CEF256 interface module; with Cisco Inline Power through voice daughter card

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
775
Fls Nº
3702
Doc:

16-999
2

Table 11 Catalyst 6500 Series 10/100 and 100/1000 Ethernet Interface Modules

Product Number	Description
WS-X6524-100FX-MM	Catalyst 6500 24-port, CEF256 100FX interface module; field-upgradable to support distributed forwarding with the addition of the Distributed Forwarding daughter card (WS-F6K-DFC= or DFC3)

Ordering Information—DFC Daughter Cards

Table 12 provides part number information for Catalyst 6500 Series 10/100 and 100/1000 Ethernet interface modules.

Table 12 Catalyst 6500 Series 10/100 and 100/1000 Distributed Forwarding Cards

Part Number	Description
WS-F6K-DFC	Distributed forwarding card
WS-F6K-DFC=	Distributed forwarding card, spare
MEM-DFC-256MB	256-MB DRAM option for DFC
MEM-DFC-256MB=	256-MB DRAM spare option for DFC
MEM-DFC-512MB	512-MB DRAM option for DFC
MEM-DFC-512MB=	512-MB DRAM spare option for DFC
WS-F6K-DFC3A	Catalyst 6500 Dist Fwd Card-3A for 65xx, 6816 Modules
WS-F6K-DFC3A=	Catalyst 6500 Dist Fwd Card-3A for 65xx, 6816 Modules, spare

Specifications

Standard Network Protocols

- Ethernet: IEEE 802.3, 10BASE-T
- Fast Ethernet: IEEE 802.3, 100BASE-TX, and 100BASE-FX
- Gigabit Ethernet: 1000BASE-TX
- IEEE 802.1d, IEEE 802.1p, IEEE 802.1q, IEEE 802.1s, IEEE 802.1w, IEEE 802.3x, IEEE 802.3z, IEEE 802.3ab, IEEE 802.3ad

Physical Specification

- Occupies one slot in a Cisco Catalyst 6500 Series chassis
- Dimensions (H x W x D): 1.2 x 14.4 x 16 in. (3.0 x 35.6 x 40.6 cm)

Environmental Conditions

- Operating temperature: 32 to 104 F (0 to 40 C)
- Storage temperature: –40 to 167 F (–40 to 75 C)
- Relative humidity: 10 to 90%, noncondensing
- Operating altitude: –60 to 4000 m

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN - CPMI - CORREIOS
776
Fls Nº
3702
Nº

16.998
2

Safety Compliance

- UL 1950
- CSA-C22.2 No. 950
- EN 60950
- IEC 950
- AS/NZS 3260
- IEC 825
- EN 60825
- 21CFR1040

EMC Compliance

- FCC Part 15 (CFR 47) Class A
- VCCI Class A with UTP, Class B with STP
- EN55022 Class A with UTP, Class B with STP
- CISPR 22 Class A with UTP, Class B with STP
- CE marking
- AS/NZS 3548 Class A with UTP, Class B with STP

Network Management

- ETHERLIKE-MIB (RFC 1643)
- IF-MIB (RFC 1573)
- Bridge MIB (RFC 1493)
- CISCO-STACK-MIB
- CISCO-VTP-MIB
- CISCO-CDP-MIB
- RMON MIB (RFC 1757)
- CISCO-PAGP-MIB
- CISCO-STP-Extensions-MIB
- CISCO-VLAN-Bridge-MIB
- CISCO-VLAN-Membership-MIB
- CISCO-UDLDP-MIB
- CISCO-ENTITY-FRU-CONTROL-MIB
- CISCO-COPS-CLIENT-MIB
- ENTITY-MIB (RFC 2037)
- HC-RMON
- RFC1213-MIB (MIB-II)
- SMON-MIB

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 777
3702
Doc:

16.997
L

Inline Power Specifications

- Output power per port: 48V DC power
- Pin assignment: 1, 2, 3, 6

Maximum Station-to-Station Cabling Distance

- 10/100BASE-TX, 100BASE-TX Fast Ethernet, and 10/100/1000: Category 5, 5e, and 6 UTP: 328 ft. (100 m), 100-ohm STP: 328 ft. (100 m); half or full duplex
- 100BASE-FX Fast Ethernet: 62.5/125-micron multimode fiber: 400-m half duplex, 2-km half or full duplex
- 100BASE-FX Fast Ethernet: 8/125-micron single-mode fiber: 10-km half or full duplex
- 10BASE-FL Ethernet: 62.5/125-micron multimode fiber: 2-km half or full duplex
- Maximum power: off (maximum power condition not reached); on (maximum power condition reached; no more phones will receive inline power from this module)

Indicators and Interfaces

- Status: green (operational); red (faulty); orange (module booting or running diagnostics)
- Link good: green (port active); orange (disabled); off (not active or not connected); blinking orange (failed diagnostic and disabled)
- 10/100/1000: RJ-45 (female)
- 10/100BASE-TX and 100BASE-TX: RJ-45 (female)
- 100BASE-FX: MT-RJ (female, multimode)
- 100BASE-FX: MT-RJ (female, single mode)
- 10BASE-FL: MT-RJ (female, multimode)

Cisco Technical Support Services

Whether your company is a large organization, a commercial business, or a service provider, Cisco is committed to maximizing the return on your network investment. Cisco offers a portfolio of technical support services to help ensure that your Cisco products operate efficiently, remain highly available, and benefit from the most up-to-date system software.

The Cisco Technical Support Services organization offers the following features, providing network investment protection and minimal downtime for systems running mission-critical applications:

- Provides Cisco networking expertise online and on the telephone
- Creates a proactive support environment with software updates and upgrades as an ongoing integral part of your network operations, not merely a remedy when a failure or problem occurs
- Makes Cisco technical knowledge and resources available to you on demand
- Augments the resources of your technical staff to increase productivity
- Complements remote technical support with onsite hardware replacement

Cisco Technical Support Services include:

- Cisco SMARTnet™ support
- Cisco SMARTnet Onsite support

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 778
Nº 3702
Doc:

16-996
L

- Cisco Software Application Services, including Software Application Support and Software Application Support plus Upgrades

For more information, visit:

http://www.cisco.com/en/US/products/svcs/ps3034/serv_category_home.html

Additional Cisco Catalyst 6500 Series Information

Visit this link for to view the following data sheets:

http://www.cisco.com/en/US/products/hw/switches/ps708/products_data_sheets_list.html

- Cisco Catalyst 6500 Series Data Sheet
- Cisco Catalyst 6500 Series Supervisor Engine 1A and Supervisor Engine 2 Data Sheet
- Cisco Catalyst 6500 Series Supervisor Engine 720 Data Sheet
- Cisco Catalyst 6500 Series Gigabit Ethernet Interface Modules Data Sheet
- Cisco Catalyst 6500 Series 10 Gigabit Ethernet Interface Modules Data Sheet
- Cisco Catalyst 6500 Series FlexWAN Interface Modules Data Sheet
- Cisco Catalyst 6500 Series Switch Fabric Interface Modules Data Sheet
- Cisco Catalyst 6500 Series Content Services Module (CSM) Data Sheet
- Cisco Catalyst 6500 Series Firewall Services Module Data Sheet
- Cisco Catalyst 6500 Series Network Application Module (NAM) Data Sheet
- Cisco Catalyst 6500 Series Intrusion Detection (IDS) Module Data Sheet
- Cisco Catalyst 6500 Series IPSec/VPN Services Module Data Sheet
- Cisco Catalyst 6500 Series SSL Services Module Data Sheet

CISCO SYSTEMS

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the **Cisco Web site at www.cisco.com/go/offices**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Catalyst, Cisco, Cisco IOS, Cisco Systems, the Cisco Systems logo, EtherChannel, and SMARTnet are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0303R)

28308/ETMG 06/02

PROS - 03/2005 - CN
CPMI - CORREIOS
779
FIS Nº
Doc 3702

ANEXO (6)

16-995

Cisco Systems

Data Sheet

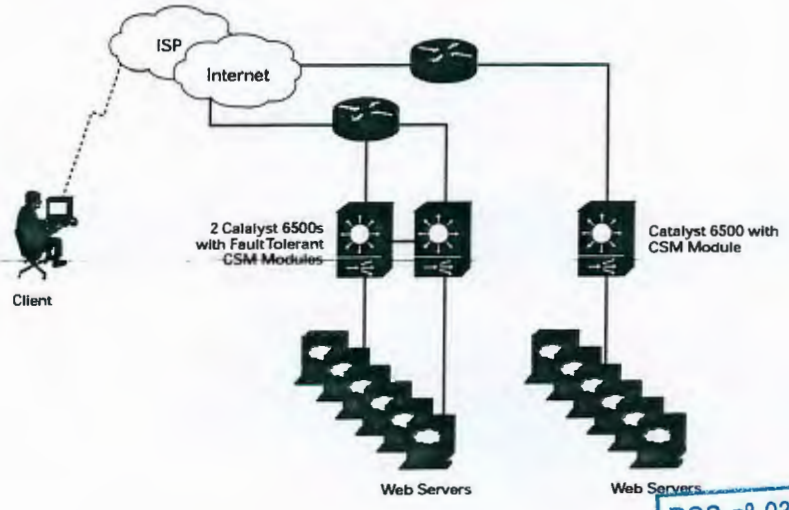
Cisco **Catalyst 6500** Series Content Switching Module

The Cisco Content Switching Module (CSM) is a Cisco Catalyst® 6500 line card that balances client traffic to farms of servers, firewalls, Secure Sockets Layer (SSL) devices, or virtual private network (VPN) termination devices. The Cisco CSM provides a high-performance, cost-effective load-balancing solution for enterprise and Internet service provider (ISP) networks. The Cisco CSM meets the demands of high-speed content delivery networks, tracking network sessions and server load conditions in real time and directing each session to the most appropriate server. Fault-tolerant Cisco CSM configurations maintain full state information and provide true hitless failover required for mission-critical functions.

The Cisco CSM provides the following key benefits (refer to Figure 1):

- Market-leading performance—The Cisco CSM establishes up to 165,000 Layer 4 connections per second (depending on software version) and provides high-speed content switching while maintaining 1 million concurrent connections.
- Outstanding price/performance value for large data centers and ISPs—The Cisco CSM features a low connection cost and occupies a small footprint. It slides into a slot in a new or existing Cisco Catalyst 6500 and enables all ports in the Cisco Catalyst 6500 for Layer 4–7 content switching.
- Multiple Cisco CSMs can be installed in the same Cisco Catalyst 6500.
- Ease of configuration—The Cisco CSM uses the same Cisco IOS® command-line interface (CLI) that is used to configure the Cisco Catalyst 6500 Switch.

Figure 1. The Cisco CSM



Cisco Systems, Inc.
All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 780
Nº Doc 3702

16.994
L

Content Switching Module Key Features

Firewall Load Balancing

The Cisco CSM allows you to scale firewall protection by distributing traffic across multiple firewalls on a per-connection basis, while ensuring that all packets belonging to a particular connection go through the same firewall. Both stealth and regular firewalls are supported.

URL and Cookie-Based Load Balancing

The Cisco CSM allows full regular expression pattern matching for policies based on URLs, cookies, and Hypertext Transfer Protocol (HTTP) header fields. The Cisco CSM supports any URL or cookie format—allowing it to load balance existing Web content without requiring URL/cookie format changes.

High Performance

The Cisco CSM performs up to 165,000 new Layer 4 TCP connection setups per second, depending on software version. These connections can be spread across 4096 virtual servers (16,384 real servers) and all the ports in a Cisco Catalyst 6500, or they can be focused on a single port. This provides a benefit over competitors who use distributed architectures that require use of all the ports in order to gain maximum performance.

Network Configurations

The Cisco CSM supports many different network topology types. A Cisco CSM can operate in a mixed bridged and routed configuration, allowing traffic to flow from the client side to the server side on the same or on different IP subnets.

IP Protocol Support

The Cisco CSM accommodates a wide range of common IP protocols—including TCP and User Datagram Protocol (UDP). Additionally, the Cisco CSM supports higher-level protocols, including HTTP, File Transfer Protocol (FTP), Telnet, Real-Time Streaming Protocol (RTSP), Domain Name System (DNS), and Simple Mail Transfer Protocol (SMTP).

User Session Stickiness

Whenever encryption or e-commerce is involved, it is important that the end user is consistently directed to the same server-that is, the server where the user's shopping cart is located or the encryption tunnel terminates. Cisco CSM User Session Stickiness provides the ability to consistently bring users back to the same server-based on SSL session ID, IP address, cookie, or HTTP redirection.

Load-Balancing Algorithms

The Cisco CSM supports the following load-balancing algorithms:

- Round robin
- Weighted Round Robin
- Least connections
- Weighted least connections
- Source and/or destination IP hash (subnet mask also configurable)
- URL hashing

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 781
Nº 3702 Data

16.993
L

Quality of Service

Providing differentiated levels of service to end users is important when generating revenue from content. The Cisco CSM takes advantage of the robust quality of service (QoS) of the Cisco Catalyst 6500, enabling traffic differentiation as follows:

- Correctly prioritizes packets based on Layer 7 rules
- Directs users who are paying more for services to faster or less loaded servers

High Availability

The Cisco CSM continually monitors server and appliation availability using health monitoring probes, inband health monitoring, return code checking, and the Dynamic Feedback Protocol (DFP). When a real server or gateway failure occurs, the Cisco CSM redirects traffic to a different location. Servers can be added and removed without disrupting service—systems can easily be scaled up or down.

Connection Redundancy

Optionally, two Cisco CSMs can be configured in a fault-tolerant configuration to share state information about user sessions and provide connection redundancy. If the active Cisco CSM fails, open connections are handled by the standby CSM without interruption, and users experience hitless failover—an important requirement for e-commerce sites and sites where encryption is used.

Global Server Load Balancing

The CSM offers multiple options for building a global or geographical load balanced environment. The CSM can act as an authoritative DNS and perform GSLB among geographically dispersed CSMs for the purposes of disaster recovery or for small GSLB environments with 2-4 locations. In addition, the CSM can report load information for it's Virtual IPs into the Global Site Selector (GSS), an appliance designed for advanced GSLB scaling up to 128 sites. With the many different GSLB options the CSM offers the ability to scale GSLB capabilities as growth demands.

Configuration Limits

- Total virtual LANs (VLANs) (client and server): 256
- Virtual servers: 4000
- Server farms: 4000

Cisco Systems, Inc.
All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 782
3702

16.993
L

- Real servers: 16,000
- Probes: 4000
- Access control list (ACL) items: 16,000

Performance Summary
1,000,000 concurrent TCP connections
165,000 connection setups per second—Layer 4
Total combined throughput of 4 Gigabits per second (client to server and server to client)
Cisco IOS Software only—Cisco Catalyst Operating System is not supported
Not fabric enabled—Functions as a bus-enabled line card
Multilayer Switch Feature Card (MSFC) or MSFC2
Occupies slot in the Cisco Catalyst 6500 chassis
Dimensions (H x W x D): 1.2 x 14.4 x 16 in. (3.0 x 35.6 x 40.6 cm)
Weight: 5 lb (2.27 kg)
Operating temperature: 32 to 104.5°F (0 to 40°C)
Nonoperating temperature: –40 to 158°F (–40 to 70°C)
Operating relative humidity: 10 to 90% (noncondensing)
Nonoperating relative humidity: 5 to 95% (noncondensing)
Operating and nonoperating altitude: Sea level to 10,000 ft (3050m)
Emissions: FCC Part 15 (CFR 47) Class A, ICES-003 Class A, EN55022 Class A, CISPR22 Class A, AS NZS 3548 Class A
Safety: CE Marking according to UL 1950, CSA 22.2 No. 950, EN 60950, IEC 60950, TS 001, AS/NZS 3260

Cisco Catalyst 6500 CSM Ordering Information

Product Number	Product Description
WS-X6066-SLB-APC	Cisco Catalyst 6500 Content Switching Module

RQS nº 03/2005 - CN -
CPMI - CORREIOS
783
Fls Nº
3702
Nº Doc:

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

16.992
2.

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems Europe
11, Rue Camille Desmoulins
92782 Issy-les-Moulineaux
Cedex 9
France
www-europe.cisco.com
Tel: 33 1 58 04 60 00
Fax: 33 1 58 04 61 00

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: 65 317 7777
Fax: 65 317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the

Cisco Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland
Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland
Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Copyright © 2002, Cisco Systems, Inc. All rights reserved. Catalyst, Cisco, Cisco IOS, Cisco Systems, and the Cisco Systems logo are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries. All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0208R)

Printed in the USA

RQS nº 03/2005 - CN -
CPMI - CORREIOS
784
Fls Nº
3702
Doc:

ANEXO (7)

16993

Data Sheet

Cisco Catalyst 6500 Series and Cisco 7600 Series
Network Analysis Module 1 and 2

Second-Generation, High-Performance Network Analysis Modules for Cisco Catalyst 6500 Series and Cisco 7600 Series

Cisco Systems®, the worldwide leader in networking for the Internet, addresses the need for multiservice network management and traffic monitoring in high-capacity switched Ethernet LANs and routed WANs with a new generation of the Network Analysis Module (NAM) for Cisco® Catalyst® 6500 Series switches and Cisco 7600 Series routers. The NAM is an integrated and powerful traffic monitoring service module that occupies a single slot in the chassis and enables network managers to gain application-level visibility into network traffic with the ultimate goal of improving performance, reducing failures, and maximizing returns on network investments.

The second-generation NAMs are available in two hardware versions, NAM-1 and NAM-2, and offer high performance monitoring and crossbar (fabric) connectivity to meet diverse network analysis needs in scalable switching and routing environments running at gigabit speeds. The NAMs come with an embedded, Web-based traffic analyzer, which provides full-scale remote monitoring and troubleshooting capabilities that are accessible through a Web browser.

Application-Level Visibility Built into the Network

The NAMs give network managers visibility into all layers of network traffic by providing application-level Remote Monitoring (RMON) functions based on RMON2 and other advanced Management Information Bases (MIBs). The NAMs add to the built-in Remote Monitoring (mini-RMON) features in Cisco Catalyst 6500 Series switches and Cisco 7600 Series routers that provide port-level traffic statistics at the Media Access Control (MAC) or data link layer. The NAMs provide intelligence to analyze traffic flows for applications, hosts, conversations, and network-based services such as quality of service (QoS) and voice over IP (VoIP).

Integrated Monitoring for LANs and WANs

The NAMS use several data sources from local and remote switches and routers to provide combined visibility into LAN and WAN environments. The NAMs collect data from physical ports, virtual LANs (VLANs), or Cisco EtherChannel®

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 785
Nº 3702
DIGIT

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

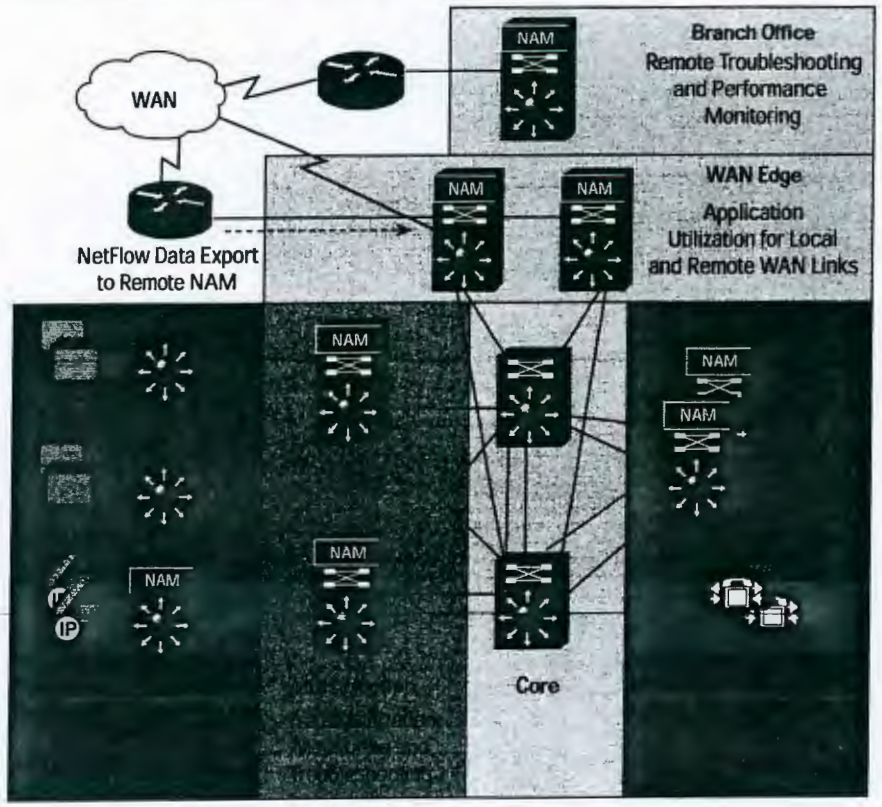
16.990
L

connections using the Switch Port Analyzer (SPAN) feature. For selective monitoring of large amount of traffic or for traffic from WAN interfaces, VLAN access control list (VACL)-based captures can be used to filter traffic before it is sent to NAM. In addition, the NAMs collect and analyze NetFlow Data Export from local and remote devices to provide broad application-level visibility into the network, including remote WAN segments. The NAMs also collect data from remote switches using the remote SPAN (RSPAN) feature of the Cisco Catalyst switches.

Flexible Deployment Scenarios

The NAMs can be deployed in the Cisco Catalyst 6500 Series at LAN aggregation points (for example, in the core or distribution layer) for proactive monitoring; at service points (for example, in data centers, server farms, or Cisco CallManager clusters in IP telephony networks) where performance is critical; and at important access points (critical clients, IP phone closets) where quick troubleshooting is required. They can also be deployed in Cisco 7600 Series routers at WAN edges or in Catalyst 6500 Series switches connected to WAN routers. When deployed at remote branch offices, the NAMs provide unique advantage to perform remote troubleshooting and traffic analysis through its Web-based Traffic Analyzer without having to send personnel or to haul large amounts of data to the central site. Figure 1 highlights the deployment of NAMs to enable comprehensive traffic monitoring and analysis for performance monitoring, troubleshooting, and capacity planning.

Figure 1
Deploying NAMs to Build Intelligence into the Network to serve a Variety of Applications



RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 786
Doc: 3702

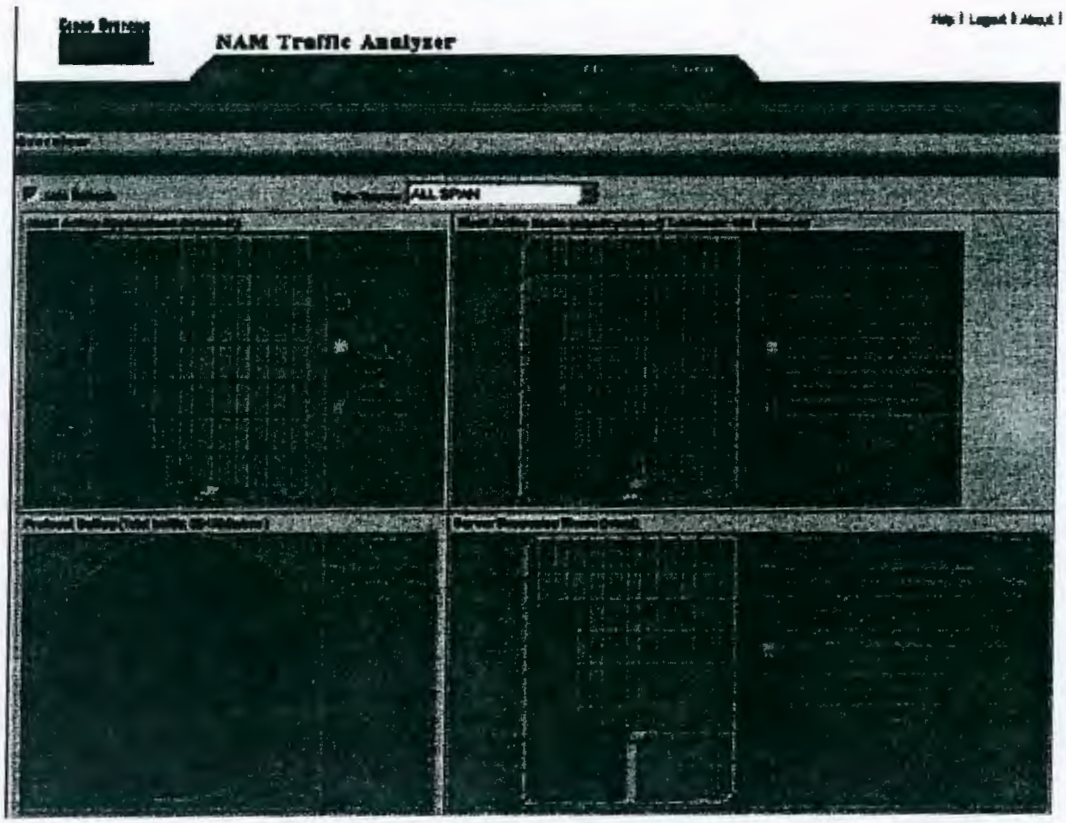
Cisco Systems, Inc.
All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

16.989
2

Easy to Deploy and Use

The NAMs come with the embedded, Web-based Traffic Analyzer with extensive monitoring and troubleshooting capabilities. Because the NAMs integrate monitoring functions directly into the switch and have complete data collection and data analysis capabilities on board, they are easy to deploy and managers can conveniently access data from anywhere using a Web browser (Figure 2). For security, users can be given role-based access and the Web-browser access can be secured with up to 168-bit encryption.

Figure 2
Web-Based Traffic Monitoring for both LAN and WAN with the embedded NAM Traffic Analyzer



The NAMs also provide the flexibility to use standards-based external applications using the Simple Network Management Protocol (SNMP). NetScout *n*Genius Real-Time Monitor, a component of the CiscoWorks LAN Management Solution (LMS), collects data from NAMs across the network and provides reports on traffic flow.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
787
Fls Nº
Doc: 3702

16 988

Major Benefits

- Increase return on network investment—The visibility provided by the NAMs enables better utilization of network resources to meet business objectives. They ease deployment of network-based services and help in capacity planning.
- Reduce productivity loss and revenue loss—Through proactive monitoring and quick troubleshooting capabilities, the NAMs prevent loss due to network degradation and downtime.
- Enhance network security—The NAMs provide investigation and verification capabilities to supplement other security mechanisms such as intrusion detection and firewalls. They can also be used to detect threats by watching anomalies in the network traffic.

Features and Applications

The data collected by the NAMs can be used for several vital management activities, including real-time and historical application monitoring, performance management, fault isolation, troubleshooting, and capacity planning. The NAMs also play an active role in managing differentiated services such as voice.

Real-Time and Historical Application Monitoring

Using RMON, RMON2, several extended RMON MIBs, and NetFlow, the NAMs detect the applications on the network and provide detailed real-time and historical information about how these applications utilize the bandwidth, which hosts access those applications, and which client/server pairs generate the most traffic (Figure 3A and 3B).

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 788
Doc: 3702

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

16.987
L

Figure 3A
Monitoring Applications and Hosts on the Network

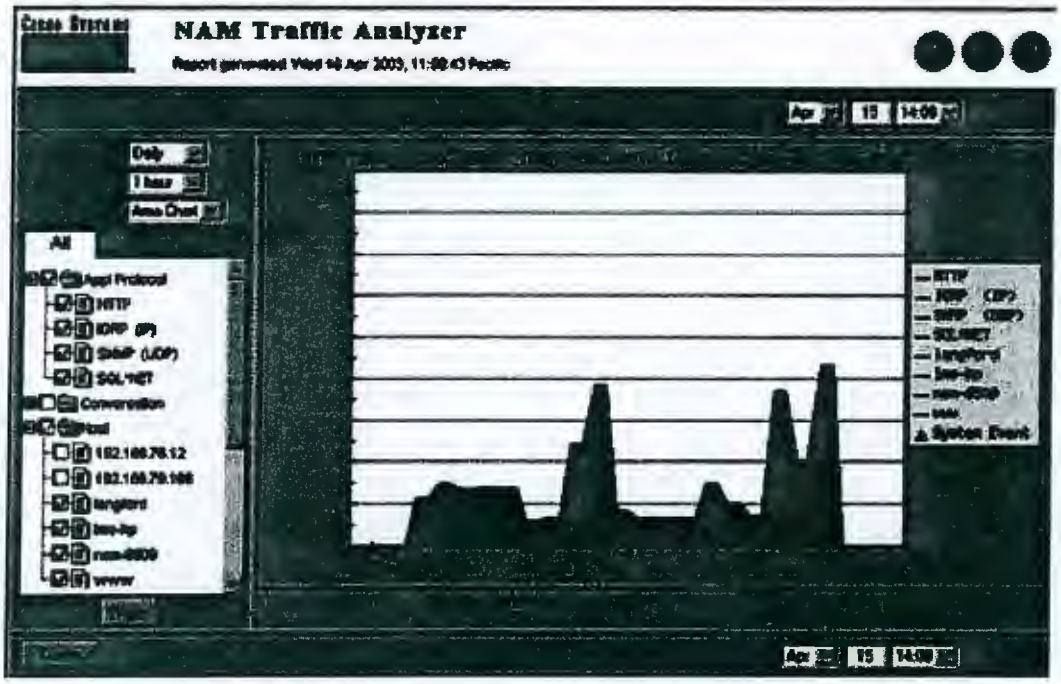
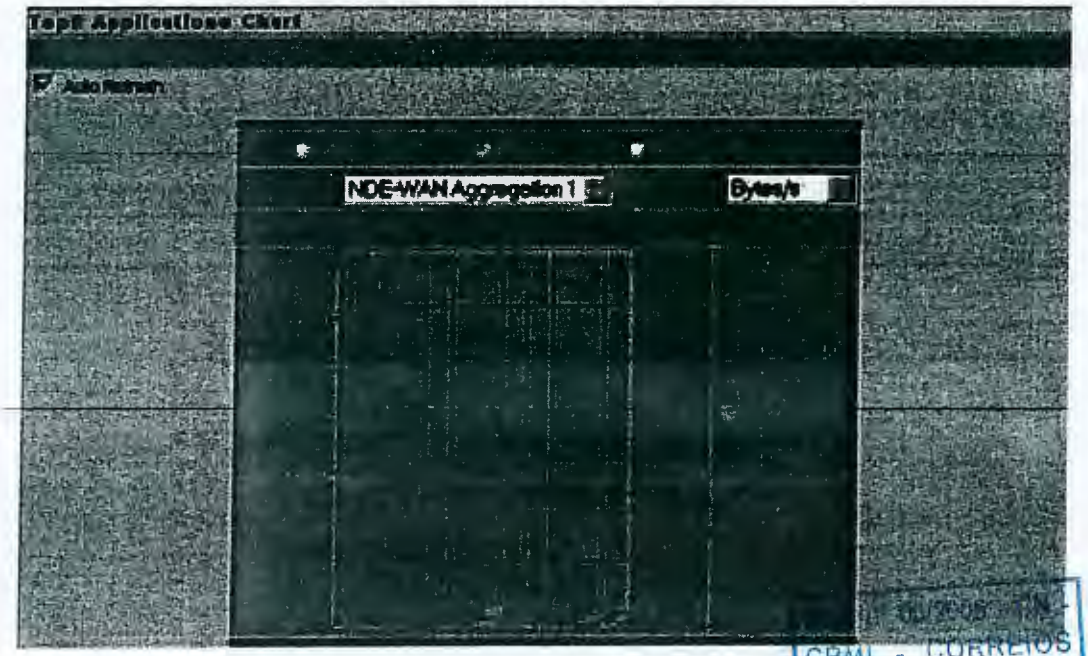


Figure 3B
Monitoring Application Utilization on a WAN link using NetFlow Data Export from a Remote Router



Cisco Systems, Inc.
All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

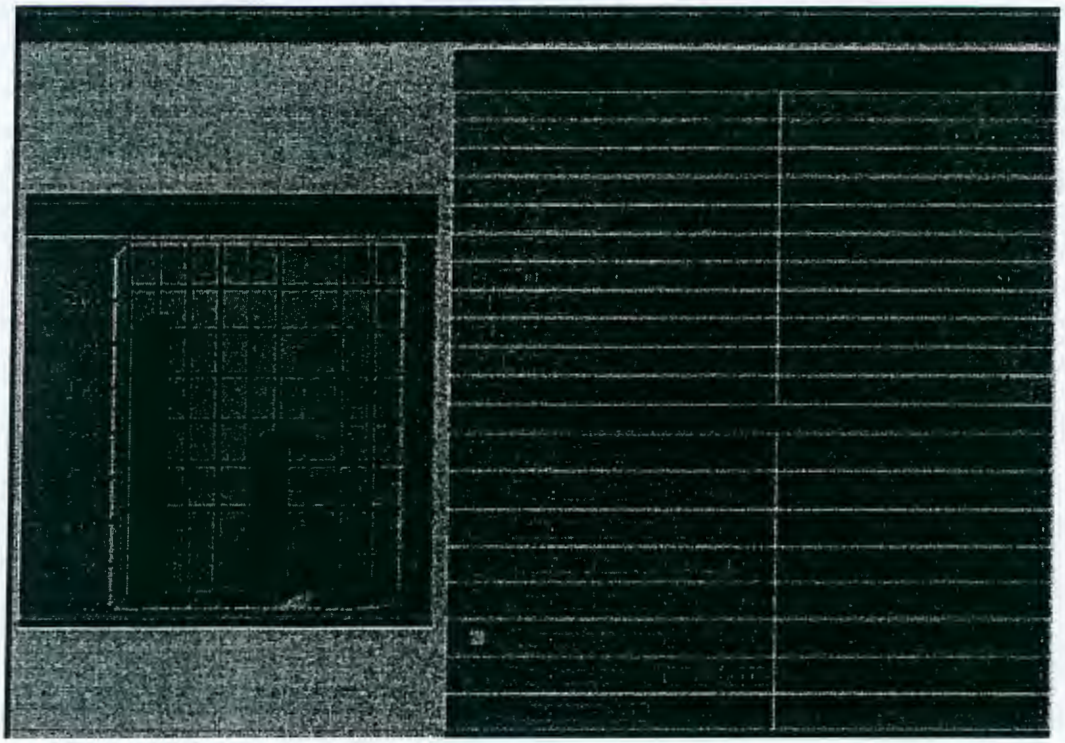
CPMI - CORREIOS
Fls Nº 789
3702

16.986

Performance Management

The NAMs provide valuable information about the delays in server responses to client requests. Using the Application Response Time (ART) MIB, developed by Cisco partner NetScout Systems, the NAMs can identify problems with applications or servers in critical environments such as e-commerce and IP telephony (Figure 4).

Figure 4
Application Response Time Monitoring



RQS nº 03/2005 - CN -
CPMI - CORREIOS
790
Fls Nº
3702
Doc:

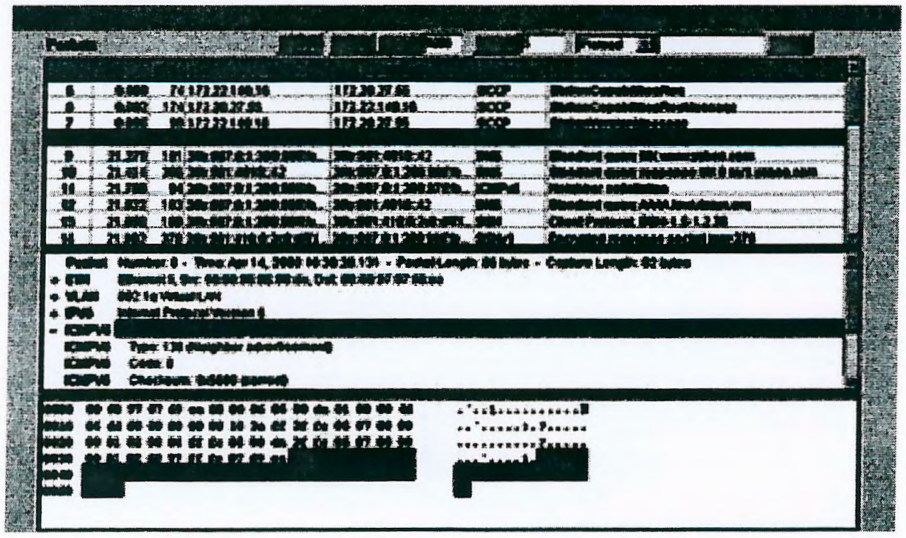
All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

16.935
2

Fault Isolation and Troubleshooting

Using the NAMs, network managers can set thresholds and alarms on various network parameters such as increased utilization, severe application response delays, and voice quality degradation, and be alerted to potential problems. The NAMs provide comprehensive views on applications, hosts, voice, quality of service (QoS), and so on, to isolate faults or malfunctions in the network. The NAM Traffic Analyzer can capture and decode packets in real time to aid troubleshooting (Figure 5).

Figure 5
Capturing and Decoding Packets with NAM



VoIP and QoS Monitoring

The NAMs can analyze voice traffic flows in real time to collect valuable information, including call setup details and voice quality metrics. Network managers can be alerted to voice quality degradation and can isolate potential problems (Figure 6).

The NAMs make the deployment of QoS for voice and other critical services effective by identifying violations of QoS policies. The NAMs support the Differentiated Services Monitoring (DSMON) MIB, which monitors traffic by differentiated services code point (DSCP) allocations defined by QoS policies (Figure 7).

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 791
Nº Doc: 3702

16.984
L

Figure 6
IP Telephony Monitoring

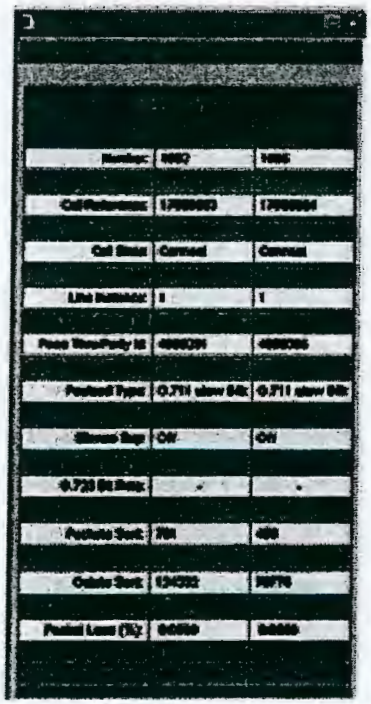
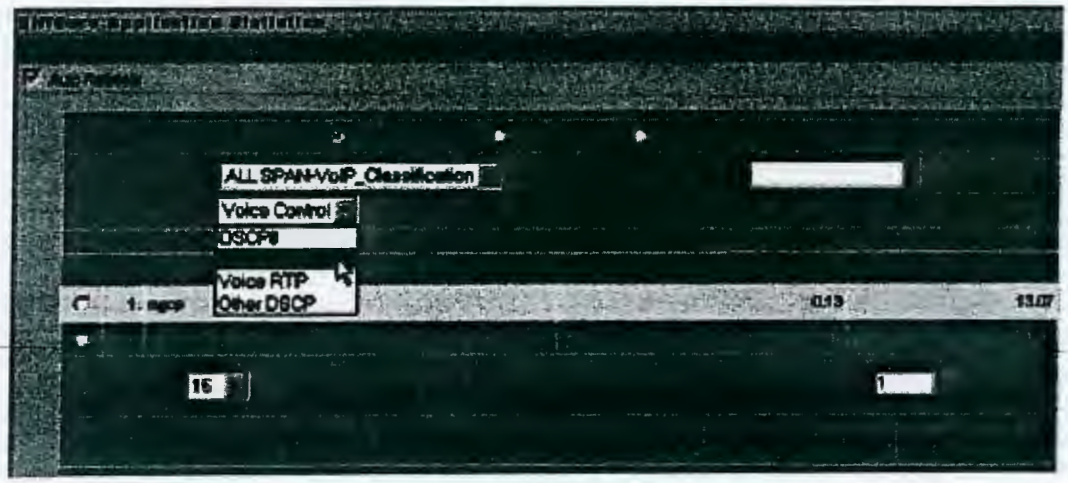


Figure 7
QoS Monitoring Using DSMON



RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 792
Doc 3702

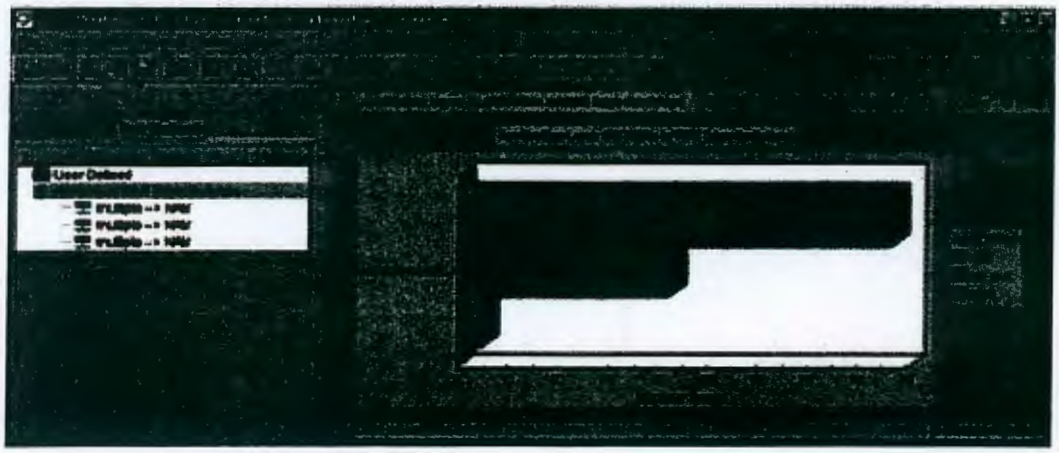
All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

16.983
2

Capacity Planning and Other Extended Applications

The data from the NAMs across the network can be collected by NetScout nGenius Real-Time Monitor, a component of the CiscoWorks LAN Management Solution (LMS) to provide consolidated views of network traffic (Figure 8). The NAMs serve as data sources for several other standards-based applications for a variety of purposes including capacity planning, long-term historical reporting and trending, anomaly-based threat detection, etc.

Figure 8
Aggregating data from NAMs across the network using NetScout nGenius Real-Time Monitor



Primary Advantages

- Integrated with network infrastructure—The NAMs occupy a single slot within the Cisco Catalyst 6500 Series or Cisco 7600 Series chassis and are deployed, managed, and supported as an integral part of the network infrastructure. They do not interfere with switching and routing functions and have their own processing resources. They are managed as a part of the network device using CiscoWorks management tools.
- Complete monitoring solution for LAN, WAN, and network-based services—The NAMs combine the functions of data collection agent and analysis application in one and provide comprehensive monitoring using a variety of data sources including RMON, RMON2 and NetFlow though the embedded Traffic Analyzer.
- Total cost of ownership savings—The integrated nature of the NAM solution saves costs in acquiring network device-specific features like mini-RMON, and in maintenance and technical support. The NAM Traffic Analyzer is embedded in the NAMs at no extra cost.
- Extensible, standards-based solution—The NAMs are compliant with open standards, and can be used with different monitoring applications to meet diverse needs.
- Secure solution—The NAM Traffic Analyzer can be deployed with up to 168-bit encryption, and SNMP can be disabled for fortifying external access to the NAM. The NAMs support Secure Shell (SSH) for secured command-line access.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 793
3702
Doc:

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

16.982
2

Network Monitoring Solutions

Cisco Systems offers a wide variety of solutions to provide complete visibility into network infrastructure. The comprehensive Cisco solution includes embedded technologies such as mini-RMON, NetFlow, Service Assurance Agent (SAA), Network-Based Application Recognition (NBAR); NAMs for the Cisco Catalyst 6500 Series and Cisco 7600 Series for value-added traffic analysis. and CiscoWorks network monitoring applications. nGenius Real-Time Monitor, a component of the CiscoWorks LAN Management Solution (LMS), collects mini-RMON data from switches to provide port utilization statistics and uses data from NAMs across the network to provide broad-based analysis and reports on network traffic. Cisco AVVID (Architecture for Voice, Video and Integrated Data) partners extend the Cisco network monitoring solution through a variety of applications that use embedded data sources and NAMs.

Technical Specifications

NAM-1

- High-performance dual processor architecture, 512 MB RAM
- Two data collection interfaces to backplane: 1 for SPAN/VACL data sources, 1 for NetFlow
- Second generation fabric enabled platform with interface to both bus and crossbar based architectures

NAM-2

- Extra high-performance dual processor architecture with hardware-based packet acceleration, 1 GB RAM
- Gigabit monitoring performance
- Three data collection interfaces to backplane: 2 for SPAN/VACL data sources (can be used independently or together), 1 for NetFlow
- Second generation fabric enabled platform with interface to both bus and crossbar based architectures

Supported Platforms

- NAM-1 and NAM-2 can be deployed in any slot in Cisco Catalyst 6500 and 6000 Series switches and Cisco 7600 Series routers [both bus- and crossbar (fabric)-based architectures]; multiple NAMs can be placed in the same chassis
- Supported with Cisco IOS® Software or Cisco Catalyst Operating System on the Supervisor Engine

Supported Topologies and Data Sources

- LAN—Switch Port Analyzer (SPAN) or Remote SPAN (RSPAN), VLAN ACL(VACL)-based captures, NetFlow (v1, v5, v6, v7, v8)
- WAN—NetFlow (v1, v5, v6, v7, v8) from local and remote devices, VLAN ACL (VACL)-based captures for FlexWAN/Optical Service Module (OSM) interfaces (Cisco IOS Software only)

Supported Interfaces and Applications

- HTTP/HTTPS with embedded web based NAM Traffic Analyzer
- SNMP v1, v2 with NetScout nGenius Real Time Monitor and other standards based applications

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 794
Nº 3702
Doc:

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

16.981

NAM Traffic Analyzer

- Embedded in NAM Software Version 2.2 and later for NAM-1/NAM-2
- Web based—Requires Microsoft Internet Explorer 5.0 or Netscape 4.7 (minimum)
- Supports Secure Sockets Layer (SSL) security with up to 168-bit encryption
- Role-based user authorization and authentication locally or using TACACS+
- Real-time and historical statistics (up to 100 days) on LAN/WAN traffic and network-based services

NAM Software Version 3.1

- Supports NAM-1 (part number WS-SVC-NAM-1), NAM-2 (WS-SVC-NAM-2) and first-generation NAM (WS-X6380-NAM)
- Supported with Cisco IOS® Software Release 12.1(13)E or Cisco Catalyst Operating System 7.3(1) minimum on the Supervisor Engine

Supported MIB Groups

The NAMs are standards-compliant and support RMON and RMON2 MIBs, as well as several extensions. The major MIB groups supported in the NAMs are:

- MIB-II (RFC 1213)—All groups except Exterior Gateway Protocol (EGP) and transmission
- RMON (RFC 2819)—All groups
- RMON2 (RFC2021)—All groups
- SMON (RFC2613)—DataSourceCaps and smonStats
- DSMON (RFC 3287)
- HC-RMON (RFC 3273)
- Application Response Time (ART)

Supported Protocols

The NAMs provide RMON2 statistics on several-hundred unique protocols, including those defined in RFC 2896, and several Cisco proprietary protocols. In addition, the NAMs can automatically detect unknown protocols and users have the flexibility to customize the protocol directory.

Examples of Protocols Supported by the NAMs for RMON2 Statistics:

- TCP and UDP over IP including IPv6
- VoIP including SCCP(Skinny), RTP/RTCP, MGCP, SIP
- Mobile IP protocols (Both IP in IP and GRE tunnelling)
- Storage area network (SAN) protocols including Fiber Channel over TCP/IP
- AppleTalk, DECnet, Novell, Microsoft
- Database protocols including Oracle, Sybase
- Bridge and router protocols
- Cisco proprietary protocols
- Unknown protocols by TCP/UDP ports, RPC program numbers, etc.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 795
3702
DRBC

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

16.990
L

Physical Specifications

- Dimensions (H x W x D): 1.2 x 14.4 x 16 in. (3.0 x 35.6 x 40.6 cm); Occupies any 1 slot in the chassis

Operating Environment

- Operating temperature: 32 F (0 C) to 104 F (40 C)
- Nonoperating and storage temperature: -40 F (-40 C) to 158 F (70 C)
- Operating relative humidity: 10% to 90% (noncondensing)
- Nonoperating relative humidity: 5% to 95% (noncondensing)
- Operating and nonoperating altitude: Sea level to 10,000 ft (3050 m)

Agency Approvals

- Regulatory: CE Marking (89/366/EEC and 73/23/EEC)
- Safety: UL 1950, CAN/CSA-C22.2 No. 950, EN 60950, IEC 60950
- Electromagnetic Emissions: FCC Part 15 (CFR 47) Class A, ICES-003 Class A, EN55022 Class A, CISPR22 Class A, AS/NZS 3548 Class A, VCCI Class A, EN55024, EN50082-1

Ordering Information

Cisco Part Number	Description
WS-SVC-NAM-1	Network Analysis Module-1 for Cisco Catalyst 6500 Series and Cisco 7600 Series
WS-SVC-NAM-2	Network Analysis Module-2 for Cisco Catalyst 6500 Series and Cisco 7600 Series
SC-SVC-NAM-3.1	Network Analysis Module Software v 3.1 for NAM-1, NAM-2 (includes ART, VoIP)

- The use of mini-RMON in Cisco Catalyst 6500 Series and Cisco 7600 Series with NAMs installed does not require the purchase of a separate RMON agent license.
- The Application Response Time (ART) MIB and the VoIP monitoring features are included at no extra cost for the NAM-1 and NAM-2. They require purchase of separate licenses (SC6K-NAM-ART-LIC= and SC6K-NAM-VOIP-LIC=) with the first-generation NAM (WS-X6380-NAM)
- Service Part Numbers for NAM-1 and NAM-2 are CON-xxx-WSSVCNAM1 and CON-xxx-WSSVNAM2 respectively, where "xxx" stands for level of support (for example, xxx= SNT = 8x5x Next Business Day)

More Information

http://www.cisco.com/en/US/products/hw/modules/ps2706/ps5025/index.html

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 796
3702

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

16.989

CISCO SYSTEMS

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the Cisco Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland
Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland
Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems, the Cisco Systems logo, Catalyst, and EtherChannel are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0303R)

203059/ETMG_04/03

ROS N° 03/2005 - 9N - CPMP - COMBELOS
Fls N° 3702
Doc:

ANEXO (3)

16 988

Technical Specifications

This appendix provides the technical specifications for the Catalyst 6000 series switches:

- Catalyst 6006 Switch, page A-2
- Catalyst 6009 Switch, page A-3
- Catalyst 6000 Series Power Supplies, page A-5
- Regulatory Standards Compliance, page A-7

Refer to the *Catalyst 6500 Series Module Installation Guide* for module and interface port specifications.

RQS nº 03/2005 - CN - CPMI - CORREIOS

Fls Nº 798

Nº 3702

Doc:

16.987

Catalyst 6006 Switch

The Catalyst 6006 switch specifications are provided in Table A-1.

Table A-1 Catalyst 6006 Switch Specifications

Item	Specification
Environmental	
Temperature, ambient operating	32°F (0°C) to 104°F (40°C)
Temperature, ambient nonoperating and storage	–40°F (–40°C) to 158°F (70°C)
Humidity (RH), ambient (noncondensing) operating	10% to 90%
Humidity (RH), ambient (noncondensing) nonoperating and storage	5% to 95%
Altitude, operating	Sea level to 6500 feet (2000 m)
Noise levels	45.8 to 49.6 dBa
Physical Characteristics	
Dimensions (H x W x D)	20.1 x 17.25 x 18.4 in. (51.1 x 43.1 x 46.0 cm) Chassis depth including cable guide is 21.64 in. (55.0 cm). Chassis requires 12 RU[1].
Weight	Chassis only: 45 lb (20.41 kg)
	Chassis fully configured with 1 supervisor engine, 5 switching modules, and 2 power supplies: 115 lb (52.15 kg)

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 799
Nº 3702
Doc:

16.936
L

Table A-1 Catalyst 6006 Switch Specifications (continued)

Item	Specification
Power Supply	1000 W AC-input, 1300 W AC-input or DC-input, 2500 W AC-input or 2500 W DC-input power supplies. An optional second power supply can be installed in the chassis.
Airflow	200 lfm[2] through system fan assembly. We recommend that you maintain a minimum air space of 6 inches (16 cm) between walls and the chassis air vents and a minimum horizontal separation of 12 inches (30.5 cm) between two chassis to prevent overheating.

1. RU = rack units
2. lfm = linear feet per minute

Catalyst 6009 Switch

The Catalyst 6009 switch specifications are provided in Table A-2.

Table A-2 Catalyst 6009 Switch/Catalyst 6509 Switch Specifications

Item	Specification
Environmental	
Temperature, ambient operating	32°F (0°C) to 104°F (40°C)
Temperature, ambient nonoperating and storage	–40°F (–40°C) to 158°F (70°C)
Humidity (RH), ambient (noncondensing) operating	10% to 90%
Humidity (RH), ambient (noncondensing) nonoperating and storage	5% to 95%
Altitude, operating	Sea level to 6500 feet (2000 m)
Noise levels	49.8 to 53.6 dBa

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 800
3702
Doc:

16.985

Table A-2 Catalyst 6009 Switch/Catalyst 6509 Switch Specifications (continued)

Item	Specification
Physical Characteristics	
Dimensions (H x W x D)	25.5 x 17.25 x 18.4 in. (64.8 x 43.1 x 46.0 cm) Chassis depth including cable guide is 21.64 in. (55.0 cm). Chassis requires 15 RU[1].
Weight	Chassis only: 55 lb (24.9 kg) Chassis fully configured with 1 supervisor engine, 8 switching modules, and 2 power supplies: 135 lb (61.2 kg)
Power Supply	1300 W AC-input or DC-input, 2500 W AC-input or DC-input power supply, or 4000 W AC-input power supply. An optional second power supply can be installed in the chassis.
Airflow	200 lfm[2] through system fan assembly. We recommend that you maintain a minimum air space of 6 inches (16 cm) between walls and the chassis air vents and a minimum horizontal separation of 12 inches (30.5 cm) between two chassis to prevent overheating.

1. RU = rack units
2. lfm = linear feet per minute

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 801
3702

16.984
L

Catalyst 6000 Series Power Supplies

Table A-3 lists the specifications for the Catalyst 6000 series power supplies.

Table A-3 Catalyst 6000 Series Power Supply Specifications

Item	Specification
1000 W AC-input Power Supply	
AC-input type	Autoranging input with power factor corrector.
AC-input voltage	100 to 240 VAC (10% for full range).
AC-input current	12 A @ 100 VAC, 6 A @ 240 VAC.
AC-input frequency	50/60 Hz (nominal) (3 Hz for full range).
Power supply output capacity	1000 W.
Power supply output	15 A @ +3.3 V, 5 A @ +5 V, 6 A @ +12 V, 20.3 A @ +42 V.
Output holdup time	20 ms minimum.
1300 W AC- and DC-input Power Supplies[1]	
AC-input type	Autoranging input with power factor corrector.
AC-input voltage	100 to 240 VAC (10% for full range).
AC-input current	17.25 A @ 100 VAC, 8 A @ 200 VAC.
AC-input frequency	50/60 Hz (nominal) (3 Hz for full range).
DC-input voltage	–48 VDC to –60 VDC continuous.
DC-input current	38 A @ -48 VDC, 30 A @ -60 VDC.
Power supply output capacity	1300 W maximum AC-input; 1360 W DC-input.
Power supply output (AC supply)	15 A @ +3.3 V, 5 A @ +5 V, 6 A @ +12 V, 27.46 A @ +42 V.
Power supply output (DC supply)	15 A @ +3.3 V, 5 A @ +5 V, 6 A @ +12 V, 30 A @ +42 V.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
802
Fls Nº
3702
Doc:

16.983
2

Table A-3 Catalyst 6000 Series Power Supply Specifications (continued)

Item	Specification
DC input terminal block	Accepts 3–10 AWG copper conductors. Actual size of the wire needed is determined by the installer or local electrician. Terminal block material rated at 120°C.
Output holdup time	20 ms minimum (AC-input power supply). 8 ms (DC-input power supply).
2500 W AC- and DC-input Power Supplies	
AC-input type	Autoranging input with power factor corrector.
AC-input voltage	100 to 120 VAC, 200 to 240 VAC (10% for full range).
AC-input current	16 A maximum at 200 VAC at 2500 W output. 16 A maximum at 100 VAC at 1300 W output.
AC-input frequency	50/60 Hz (nominal) (3% for full range).
Power supply output capacity	1300 W maximum (100–120 VAC). 2500 W maximum (200–240 VAC or –48 to –60 VDC).
System power dissipation	3520 W (total input power) or 3.6 KVA (high-line operation).
DC-input voltage	–48 VDC to –60 VDC continuous.
DC-input current	80 A @ -40.5 VDC, 70 A @ -48 VDC, 55 A @ -60 VDC.
Power supply output (AC supply)	15.5 A @ +3.3 V, 5 A @ +5 V, 6 A @ +12 V, 27.5 A @ +42 V (100/120 VAC). 15 A @ +3.3 V, 5 A @ +5 V, 10 A @ +12 V, 55.5 A @ +42 V (200/240 VAC).
Power supply output (DC supply)	15 A @ +3.3 V, 5 A @ +5 V, 10 A @ +12 V, 55.5 A @ +42 V.
DC input terminal block	Accepts 2–14 AWG copper conductors. Actual size of the wire needed is determined by the installer or local electrician. Terminal block material rated at 150°C.
Output holdup time	20 ms minimum (AC-input power supply). 4 ms (DC-input power supply).

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 803
3702
Doc:

16-982

Table A-3 Catalyst 6000 Series Power Supply Specifications (continued)

Item	Specification
4000 W AC-input Power Supply	
AC-input type	High-line input with power factor corrector, 30 A single-phase circuit.
AC-input voltage	200 to 240 VAC (10% for full range).
AC-input current	23 A.
Power supply output capacity	4000 W maximum.
AC-input frequency	50/60 Hz (nominal) (3% for full range).
KVA rating	5.4 kVA maximum.
Maximum output current	15 A @ +3.3 V, 5 A @ +5 V, 10 A @ +12 V, 91.20 A @ +42 V.
Output holdup time	20 ms minimum.

1. Some early versions of the 1300 W AC-input power supply were marked as 1800 W. This value refers to the input power rating or maximum system power dissipation of the power supply. The output power of the power supply is 1300 W. Power supplies currently shipping are marked as 1300 W.

Regulatory Standards Compliance

Catalyst 6000 series switches comply with the regulatory standards listed in the *Regulatory Compliance and Safety Information for the Catalyst 6500 Series Switches* document.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 804
3702
Doc:

16.981

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 805
Nº 3702
Doc:

ANEXO (9) A

16.980
L

Cisco Catalyst 6500 Content **Switching** Module Software Version 2.1(1)

New Features

Firewall Load Balancing

Firewall load balancing allows you to scale firewall protection by distributing traffic across multiple firewalls on a per-connection basis. Version 2.1(1) of the Cisco Catalyst® 6500 Content Switching Module (CSM) supports configurations for both standard and stealth firewalls and has the performance necessary to scale for high-performance networks with many firewalls.

Connection RedundancyStateful Failover

You can configure two CSMs, either in the same chassis or in two different chassis, in a fault-tolerant pair to share state information about user sessions and provide connection redundancy. If the active CSM fails, open connections are handled by the standby CSM without interruption, and users experience hitless failover—an important requirement for e-commerce sites and sites where encryption is used.

Multiple CSMs in a Chassis

This feature allows multiple CSM blades to be simultaneously inserted into a Catalyst 6500 Series Switch for redundancy or increased performance. In addition, you can simultaneously use both IOS-SLB and one or more CSMs in the same chassis.

HTTP 1.1 Persistence

With connection persistence, you can dispatch multiple HTTP requests from the client to the server on the same persistent connection. Implementation of "persistence" support allows for independent switching of each successive HTTP request in a persistent connection. As a new HTTP request arrives, it can be switched to the same server as the prior request or to a different server.

Load Balancing of All Common IP Protocols

In Version 1.1, the CSM load-balanced TCP traffic only. The current version of CSM balances traffic consisting of all common IP protocols including User Datagram Protocol (UDP).

URL Hashing

This feature is an additional predictor for Layer 7 connections in which the real server is chosen using a hash value based on the URL. This hash value is computed on the entire URL or on a portion of it.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls' Nº 806
3702
Doc:

Cisco Systems, Inc.
All contents are Copyright © 1992–2001 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

16.979

Generic Header Parsing

The CSM parses, matches, and switches connections based on the HTTP URL or cookie value. With this version, additional information about the end user is included in the header record of a HTTP request. The information, such as an end user's browser device type or selected language, is important to business segments that provide content services to end users. The content must be tailored for an end user with a personal handheld device versus for an end user with a desktop PC. The ability to select Web servers based on any user data helps businesses better organize content for their customers.

VPN and IP Security Protocol Load Balancing

In addition to support for generic IP protocols, specific enhancements to the CSM optimize virtual private networking (VPN) and IP Security Protocol (IPSec) load balancing.

SNMP Server Health Traps

Simple Network Management Protocol (SNMP) server traps can now be configured on the CSM. Full SNMP support will be available on the CSM in a future release.

Orderable Product Numbers

CSM Software Release	Hardware Part Number	Software Part Number	Hardware Requirements	Native Cisco IOS Software Release	Added Features
1.2(1)	WS-X6066-SLB-APC	SC6k-1.2-CSM	Supervisor 1A with Multiswitch Feature Card (MSFC) and Policy Feature Card (PFC) or Supervisor 2 Module with MSFC 2	12.1(8a)e	Supervisor 2 support Route Health Injection
2.1(1)	WS-X6066-SLB-APC	SC6k-2.1-CSM	Supervisor 1A with MSFC & PFC or Supervisor 2 with MSFC 2	12.1(8a)EX or 2.1	Firewall Load Balancing Non-TCP Load Balancing URL Hashing HTTP 1.1 Persistence Full Stateful Failover Generic Header Parsing SNMP Server Health Traps Multiple CSM in a Chassis VPN/IPSec Load Balancing

Further Information

Download this software version at:
http://www.cisco.com/cgi-bin/tablebuild.pl/cat6000-intellother

CSM Data Sheet: http://www.cisco.com/en/US/products/hw/modules/ps2706/products_data_sheet09186a00800887f3.html

CSM Installation and Configuration Guide: httP://www.cisco.com/en/US/products/hw/switches/ps708/products_installation_and_configuration_guide_book09186a008007fa85.html

Version 1.2(1) Release Notes: http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/relnotes/index.htm

Marketing Contacts

Dyan Gray, dpgray@cisco.com

Stephanie Pache, sapache@cisco.com

RQS nº 03/2005 - CN -
CPMI - CORREIOS
807
Fls Nº
Doc 3702

Cisco Systems, Inc.
All contents are Copyright © 1992–2001 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

16-978

Stefano Testa, testas@cisco.com

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems Europe
11, Rue Camille Desmoulins
92782 Issy-les-Moulineaux
Cedex 9
France
www-europe.cisco.com
Tel: 33 1 58 04 60 00
Fax: 33 1 58 04 61 00

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems Australia, Pty., Ltd
Level 9, 80 Pacific Highway
P.O. Box 469
North Sydney
NSW 2060 Australia
www.cisco.com
Tel: +61 2 8448 7100
Fax: +61 2 9957 4350

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the

Cisco Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia
Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru
Philippines • Poland • Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa
Spain • Sweden • Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Copyright © 2001, Cisco Systems, Inc. All rights reserved. AccessPath, AtmDirector, Browse with Me, CCIP, CCSI, CD-PAC, *CiscoLink*, the Cisco *Powered* Network logo, Cisco Systems Networking Academy, the Cisco Systems Networking Academy logo, Fast Step, Follow Me Browsing, FormShare, FrameShare, GigaStack, IGX, Internet Quotient, IP/VC, iQ Breakthrough, iQ Expertise, iQ FastTrack, the iQ logo, iQ Net Readiness Scorecard, MGX, the Networkers logo, *Packet*, RateMUX, ScriptBuilder, ScriptShare, SlideCast, SMARTnet, TransPath, Unity, Voice LAN, Wavelength Router, and WebViewer are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, Discover All That's Possible, and Empowering the Internet Generation are service marks of Cisco Systems, Inc. and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Enterprise/Solver, EtherChannel, EtherSwitch, FastHub, FastSwitch, IOS, IP/TV, LightStream, MICA, Network Registrar, PIX, Post-Routing, Pre-Routing, Registrar, StrataView Plus, Stratm, SwitchProbe, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0108R)

LW2792 10/01

Printed in the USA

PUC Nº 0432005 - CN -
CT/MF - CORREIOS
Fls Nº 808
Nº Doc: 3702

ANEXO (27)

16.977
L

Catalyst 6500 Series Supervisor Engines

The supervisor engines for Catalyst® 6500 Series switches deliver the latest advanced switching technology with proven Cisco software to power a new generation of scalable and intelligent multilayer switching solutions for both enterprise and service provider environments. Designed to bring data, voice, and video integration onto a single platform for fully integrated communications in the access, distribution, and core layers of the network, the Catalyst 6500 Series Supervisor Engines provide a modular and flexible approach to building intelligent, resilient, scalable, and converged high performance multilayer switching solutions. The table below highlights the options available in the supervisor engines for the Catalyst 6500 Series switches.

Table 1 Available Options in the Catalyst 6500 Supervisor Engines

	Max Port Density		Forwarding Performance			QoS & Security		High Availability			
	10/100	Gigabit	Bandwidth	Aggregate System Forwarding Performance	IP Multicast Hardware Support	QoS/ACL Look Up Performance	ACL Entries (QoS + Security)	Stateful Failover	Backplane Redundancy with SFM	HSRP	Ether Channel Across Modules
Supervisor1A	384	130	32 Gbps	15 Mpps				Yes			Yes
Supervisor1A + PFC	384	130	32 Gbps	15 Mpps		15 Mpps	16K	Yes			Yes
Supervisor2 + PFC2	576	194	256 Gbps	30 Mpps		30 Mpps	32K+32K	Yes	Yes		Yes
Supervisor1A+ PFC+MSFC2	384	130	32 Gbps	15 Mpps	(S,G)	15 Mpps	16K	Yes		Yes	Yes
Supervisor2+ PFC2+MSFC2	576	194	256 Gbps	30 / 210[1] Mpps	(S,G) & (*,G)	30 / 210[1] Mpps	32K + 32K	Yes	Yes	Yes	Yes

1. When deployed in Distributed CEF mode

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 809
Doc: 3702

Cisco Systems, Inc.
All contents are Copyright © 1992–2001 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

16.976

Table 1 Available Options in the Catalyst 6500 Supervisor Engines (continued)

	Management				Applications		
	Policing Performance	Number of Aggregate Policers	Netflow Statistics	Remote SPAN	Flex WAN Support	Optical Switch Modules Support	Application
Supervisor1A							Wiring closets with Layer 2 forwarding
Supervisor1A + PFC	15 Mpps	1023	Yes	Yes			Premier AVVID Wiring Closets with Enhanced QoS, Security, with Layer 2 forwarding
Supervisor2 + PFC2	30 Mpps	1023	Yes	Yes			High Density Premier AVVID Wiring Closets and Server Farms
Supervisor1A+ PFC+MSFC2	15 Mpps	1023	Yes	Yes	Yes		Distribution and Backbone applications
Supervisor2+ PFC2+MSFC2	30 Mpps	1023	Yes	Yes	Yes	Yes	High Performance Distribution, Backbone, WAN Edge Applications

The Catalyst 6500 Series supervisors listed in Table 1 can be deployed in any of the Catalyst 6500 series chassis to meet the rapidly evolving needs of today's networks (Please note that Catalyst 6513 chassis requires Supervisor Engine 2). This broad range of highly modular supervisor offerings enables the Catalyst 6500 Series to deliver products that are optimized for the access, distribution, and core layers of the network.

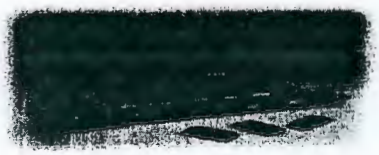
Wiring Closet and Server Farm Applications

As the access point into an enterprise network the wiring closet must provide more than sheer "speeds and feeds". The full benefits of a converged data, multimedia, and voice network can be realized only when the valuable network services are that created extend from the network core to the access layer. As such, wiring closets and server farms must provide:

- Scalable connectivity
- Security
- High availability

In addition, they must define and enforce the operational characteristics of the entire enterprise network.

Figure 1 Supervisor 1A



RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 810
Doc: 3702

Cisco Systems, Inc.
All contents are Copyright © 1992–2001 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

16.975

The Catalyst 6500 Supervisor Engine 1A supports up to 15 Mpps of Layer 2 forwarding and scales 10/100 Ethernet port densities to 384 ports per chassis. The Catalyst 6500 Series Supervisor Engine 1A can be used in the Catalyst 6000 (6006, 6009) and Catalyst 6500 (6506, 6509) Series chassis, thereby providing investment protection through scalability and common sparing. The Supervisor Engine 1A provides Quality of service (QoS) using Layer 2 destination MAC addresses, VLANs, and marking using layer 2 CoS values.

Figure 2 Supervisor Engine 1A with PFC

The addition of the Policy Feature Card (PFC) to the Supervisor Engine 1A provides granular per-port recognition and classification of different types of traffic, and enables admission control to manage which applications are granted access to the network. The PFC is an integral part of the CiscoAssure end-to-end quality of service (QoS) and policy-based security solution.

The PFC can identify user applications such as voice, enterprise resource planning (ERP), or multicast and classify traffic with the appropriate priority level. The PFC delivers the intelligence to arbitrate traffic across various metrics such as application type, user, security, predetermined policy, and so on to ensure that business-critical traffic is unaffected by unimportant applications such as network games. For example, delay sensitive traffic, such as voice over IP (VoIP), can be given higher priority over a "Doom" game traffic.

The PFC also enables admission control in the access layer to prevent unauthorized applications from being allowed onto the network. It also supports intra-VLAN hardware-based protocol filtering, thus enabling intelligent broadcast control and increasing resource utilization and network performance. Furthermore, it supports the ability to redirect specific traffic to a selected port or group of ports for network analysis.

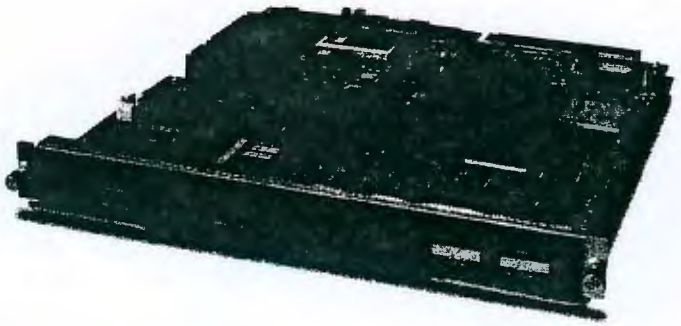
When the advanced feature benefits of the PFC are coupled with other Cisco solutions such as IP-telephony handsets, customers can realize the financial benefits of a converged voice/video/data access layer network. Two networks can be collapsed into a single, intelligent IP-based network for more cost-effective moves, adds, and changes, decreased management staff, and access to new Web-based multiservice applications such as video on demand (VoD), NetMeeting, and "click-to-call" applications. The ability to deliver these benefits by providing enhanced intelligent network services at wire speeds makes the Catalyst 6500 Series switches the most advanced switches in the industry.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 811
Doc: 3702

All contents are Copyright © 1992–2001 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

16.975
2

Figure 3 Supervisor Engine 2



Designed to meet the needs of very high density, resilient wiring closets and data centers/server farms, the Catalyst 6500 Series Supervisor Engine 2 provides industry-leading scalability of intelligent multilayer switching services up to 210 Mpps. The Catalyst 6500 Series Supervisor Engine 2 can be used in the Catalyst 6000 (6006, 6009) and Catalyst 6500 (6506, 6509, 6513) Series chassis, and it scales 10/100 Ethernet port densities to 576 ports per chassis. When deployed in Catalyst 6500 Series chassis (Catalyst 6506, 6509, 6513), the Supervisor Engine 2 in conjunction with the Switch Fabric Module (SFM, SFM2) can scale the total system bandwidth to 256 Gbps. This scalability in performance and densities offers an economical approach to deploying networks that can be incrementally scaled to meet the rapidly evolving needs of mission critical networks.

The PFC2, which is standard on the Supervisor Engine 2, is a critical component of the CEF architecture. While offering all the benefits of the PFC, the PFC2 on the Supervisor Engine 2 significantly scales the centralized forwarding and hardware support for QoS and Access Control Lists ACLs to 30 Mpps. The PFC2 also provides increased granularity of high performance support for per-port QoS and ACLs by supporting 4-times larger tables for ACL and QoS entries.

To facilitate uninterrupted availability of mission critical applications to users, Catalyst 6500 Series switches enable a resilient, self-healing network architecture by supporting synchronized dual supervisor configurations in both the Supervisor Engines 1A and 2. If a supervisor fails, High-Availability switchover transfers switch control to the redundant Supervisor within 1 to 3 seconds. This stateful failover is facilitated by the maintenance synchronized protocol states between the primary and redundant supervisors. Another major benefit of this High Availability architecture of the Catalyst 6500 Series Supervisor Engines 1A & 2 is the Hitless Software Upgrade feature, which allows customers to transparently upgrade

Core and Distribution Applications

Enterprises and service providers have recently begun to deploy applications based on Internet technology to enable solutions such as converged voice and data networking, e-commerce, e-learning, and centralized application delivery. Deployment of these applications requires higher end-to-end bandwidth to support simultaneous application delivery to hundreds or even thousands of end users. It is also critical that the intelligent network services required to control individual traffic flows, such as QoS and security, can grow along with the bandwidth to ensure scalable application delivery tied to business priorities and requirements. At the same time, businesses are not able to decommission existing applications or networks overnight in favor of new Internet-based business applications. Instead, existing applications and infrastructure must coexist with the new solutions for some time as the network is updated and the support staff is trained to support the new application requirements.

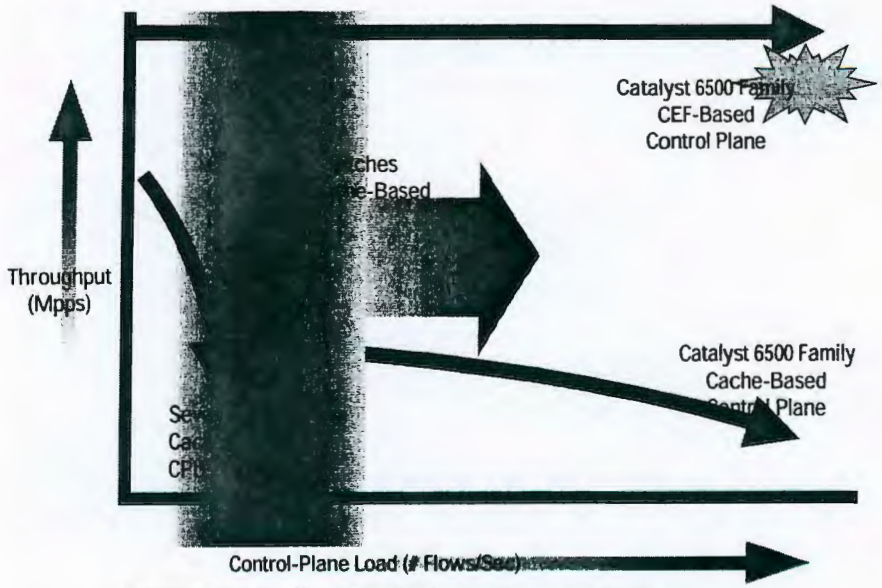
RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 812
3702
Doc:

All contents are Copyright © 1992–2001 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

16.974

The Catalyst 6500 Supervisor Engine 2 is an innovative solution to the requirement for scalable bandwidth with intelligent network services and flexible migration options. Based on the state-of-the-art Cisco Express Forwarding (CEF) architecture, the Supervisor Engine 2 delivers unmatched scalability in intelligence and performance under conditions of highly dynamic traffic flows. Starting with 30 Mpps of centralized CEF, the Catalyst 6500 Series Supervisor Engine 2 provides industry-leading scalability of intelligent multilayer switching services up to 210 Mpps. This scalability enables enterprises and service providers to deploy highly integrated Internet business solutions that require high end-to-end bandwidth to support simultaneous application delivery to hundreds or even thousands of end users.

Figure 4 Scaling Data-Plan Performance with Cisco Express Forwarding



See Mier Communications, Inc.'s Report: **www.mier.com/publications**

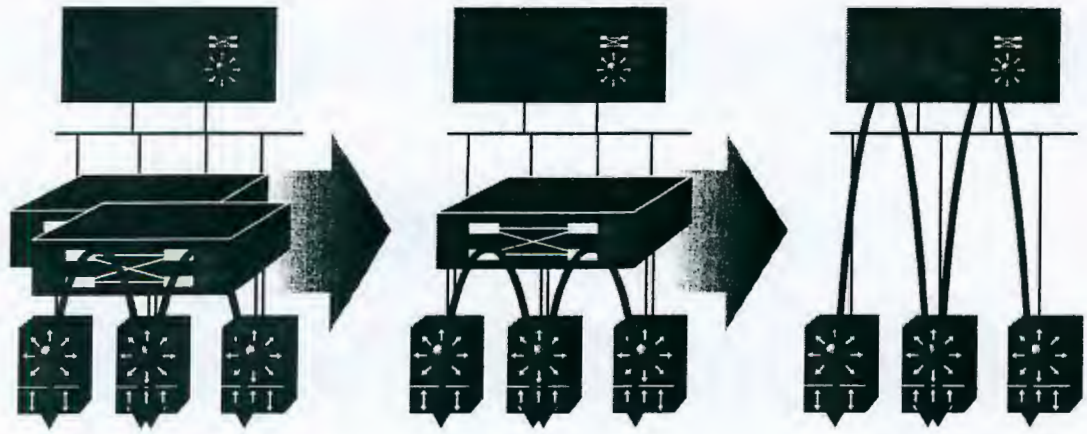
When deployed in Catalyst 6500 Series chassis (Catalyst 6506, 6509, 6513), the Supervisor Engine 2 in conjunction with the Switch Fabric Module (SFM, SFM2) can scale the total system bandwidth to 256 Gbps. When used in this configuration, the system will provide an added benefit of industry-leading network availability and resiliency (see Figure 5).

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 813
Doc: 3702

Cisco Systems, Inc.
All contents are Copyright © 1992–2001 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

16.973

Figure 5 2 Levels of Backplane Redundancy



- Each module interfaces both 256 Fabrics (active)
- Modules also interface with 32 Gbps passive Bus

- If primary fabric fails, modules defer to redundant fabric
- Modular fabric design allows upgrade of failed fabric

- If both fabrics fail, modules defer to passive 32 Gbps Bus
- **Connectivity is NOT lost**

In addition to the scalability in performance and industry leading resilience, the Supervisor Engine 2 provides powerful security and QoS features (For more info on these features, please see under the Supervisor 2 + PFC 2 section of this document). The QoS mechanisms on the PFC2 provide classification and scheduling to ensure that proper quality of service is delivered throughout the network. These features are important because the links in the distribution and core maintain a high utilization as they aggregate traffic from the lower layers. It is on these links that prioritization of traffic is important - so that high priority traffic will transit the core/distribution with low delay and latency.

Figure 6 Supervisor 1A with PFC and Multilayer Switch Feature Card 2 (MSFC2)

Cisco Systems, Inc.
All contents are Copyright © 1992–2001 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 814
3702
Doc

16.972
2

The functionality of the Supervisor Engines 1A and 2 is significantly enhanced by the addition of the Multilayer Switch Feature Card 2 (MSFC2) module option to meet the needs of the networks in the core and the distribution layer.

The MSFC2 daughter module when used with the PFC (PFC, PFC2) enabled Supervisor Engines 1A and 2 provides intelligent high performance multilayer switching up to 15 and 210 Mpps, respectively. MSFC2 provides a wide range of software services to enable scalable, end-to-end multicast traffic, security, and extra QoS mechanisms in addition to those provided by the PFC. For example, the MSFC2 provides support for the Protocol Independent Multicast (PIM) routing protocol, including PIM sparse, dense, sparse/dense modes, as well as granular security ACLs. MSFC2 also supports up to 1000 terminated virtual LANs (VLANs). In addition, MSFC2 will enable features like unicast Reverse path Forwarding (RPF) and TCP intercept in hardware on Catalyst 6500 Series switches configured with Supervisor Engine 2.

The MSFC2 enabled Catalyst 6500 Series Supervisor Engines 1&2 will provide the following benefits:

- Scalability: Supervisor Engine 2, when used in combination with the Switch Fabric Modules (SFM, SFM2) and Distributed Forwarding Cards (DFCs), enables the distributed forwarding architecture that scales the aggregate forwarding performance up to 210 Mpps.
- Fast convergence: In the backbone, the ability to recover from route failures and to route around them is of paramount importance. The MSFC2 addresses this need for immediate convergence by responding to routing topology changes and performing hardware-assisted invalidation of flow entries.
- Security: An important attribute of classical routing in a network is the ability to set up access lists to filter or altogether prevent traffic between hosts on different subnets. The MSFC2 is able to enforce multiple levels of security on every packet of the flow at wire speed. Because the MSFC2 parses the packet up to the transport layer, it enables access lists to be validated. By providing multiple levels of security, the MSFC2 enables users to set up rules and control traffic based on IP addresses as well as transport-layer application port numbers.
- Accounting and traffic management: A key requirement when deploying Layer 3 switching is to provide visibility of flows as they are switched for troubleshooting, traffic management, and accounting purposes. The MSFC2 and the PFC enable detailed data collection of flow statistics maintained in hardware, with no impact on switching performance. The records for expired flows are grouped together and exported to applications such as Netsys for network and Remote Monitoring II (RMON II) traffic management and monitoring, as well as to accounting applications.

This ability of the MSFC2 to enable full-featured multilayer switching and services at line-rate speeds is very important in the distribution and backbone applications in the enterprise and service provider networks. An example is the Policy Routing feature. Policy Based Routing is a flexible mechanism whereby routing decisions are based on more information than just the destination address. For instance, a service provider might enable policy routing to allow certain packets to be routed a different way other than using the typical shortest-path route. Some possible applications for policy routing are to provide equal access, protocol-sensitive routing, source-sensitive routing, routing based on interactive versus batch traffic, or routing based on dedicated links.

Summary

Enterprise networks continue to evolve to meet the demands of new networked applications, the bandwidth they consume, and the intelligent network services they require to enforce fairness and security. Network managers must deploy an infrastructure capable of not only supporting current requirements for bandwidth and network services, but also one capable of easily scaling to meet future requirements. This must be accomplished with an easy, seamless migration toward higher-speed Internet access services. The Catalyst 6500 Series supervisor engines provide the required seamless bandwidth scalability with tightly coupled network services, while also uniquely providing a bridge between existing LAN/WAN networks and legacy voice networks to future high-speed converged networks.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 815
3702
Doc:

All contents are Copyright © 1992–2001 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

IE-971
2

Ordering Information

Product Description	Product ID
Supervisor 1A	WS-X6K-SUP1A-2GE
Supervisor 1A + PFC	WS-X6K-SUP1A-PFC
Supervisor 2 + PFC2	WS-X6K-S2-PFC2
Supervisor 1A + PFC + MSFC2	WS-X6K-SUP1A-MSFC2
Supervisor 2 + PFC2 + MSFC2	WS-X6K-S2-MSFC2
Supervisor 2 + PFC2 + MSFC2 with 256 MB DRAM on the Supervisor and MSFC2	WS-X6K-S2U-MSFC2

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems Europe
11, Rue Camille Desmoulins
92782 Issy-les-Moulineaux
Cedex 9
France
www-europe.cisco.com
Tel: 33 1 58 04 60 00
Fax: 33 1 58 04 61 00

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems Australia, Pty., Ltd
Level 9, 80 Pacific Highway
P.O. Box 469
North Sydney
NSW 2060 Australia
www.cisco.com
Tel: +61 2 8448 7100
Fax: +61 2 9957 4350

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the

Cisco Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia
Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru
Philippines • Poland • Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa
Spain • Sweden • Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Copyright © 2001, Cisco Systems, Inc. All rights reserved. Printed in the USA. Catalyst, Cisco, Cisco IOS, Cisco Systems, and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0106R)

10/01 LW2657

RSC 1003/2005 - CN -
CPMI - CORREIOS
Fls. Nº 816
3702
Doc:

ANEXO (28)

16.970

Catalyst 6500 Series Distributed Forwarding Card (DFC)/DFC3A Installation Note

Product numbers:
WS-F6K-DFC(=)
WS-F6K-DFC3A(=)

This publication contains the procedure for installing the Catalyst 6500 series Distributed Forwarding Card (DFC) and DFC3A on Catalyst 6500 series fabric-enabled modules.

Note You install the DFC or DFC3A only on fabric-enabled modules. See the "Requirements" section on page 2 for more information.

Contents

This publication contains these sections:

- Overview, page 2
- Requirements, page 2
- Safety Overview, page 4
- Required Tools, page 8
- Installing the DFC or DFC3A, page 8
- Related Documentation, page 15
- Obtaining Documentation, page 15
- Obtaining Technical Assistance, page 16
- Obtaining Additional Publications and Information, page 18

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

Copyright © 2000–2003 Cisco Systems, Inc. All rights reserved.

RQS nº 03/2005 - CN - CPMI - CORREIOS
817
Fls Nº
3702
Doc:

16 969

Overview

The DFC and DFC3A on fabric-enabled switching modules provide Layer 2 and Layer 3 routing and forwarding capabilities locally on each module and provides Layer 3 switching with distributed Cisco Express Forwarding (dCEF). The DFC3A adds Multiprotocol Label Switching (MPLS), NAT, and Layer 4 services.

The DFC ships with 128-MB SDRAM at 100 MHz with Error Checking and Correction (ECC) (single-bit error detection and correction; 2-bit error detection) and is upgradeable to 256 MB with ECC or 512 MB with ECC.

The DFC3 ships with 512-MB double data rate (DDR) SDRAM at 100 MHz with ECC.

Requirements

The requirements for using the DFC or DFC3A are as follows:

- DFC Requirements, page 2
- DFC3A Requirements, page 3

DFC Requirements

To install and use the DFC, you need the following:

- Catalyst 6500 series switch (Catalyst 6506, 6509, 6509-NEB, or 6513) or Cisco 7600 series Internet Router (Cisco 7606, 7609, or 7613)
- Supervisor Engine 2 with Multilayer Switch Feature Card 2 (MSFC2) running Cisco IOS software on the Supervisor Engine 2 and MSFC2

Note You cannot have a DFC in a system with a Supervisor Engine 720.

- Fabric-enabled module

RQS nº 03/2005 - CN - CPMI - CORREIOS
78-11627-02 | 818
Fls Nº
Doc: 3702

16.968
L

- Switch Fabric Module (SFM) (WS-C6500-SFM) or SFM 2 (WS-X6500-SFM2)

Note The SFM must be installed in slot 5 or slot 6 of the 6-slot or the 9-slot chassis. The SFM cannot be installed in the 3-slot or 13-slot chassis.

Note The SFM 2 must be installed in slot 5 or slot 6 of the 6-slot or the 9-slot chassis, or in slot 7 or slot 8 of the 13-slot chassis.

DFC3A Requirements

To install and use the DFC3A, you need the following:

- Catalyst 6500 series switch (Catalyst 6503, 6506, 6509, 6509-NEB, or 6513) or Cisco 7600 series Internet Router (Cisco 7603, 7606, 7609, or 7613)
- Supervisor Engine 720 with MSFC3 running Cisco IOS software on the Supervisor Engine 720 and MSFC3

Note You cannot have a DFC3A in a system with a Supervisor Engine 2.

- Fabric-enabled module

Note Supervisor Engine 720 supports a DFC3 on these WS-X6516-GBIC hardware revisions:

- Lower than 5.0
- 5.4 and higher

Supervisor Engine 720 does not support a DFC3 on WS-X6516-GBIC hardware revisions 5.0 through 5.3. With a Supervisor Engine 720 and with a DFC3 installed, WS-X6516-GBIC hardware revisions 5.0 through 5.3 do not power up.

Without a DFC3, WS-X6516-GBIC hardware revisions 5.0 through 5.3 operate in bus mode.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 819
3702
Doc.

16.967
L

Safety Overview

Safety warnings appear throughout this publication in procedures that, if performed incorrectly, may harm you. A warning symbol precedes each warning statement.

Warning **IMPORTANT SAFETY INSTRUCTIONS**

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. To see translations of the warnings that appear in this publication, refer to the translated safety warnings that accompanied this device.

Note: SAVE THESE INSTRUCTIONS

Note: This documentation is to be used in conjunction with the specific product installation guide that shipped with the product. Please refer to the Installation Guide, Configuration Guide, or other enclosed additional documentation for further details.

Waarschuwing **BELANGRIJKE VEILIGHEIDSINSTRUCTIES**

Dit waarschuwingssymbool betekent gevaar. U verkeert in een situatie die lichamelijk letsel kan veroorzaken. Voordat u aan enige apparatuur gaat werken, dient u zich bewust te zijn van de bij elektrische schakelingen betrokken risico's en dient u op de hoogte te zijn van de standaard praktijken om ongelukken te voorkomen. Voor een vertaling van de waarschuwingen die in deze publicatie verschijnen, dient u de vertaalde veiligheidswaarschuwingen te raadplegen die bij dit apparaat worden geleverd.

Opmerking BEWAAR DEZE INSTRUCTIES.

Opmerking Deze documentatie dient gebruikt te worden in combinatie met de installatiehandleiding voor het specifieke product die bij het product wordt geleverd. Raadpleeg de installatiehandleiding, configuratiehandleiding of andere verdere ingesloten documentatie voor meer informatie.

Varoitus **TÄRKEITÄ TURVALLISUUTEEN LIITTYVIÄ OHJEITA**

Tämä varoitusmerkki merkitsee vaaraa. Olet tilanteessa, joka voi johtaa ruumiinvammaan. Ennen kuin työskentelet minkään laitteiston parissa, ota selvää sähkökytkentöihin liittyvistä vaaroista ja tavanomaisista onnettomuuksien ehkäisykeinoista. Tässä asiakirjassa esitettyjen varoitusten käännökset löydät laitteen mukana toimitetuista ohjeista.

Huomautus SÄILYTÄ NÄMÄ OHJEET

Huomautus Tämä asiakirja on tarkoitettu käytettäväksi yhdessä tuotteen mukana tulleen asennusoppaan kanssa. Katso lisätietoja asennusoppaasta, kokoonpano-oppaasta ja muista mukana toimitetuista asiakirjoista.

RQS nº 03/2005 - CN - CPMI - CORREIOS
78-11627-02
Fls. Nº 820
3702
Doc:

Attention **IMPORTANTES INFORMATIONS DE SÉCURITÉ**

Ce symbole d'avertissement indique un danger. Vous vous trouvez dans une situation pouvant causer des blessures ou des dommages corporels. Avant de travailler sur un équipement, soyez conscient des dangers posés par les circuits électriques et familiarisez-vous avec les procédures couramment utilisées pour éviter les accidents. Pour prendre connaissance des traductions d'avertissements figurant dans cette publication, consultez les consignes de sécurité traduites qui accompagnent cet appareil.

Remarque CONSERVEZ CES INFORMATIONS

Remarque Cette documentation doit être utilisée avec le guide spécifique d'installation du produit qui accompagne ce dernier. Veuillez vous reporter au Guide d'installation, au Guide de configuration, ou à toute autre documentation jointe pour de plus amples renseignements.

Warnung **WICHTIGE SICHERHEITSANWEISUNGEN**

Dieses Warnsymbol bedeutet Gefahr. Sie befinden sich in einer Situation, die zu einer Körperverletzung führen könnte. Bevor Sie mit der Arbeit an irgendeinem Gerät beginnen, seien Sie sich der mit elektrischen Stromkreisen verbundenen Gefahren und der Standardpraktiken zur Vermeidung von Unfällen bewusst. Übersetzungen der in dieser Veröffentlichung enthaltenen Warnhinweise sind im Lieferumfang des Geräts enthalten.

Hinweis BEWAHREN SIE DIESE SICHERHEITSANWEISUNGEN AUF

Hinweis Dieses Handbuch ist zum Gebrauch in Verbindung mit dem Installationshandbuch für Ihr Gerät bestimmt, das dem Gerät beiliegt. Entnehmen Sie bitte alle weiteren Informationen dem Handbuch (Installations- oder Konfigurationshandbuch o. Ä.) für Ihr spezifisches Gerät.

Figyelem! **FONTOS BIZTONSÁGI ELŐÍRÁSOK**

Ez a figyelmezető jel veszélyre utal. Sérülésveszélyt rejtő helyzetben van. Mielőtt bármely berendezésen munkát végezte, legyen figyelemmel az elektromos áramkörök okozta kockázatokra, és ismerkedjen meg a szokásos balesetvédelmi eljárásokkal. A kiadványban szereplő figyelmeztetések fordítása a készülékhez mellékelt biztonsági figyelmeztetések között található.

Megjegyzés ŐRIZZE MEG EZEKET AZ UTASÍTÁSOKAT!

Megjegyzés Ezt a dokumentációt a készülékhez mellékelt üzembe helyezési útmutatóval együtt kell használni. További tudnivalók a mellékelt Üzembe helyezési útmutatóban (Installation Guide), Konfigurációs útmutatóban (Configuration Guide) vagy más dokumentumban találhatók.

Avvertenza **IMPORTANTI ISTRUZIONI SULLA SICUREZZA**

Questo simbolo di avvertenza indica un pericolo. La situazione potrebbe causare infortuni alle persone. Prima di intervenire su qualsiasi apparecchiatura, occorre essere al corrente dei pericoli relativi ai circuiti elettrici e conoscere le procedure standard per la prevenzione di incidenti. Per le traduzioni delle avvertenze riportate in questo documento, vedere le avvertenze di sicurezza che accompagnano questo dispositivo.

Nota CONSERVARE QUESTE ISTRUZIONI

Nota La presente documentazione va usata congiuntamente alla guida di installazione specifica spedita con il prodotto. Per maggiori informazioni, consultare la Guida all'installazione, la Guida alla configurazione o altra documentazione acclusa.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 821
3702

Advarsel **VIKTIGE SIKKERHETSINSTRUKSJONER**

Dette varselssymbolet betyr fare. Du befinner deg i en situasjon som kan forårsake personskade. Før du utfører arbeid med utstyret, bør du være oppmerksom på farene som er forbundet med elektriske kretssystemer, og du bør være kjent med vanlig praksis for å unngå ulykker. For å se oversettelser av advarslene i denne publikasjonen, se de oversatte sikkerhetsvarslene som følger med denne enheten.

Merk TA VARE PÅ DISSE INSTRUKSJONENE

Merk Denne dokumentasjonen skal brukes i forbindelse med den spesifikke installasjonsveiledningen som fulgte med produktet. Vennligst se installasjonsveiledningen, konfigureringsveiledningen eller annen vedlagt tilleggsdokumentasjon for detaljer.

Aviso **INSTRUÇÕES IMPORTANTES DE SEGURANÇA**

Este símbolo de aviso significa perigo. O utilizador encontra-se numa situação que poderá ser causadora de lesões corporais. Antes de iniciar a utilização de qualquer equipamento, tenha em atenção os perigos envolvidos no manuseamento de circuitos eléctricos e familiarize-se com as práticas habituais de prevenção de acidentes. Para ver traduções dos avisos incluídos nesta publicação, consulte os avisos de segurança traduzidos que acompanham este dispositivo.

Nota GUARDE ESTAS INSTRUÇÕES

Nota Esta documentação destina-se a ser utilizada em conjunto com o manual de instalação incluído com o produto específico. Consulte o manual de instalação, o manual de configuração ou outra documentação adicional inclusa, para obter mais informações.

¡Advertencia! **INSTRUCCIONES IMPORTANTES DE SEGURIDAD**

Este símbolo de aviso indica peligro. Existe riesgo para su integridad física. Antes de manipular cualquier equipo, considere los riesgos de la corriente eléctrica y familiarícese con los procedimientos estándar de prevención de accidentes. Vea las traducciones de las advertencias que acompañan a este dispositivo.

Nota GUARDE ESTAS INSTRUCCIONES

Nota Esta documentación está pensada para ser utilizada con la guía de instalación del producto que lo acompaña. Si necesita más detalles, consulte la Guía de instalación, la Guía de configuración o cualquier documentación adicional adjunta.

Varning! **VIKTIGA SÄKERHETSANVISNINGAR**

Denna varningssignal signalerar fara. Du befinner dig i en situation som kan leda till personskada. Innan du utför arbete på någon utrustning måste du vara medveten om farorna med elkretsar och känna till vanliga förfaranden för att förebygga olyckor. Se översättningarna av de varningsmeddelanden som finns i denna publikation, och se de översatta säkerhetsvarningarna som medföljer denna anordning.

OBS! SPARA DESSA ANVISNINGAR

OBS! Denna dokumentation ska användas i samband med den specifika produktinstallationshandbok som medföljde produkten. Se installationshandboken, konfigurationshandboken eller annan bifogad ytterligare dokumentation för närmare detaljer.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
78-11627-02
Fls Nº 822
3702
Nº
Doc:

Предупреждение ВАЖНЫЕ СВЕДЕНИЯ ПО БЕЗОПАСНОСТИ

Этот символ предупреждает о наличии опасности. При неправильных действиях возможно получение травм. Перед началом работы с любым оборудованием необходимо ознакомиться с ситуациями, в которых возможно поражение электротоком, и со стандартными действиями для предотвращения несчастных случаев. Переведенный текст предупреждений содержится в соответствующем документе, поставляемом вместе с устройством.

Примечание СОХРАНЯЙТЕ ЭТУ ИНСТРУКЦИЮ
Примечание Эта инструкция должна использоваться вместе с руководством по установке конкретного изделия, входящим в комплект поставки. Дополнительные сведения см. в руководстве по установке, руководстве по настройке и другой документации, поставляемой с изделием.

警告 有关安全的重要说明

这个警告符号指有危险·您所处的环境可能使身体受伤·操作设备前必须意识到电流的危险性·务必熟悉操作标准·以防发生事故·如果需要了解本说明中出现的警告符号的译文·请参阅本装置所附之安全警告译文·

注意 保存这些说明
注意 本文件应与本产品附带的具体安装说明一并阅读·如欲了解详情·请参阅《安装说明》、《配置说明》或所附的其他文件·

警告 安全上の重要な注意事項

「危険」の意味です。人身事故を予防するための注意事項が記述されています。装置の取り扱い作業を行うときは、電気回路の危険性に注意し、一般的な事故防止対策に留意してください。このマニュアルに記載されている警告の各国語版は、装置に付属の「Translated Safety Warnings」を参照してください。

注 これらの注意事項を保管しておいてください。
注 この資料は、製品に付属のインストレーション ガイドと併用してください。詳細は、インストレーション ガイド、コンフィギュレーション ガイド、または添付されているその他のマニュアルを参照してください。

Warning **Only trained and qualified personnel should be allowed to install, replace, or service this equipment.**

RQS nº 03/2005 - CN -
CPMI - CORREIOS
825
Fls Nº
Doc 3702

16-963

Required Tools

These tools are required to install the Catalyst 6500 series DFC or DFC3A:

- Antistatic mat or foam pad to support the removed module
- Number 1 Phillips screwdriver for the screws and cap nuts that fasten the DFC to the module
- Your own ESD-prevention equipment or the disposable grounding wrist strap included with all upgrade kits, field-replaceable units (FRUs), and spares

Whenever you handle a module, always use a wrist strap or other grounding device to prevent electrostatic discharge (ESD). For information on preventing ESD, refer to the "Preventing ESD" section of the *Site Preparation and Safety Guide*.

stalling the DFC or DFC3A

Note In this section, the term "DFC" refers to the DFC and DFC3A.

Note The figures in this procedure show the DFC. The procedure is the same for the DFC and DFC3A.

To install the DFC on a fabric-enabled module, follow these steps:

Caution During this procedure, wear grounding wrist straps to avoid ESD damage to the card. Do not directly touch the backplane with your hand or any metal tool, or you could shock yourself.

Step 1 Remove the module from the Catalyst 6500 series switch. (Refer to the *Catalyst 6500 Series Module Installation Guide* for removal instructions.)

Step 2 Place the module on an antistatic mat or foam, with the front of the module facing toward you (see Figure 2).

Step 3 Remove the DFC from its antistatic bag.

Step 4 Align the two mounting holes on the DFC (see Figure 1) with the two male standoffs on the module (see Figure 2). Make sure that the remaining mounting holes on the DFC are aligned with the remaining standoffs.

Note The DFC is designed to be installed on different modules; therefore, there may be more mounting holes on the DFC than there are standoffs on the module. Not all mounting holes on the DFC will be used in all installations. Visually verify that there are standoffs beneath the mounting holes before installing the securing screws.

ROS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 824
Doc: 3702

16.962

Figure 1 Mounting Holes on the DFC

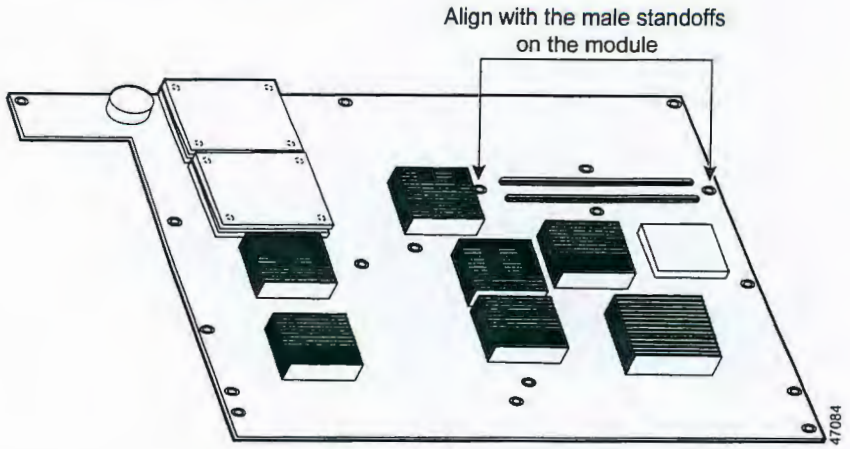
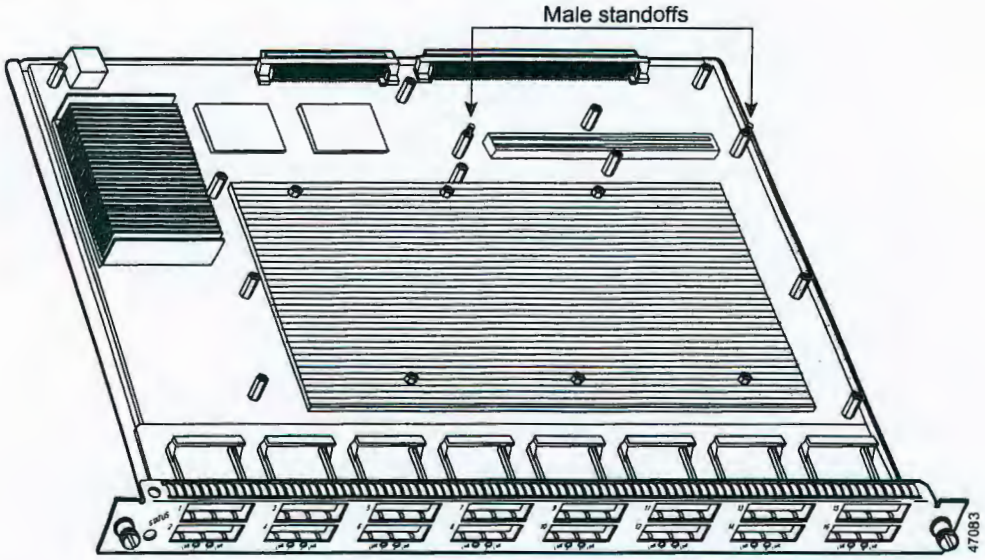


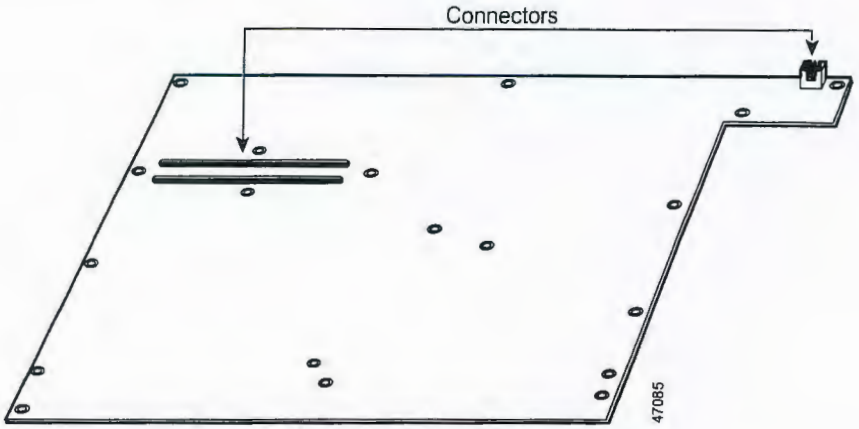
Figure 2 Male Standoff Locations on the Module



Step 5 Ensure that the connectors on the DFC are aligned with the connectors on the module. Figure 3 shows the connectors on the underside of the DFC.

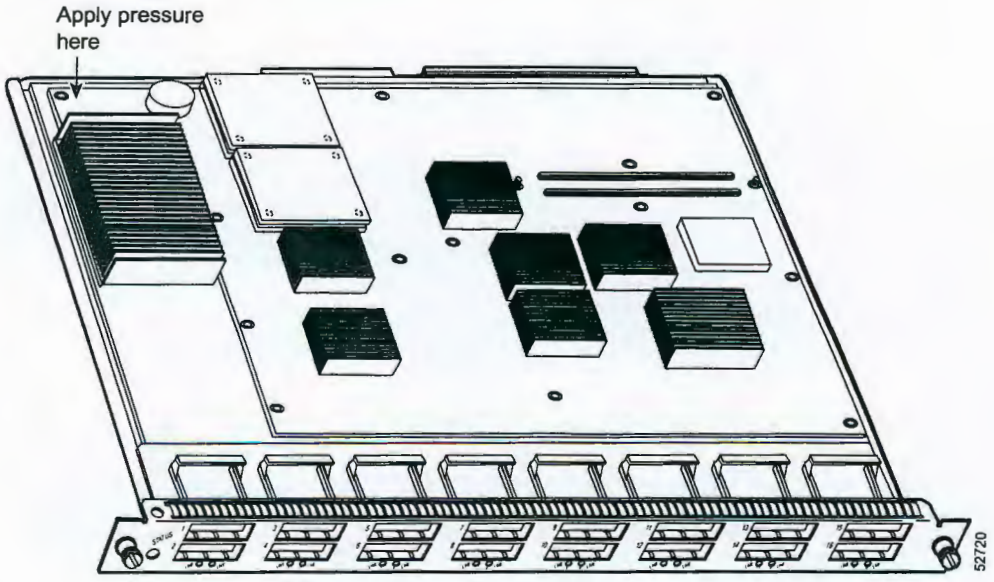
RQS nº 03/2005 - CN -
CPMI - CORREIOS
825
Fls Nº 9
3702

Figure 3 Distributed Forwarding Card Connectors



Step 6 Apply pressure to the area shown in Figure 4 to seat the power connector.

Figure 4 Seating the Power Connector



Note The following step shows how to preseat the DFC on the module. Preseating the DFC allows you to verify that the keys on the connectors are properly aligned. Fully seating the DFC when the connectors are not aligned will damage the connectors on both the DFC and the module. If you damage a connector, you will have to return the module to Cisco for repair. It is important that the DFC is preseated prior to being fully seated.

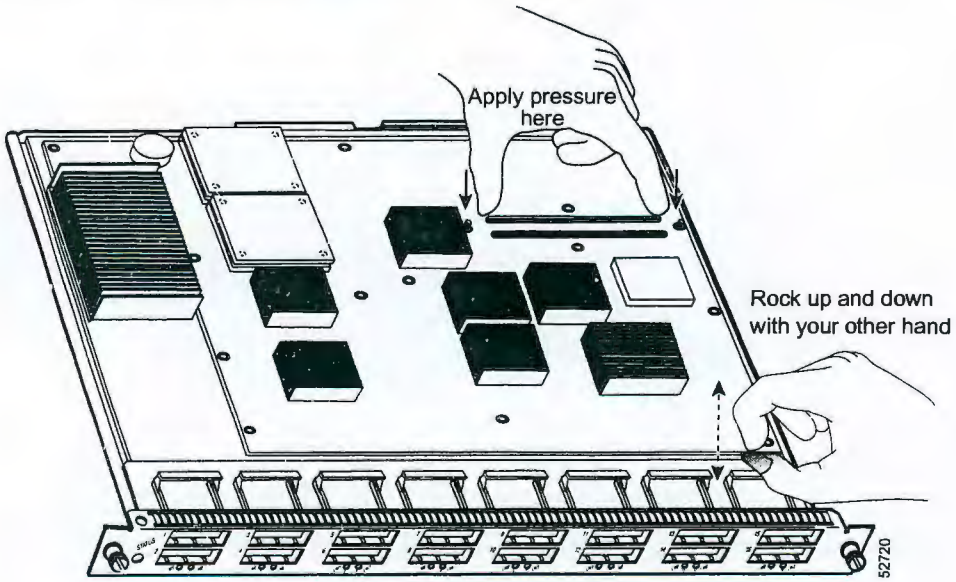
RQS nº 03/2005 - CN - CPMI - CORREIOS
826
Fls Nº
78-11627-02
Doc: 3702

16.960

Caution Use care not to damage the connectors on the module. If you damage a connector, you will have to return the module to Cisco for repair.

Step 7 With your left hand, apply firm pressure at the location shown in Figure 5. While applying pressure with your left hand, rock the DFC up and down with your right hand, no more than half an inch in either direction, to preseat the DFC on the module.

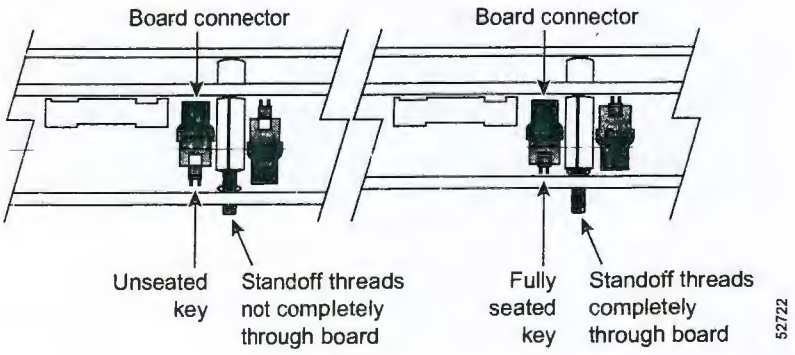
Figure 5 Preseating the Connector



Step 8 Verify that the keys on the connector are aligned and that the gap between the key and the opposing connector is no more than 1/16 inch (1.6 mm) before fully seating the module (see Figure 6):

- If the keys are not aligned, remove the DFC and repeat Step 4 through Step 7.
- If the keys are not seated far enough, repeat Step 7.

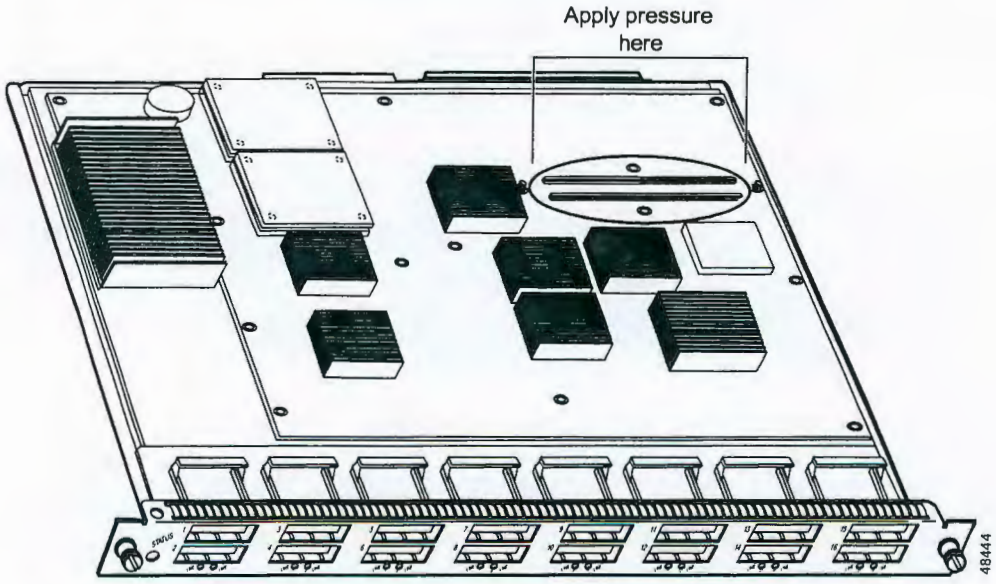
Figure 6 Connector Keys



RQS nº 03/2005 - CN - CPMI - CORREIOS
827
Fls Nº 11
3702

Step 9 With the heel of your hand, apply firm pressure to the location shown in Figure 7 to fully seat the DFC on the module.

Figure 7 Seating the Distributed Forwarding Card on the Module



Note The DFC is fully seated when there is no gap between the connector keys, and the bottom of the DFC is in contact with the tops of the standoffs (see Figure 6).

Caution Using the screws to seat the DFC could warp the card. *Before* you install and tighten the securing screws, ensure that the DFC is fully seated by visually verifying that there is no gap between the male and female keys on the connectors and that the bottom of the DFC is in contact with the tops of the standoffs (see Figure 6).

Step 10 Use a Phillips-head screwdriver to install the two screws at the front of the DFC and the one screw at the power connector in the order shown in Figure 8.

Note You should visually verify that there are standoffs beneath the mounting holes before installing the securing screws.

RQS nº 03/2005 - CN - CPMI - CORREIOS
78-11627-02 828
Fls Nº
Doc 3702

Documentation

Nº 958

Table of Contents

Product Overview
Catalyst 6503 Switch
Catalyst 6506 Switch
Catalyst 6509 Switch
Catalyst 6509-NEB Switch
Catalyst 6513 Switch
System Features

- Port Density
- Redundancy
- Component Hot Swapping

Fan Assembly
Power Supplies

- 950 W Power Supply (PWR-950-AC and PWR-950-DC)
- 1000 W, 1300 W, 2500 W, and 4000 W Power Supplies
- Power Supply Redundancy
- Environmental Monitoring of the Power Supply
- Power Supply Fan Assembly

Product Overview

This chapter describes the Catalyst 6500 series switches and contains these sections:

- Catalyst 6503 Switch
- Catalyst 6506 Switch
- Catalyst 6509 Switch
- Catalyst 6509-NEB Switch
- Catalyst 6513 Switch
- System Features
- Fan Assembly
- Power Supplies

The Catalyst 6500 series switch chassis are listed in Table 1-1.

Table 1-1 Catalyst 6500 Series Switches

Catalyst 6500 Series Switch	Orientation/Number of Slots
Catalyst 6503	Horizontal 3-slot

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 829
Nº Doc 3702

16.957

Catalyst 6506	Horizontal 6-slot
Catalyst 6509	Horizontal 9-slot
Catalyst 6509-NEB	Vertical 9-slot
Catalyst 6513	Horizontal 13-slot

Note In this publication, the term Catalyst 6500 series refers only to the switch chassis listed in Table 1-2. The Catalyst 6000 series switches (Catalyst 6006 switch and Catalyst 6009 switch) are described in a separate publication, the Catalyst 6000 Series Switches Installation Guide.

Note Throughout this publication, except where noted, the term supervisor engine is used to refer to Supervisor Engine 1, Supervisor Engine 2, and Supervisor Engine 720.

Catalyst 6503 Switch

The Catalyst 6503 switch is a 3-slot horizontally-aligned switch. The Catalyst 6503 switch supports the following:

- A supervisor engine with two gigabit interface uplinks and an optional redundant supervisor engine in one of the following configurations:
  - Two supervisor engines, each with no Multilayer Switch Feature Card (MSFC) and no Policy Feature Card (PFC)
  - Two supervisor engines, each configured with a PFC daughter card
  - Two supervisor engines, each configured with both an MSFC and a PFC daughter card

Note The uplink ports are fully functional on the redundant supervisor engine in standby mode.

Note Both supervisor engines in a single chassis must be completely identical.

- Up to two hot-swappable Catalyst 6500 series modules:
  - The Switch Fabric Modules (WS-C6500-SFM and WS-X6500-SFM2) are not supported on the Catalyst 6503 switch.
  - The WS-X6816-GBIC 16-port Gigabit Ethernet fabric-enabled module is not supported on the Catalyst 6503 switch.
- Backplane bandwidth of 32 Gbps
- Hot-swappable fan assembly
- Two power entry modules (PEMs)
- Redundant AC-input or DC-input power supplies (950W power supply only)

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 830
Doc: 3702

16.956

Figure 1-1 Catalyst 6503 Switch—Front View

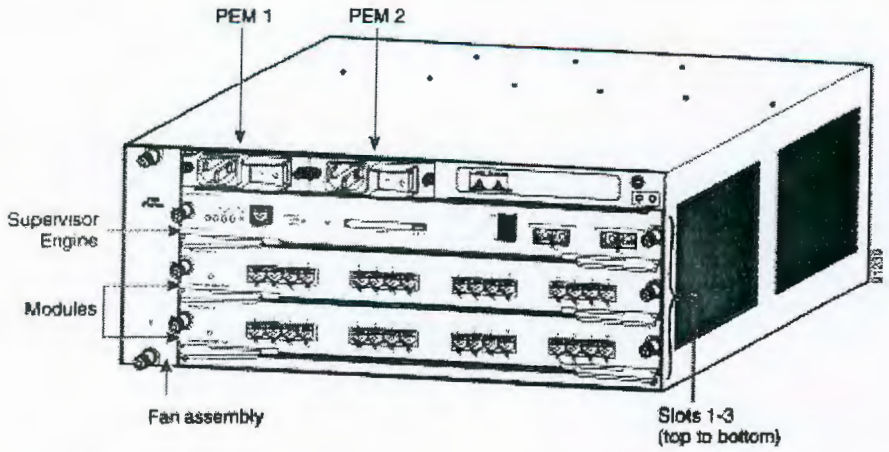
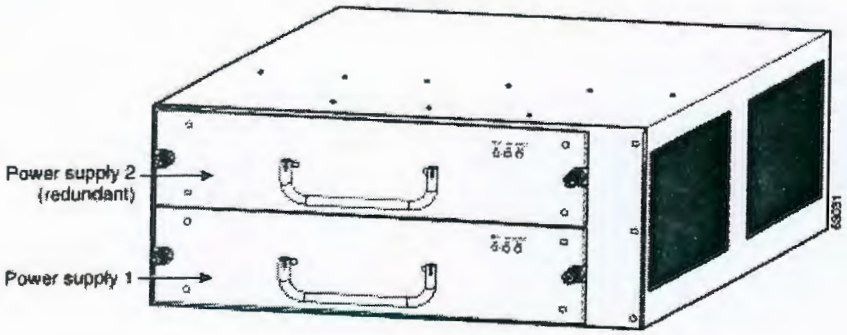


Figure 1-2 Catalyst 6503 Switch—Rear View



Catalyst 6506 Switch

The Catalyst 6506 switch chassis is a 6-slot horizontally-aligned chassis. The Catalyst 6506 switch supports the following:

- A supervisor engine with two Gigabit Ethernet uplink ports (slot 1)
- An optional redundant supervisor engine (slot 2)

Note Supervisor Engine 720 must be installed in chassis slots 5 or 6. Slots 1 and 2 are available for switching modules.

Note The uplink ports are fully functional on the redundant supervisor engine in standby mode.

Both supervisor engines in a single chassis must be completely identical. You can configure the redundant supervisor engines in a Catalyst 6506 switch in one of three configurations:

- Two supervisor engines, each with no Multilayer Switch Feature Card (MSFC) and no Policy Feature Card (PFC)

ECT - 03/2005 - CN - CPMI - CORREIOS
Fls Nº 831
3702
Doc:

16.955

- Two supervisor engines, each configured with a PFC daughter card
- Two supervisor engines, each configured with both an MSFC and a PFC daughter card

- Up to five additional hot-swappable Catalyst 6500 series switching modules
  - Fabric-enabled module support provided in slots 2-6 (requires Switch Fabric Module)

Note Supervisor Engine 720 has built-in switching fabric and does not require that Switch Fabric Modules be installed in the chassis.

- Hot-swappable fan tray

Note The high capacity fan tray (WS-C6K-6SLOT-FAN2) must be installed when a Supervisor Engine 720 is installed in the chassis.

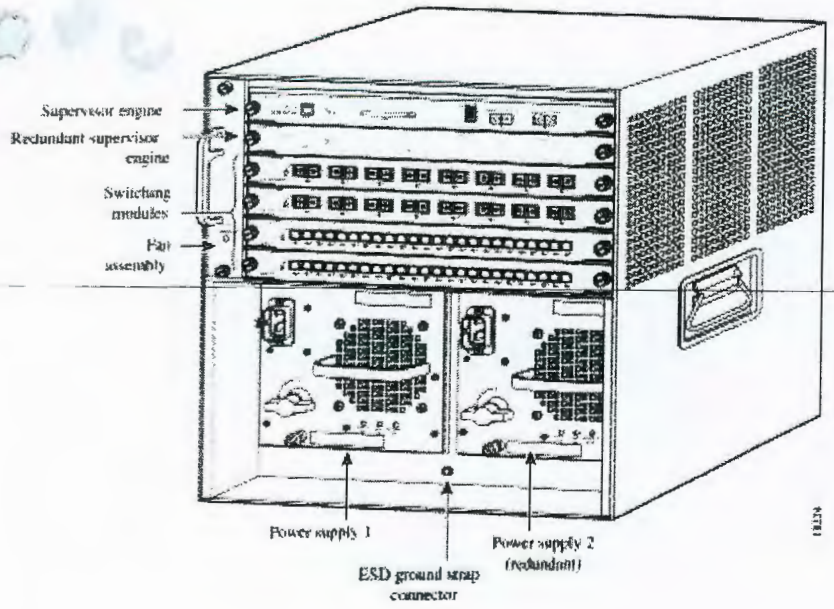
- Redundant AC-input or DC-input power supplies

Note When a Supervisor Engine 720 and the high capacity fan tray are installed, you must install 2500 W or higher capacity power supplies in the chassis.

- Backplane bandwidth of 32 Gbps scalable up to 256 Gbps

Note Backplane bandwidth greater than 32 Gbps requires that you install either a Switch Fabric Module or a Supervisor Engine 720 in the switch chassis.

Figure 1-3 Catalyst 6506 Switch



- A Switch Fabric Module (WS-C6500-SFM or WS-X6500-SFM2)
  - The Switch Fabric Module requires Supervisor Engine 2.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 832
3702

Note Switch Fabric Modules are not supported by Supervisor Engine 720.

- You must install a Switch Fabric Module in either slot 5 or slot 6 of the Catalyst 6506 switch. For redundancy, you can install a standby Switch Fabric Module. The module first installed functions as the primary module. When you install two Switch Fabric Modules at the same time, the module in slot 5 acts as the primary module, and the module in slot 6 acts as the backup. If you reset the module in slot 5, the module in slot 6 becomes the primary module.
- Mixing an SFM (WS-C6500-SFM) with an SFM2 (WS-X6500-SFM2) in the same Catalyst 6506, Catalyst 6509, or Catalyst 6509-NEB chassis is supported.
- Fabric-enabled module support is provided in all slots. (A Switch Fabric Module is required.)

Catalyst 6509 Switch

The Catalyst 6509 switch chassis has nine horizontal slots that are numbered from top to bottom. (See Figure 1-4.) Slot 1 is reserved for the supervisor engine, which provides switching, local and remote management, and multiple gigabit uplink interfaces.

Slot 2 can contain an additional supervisor engine, which can act as a backup if the first supervisor engine fails. If a redundant supervisor engine is not required, slot 2 is available for a switching module.

For a detailed description of supervisor engine operation in a redundant configuration, refer to your software configuration guide.

The Catalyst 6509 switch supports the following:

- A supervisor engine with two Gigabit Ethernet uplink ports and an optional redundant supervisor engine

Note Supervisor Engine 720 must be installed in chassis slots 5 or 6. Slots 1 and 2 are available for switching modules.

Note The uplink ports are fully functional on a redundant supervisor engine in standby mode.

Both supervisor engines in a single chassis must be completely identical. You can configure the redundant supervisor engines in a Catalyst 6500 series switch in one of three configurations:

- Two supervisor engines, each with no MSFC and no PFC
- Two supervisor engines, each configured with a PFC daughter card
- Two supervisor engines, each configured with both an MSFC and a PFC daughter card

- Backplane bandwidth scalable up to 256 Gbps

Note Backplane bandwidth greater than 32 Gbps requires that you install a Switch

ECT/ROS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 833
Doc: 3702

Fabric Module or a Supervisor Engine 720 in the Catalyst 6509-NEB switch chassis.

16-953
2

- A Switch Fabric Module (WS-C6500-SFM or WS-X6500-SFM2)
  - The Switch Fabric Modules require Supervisor Engine 2.
  - You must install the Switch Fabric Module in either slot 5 or slot 6 of the Catalyst 6509-NEB switch. For redundancy, you can install a standby Switch Fabric Module. The module first installed functions as the primary module. When you install two Switch Fabric Modules at the same time, the module in slot 5 acts as the primary module, and the module in slot 6 acts as the backup. If you reset the module in slot 5, the module in slot 6 becomes the primary module.
  - Mixing an SFM (WS-C6500-SFM) with an SFM2 (WS-X6500-SFM2) in the same Catalyst 6506, Catalyst 6509, or Catalyst 6509-NEB chassis is supported.

Note Supervisor Engine 720 has built-in switching fabric and does not require that Switch Fabric Modules be installed in the chassis.

- Up to eight additional Catalyst 6500 series modules
  - Fabric-enabled module support provided in all slots (requires Switch Fabric Module)
- Hot-swappable fan assembly

Note The high capacity fan tray (WS-C6K-9SLOT-FAN2) must be installed when a Supervisor Engine 720 is installed in the chassis.

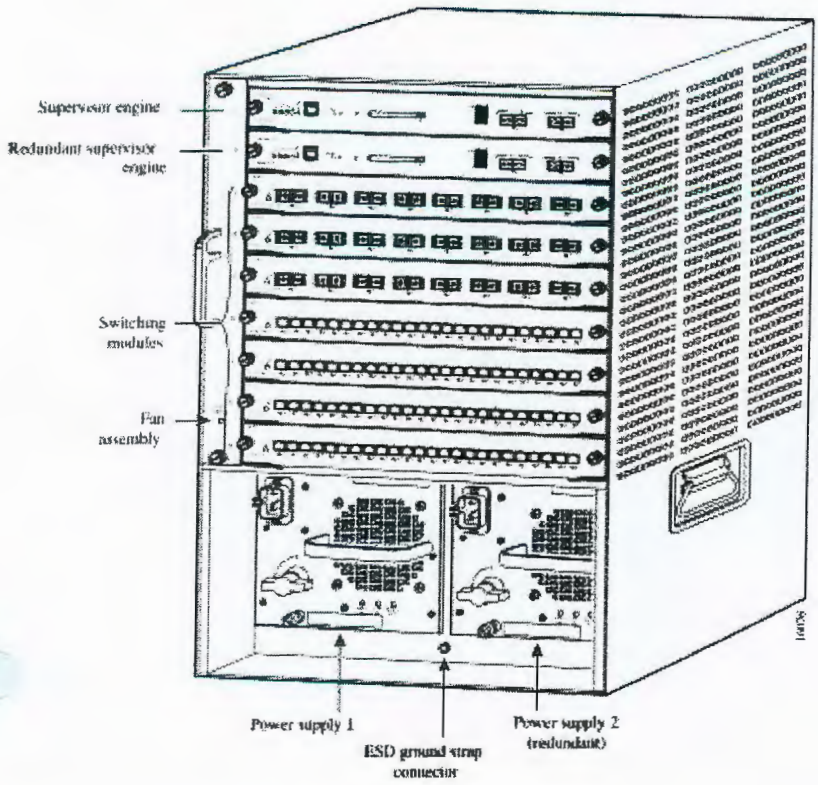
- Redundant AC-input or DC-input power supplies

Note When a Supervisor Engine 720 and the high capacity fan tray are installed, you must install 2500 W or higher capacity power supplies in the chassis.

Figure 1-4 Catalyst 6509 Switch

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 834
3702
Doc:

16.952



Catalyst 6509-NEB Switch

The Catalyst 6509-NEB switch chassis has nine vertical slots that are numbered from right to left. (See Figure 1-5.) Slot 1 is reserved for the supervisor engine, which provides switching, local and remote management, and multiple gigabit uplink interfaces.

Slot 2 can contain an additional supervisor engine, which can act as a backup if the first supervisor engine fails. If a redundant supervisor engine is not required, slot 2 is available for a switching module.

For a detailed description of supervisor engine operation in a redundant configuration, refer to your software configuration guide.

The Catalyst 6509-NEB switch supports the following:

- A supervisor engine with two Gigabit Ethernet uplink ports and an optional redundant supervisor engine

Note Supervisor Engine 720 must be installed in slots 5 or 6. Slots 1 and 2 are available for switching modules.

Note The uplink ports are fully functional on the redundant supervisor engine in standby mode.

Both supervisor engines in a single chassis must be completely identical. You can configure the redundant supervisor engines in a Catalyst 6500 series switch in one of three configurations:

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 835
3702

16.951
L

- Two supervisor engines, each with no MSFC and no PFC
- Two supervisor engines, each configured with a PFC daughter card
- Two supervisor engines, each configured with both an MSFC and a PFC daughter card

- Backplane bandwidth scalable up to 256 Gbps

Note Backplane bandwidth greater than 32 Gbps requires that you install either a Switch Fabric Module or a Supervisor Engine 720 in the Catalyst 6509-NEB switch chassis.

- A Switch Fabric Module (WS-C6500-SFM or WS-X6500-SFM2)
  - The Switch Fabric Modules require Supervisor Engine 2.
  - You must install the Switch Fabric Module in either slot 5 or slot 6 of the Catalyst 6509-NEB switch. For redundancy, you can install a standby Switch Fabric Module. The module first installed functions as the primary module. When you install two Switch Fabric Modules at the same time, the module in slot 5 acts as the primary module, and the module in slot 6 acts as the backup. If you reset the module in slot 5, the module in slot 6 becomes the primary module.
  - Mixing an SFM (WS-C6500-SFM) with an SFM2 (WS-X6500-SFM2) in the same Catalyst 6506, Catalyst 6509, or Catalyst 6509-NEB chassis is supported.

Note The Supervisor Engine has built-in switching fabric and does not require that Switch Fabric Modules be installed in the chassis.

- Up to eight additional Catalyst 6500 series hot-swappable modules
  - Fabric-enabled module support provided in all slots (requires Switch Fabric Module or Supervisor Engine 720)
- Hot-swappable fan assembly

Note The high capacity fan tray (WS-C6509-NEB-FAN2) must be installed when a Supervisor Engine 720 is installed in the chassis.

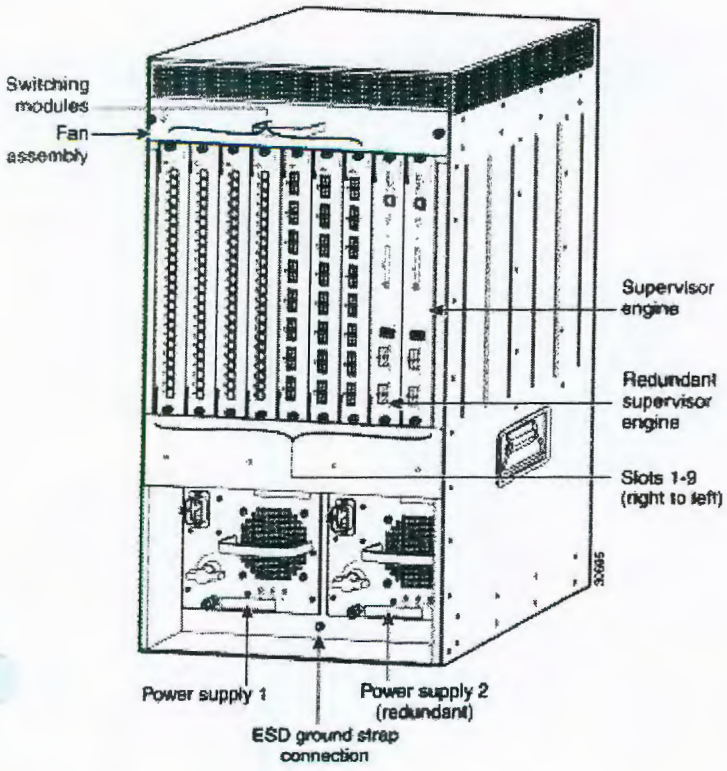
- Redundant AC-input or DC-input power supplies

Note When a Supervisor Engine 720 and the high capacity fan tray are installed, you must install 2500 W or larger capacity power supplies in the chassis.

Figure 1-5 Catalyst 6509-NEB Switch

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 836
Doc: 702

16.950
L



Catalyst 6513 Switch

The Catalyst 6513 switch chassis has 13 slots. (See Figure 1-6.) Slot 1 is reserved for a Supervisor Engine 2, which provides switching, local and remote management, and multiple gigabit uplink interfaces.

Note The Catalyst 6513 switch requires a Supervisor Engine 2 or Supervisor Engine 720.

Slot 2 can contain an additional Supervisor Engine 2, which can act as a backup if the first supervisor engine fails. If a redundant supervisor engine is not required, slot 2 is available for a witching module.

Note Supervisor Engine 720 must be installed in slots 7 or 8.

For a detailed description of supervisor engine operation in a redundant configuration, refer to your software configuration guide

The Catalyst 6513 switch supports the following:

- A Supervisor Engine 2 with two Gigabit Ethernet uplink ports and an optional redundant Supervisor Engine 2

Note The uplink ports are fully functional on the redundant Supervisor Engine 2 in standby mode.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 837
3702
Doc:

Both supervisor engines in a single chassis must be completely identical. You can configure the redundant supervisor engines in a Catalyst 6500 series switch in one of three configurations:

  - Two supervisor engines, each with no MSFC and no PFC
  - Two supervisor engines, each configured with a PFC daughter card
  - Two supervisor engines, each configured with both an MSFC and a PFC daughter card
- Backplane bandwidth scalable up to 256 Gbps

Note Backplane bandwidth greater than 32 Gbps requires that you install either a Switch Fabric Module or Supervisor Engine 720 in the Catalyst 6513 switch chassis.

- A Switch Fabric Module (supports WS-X6500-SFM2 only)
  - The Switch Fabric Module requires Supervisor Engine 2. Supervisor Engine 1A does not support the Switch Fabric Module.
  - You must install the Switch Fabric Module in slot 7 or slot 8 of the Catalyst 6513 switch. For redundancy, you can install a standby Switch Fabric Module. The module first installed functions as the primary module. When you install two Switch Fabric Modules at the same time, the module in slot 7 acts as the primary module, and the module in slot 8 acts as the backup. If you reset the module in slot 7, the module in slot 8 becomes the primary module.

Note Supervisor Engine 720 has built-in switching fabric and does not require that Switching Fabric Modules be installed in the chassis.

- Up to 12 additional hot-swappable switching modules
  - Fabric-enabled module support provided in all slots (requires a Switch Fabric Module (WS-X6500-SFM2) or Supervisor Engine 720 be installed)
  - Dual Fabric connectivity supported in slots 9-13 (requires a Switch Fabric Module (WS-X6500-SFM2) or Supervisor Engine 720 be installed)
- Hot-swappable fan assembly

Note The high capacity fan tray (WS-C6K-13SLT-FAN2) must be installed when a Supervisor Engine 720 is installed in the chassis.

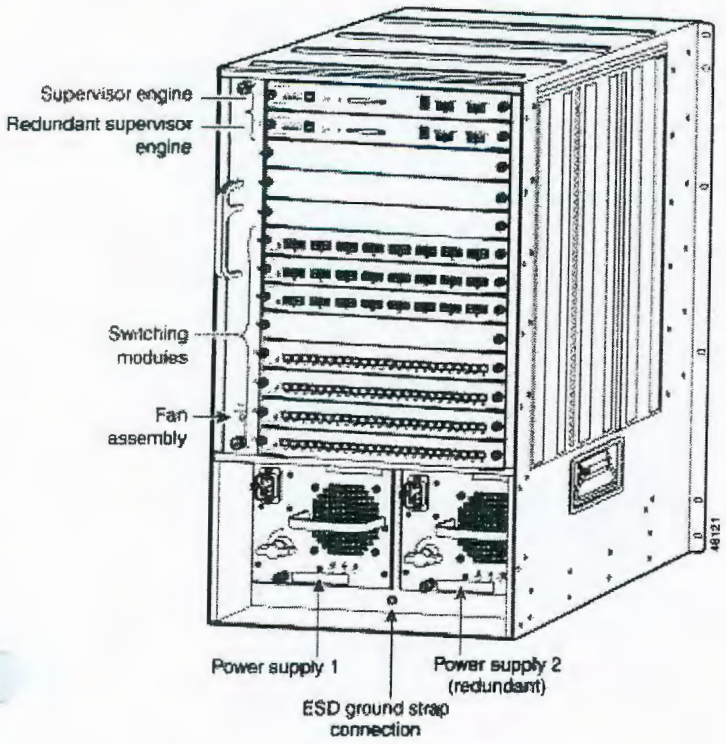
- Redundant AC-input or DC-input power supplies

Note When a Supervisor Engine 720 and the higher capacity fan tray are installed, you must install 2500 W or higher capacity power supplies in the chassis.

Figure 1-6 Catalyst 6513 Switch

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 838
Nº 3702 Doc:

16 943



System Features

This section describes the hardware features for the Catalyst 6500 series switches. For software descriptions, refer to your software configuration guide. For module descriptions and installation procedures, refer to the *Catalyst 6500 Series Switches Module Installation Guide*.

Port Density

Table 1-2 lists the port densities of the Catalyst 6500 series switches.

Table 1-2 Catalyst 6500 Series Port Density

Architecture	Catalyst 6500 Series Switches
Number of 10 Gigabit Ethernet Ports	2 (3 slots) Catalyst 6503 switch 5 (6 slots) Catalyst 6506 switch 8 (9 slots) Catalyst 6509 switch 12 (13 slots) Catalyst 6513 switch
Number of Gigabit Ethernet Ports	34 (3 slots) Catalyst 6503 switch 82 (6 slots) Catalyst 6506 switch 130 (9 slots) Catalyst 6509 switch 194 (13 slots) Catalyst 6513 switch
Number of 100BASE-FX Ethernet Ports	96 (3 slots) Catalyst 6503 switch 120 (6 slots) Catalyst 6506 switch 192 (9 slots) Catalyst 6509 switch 288 (13 slots) Catalyst 6513 switch

RQS nº 03/2005 - CN - CPMI - CORREIOS
839
Fls. Nº 3702
Doc:

16.947
2

Number of 10/100 Ethernet Ports	96 (3 slots) Catalyst 6503 switch 240 (6 slots) Catalyst 6506 switch 384 (9 slots) Catalyst 6509 switch 576 (13 slots) Catalyst 6513 switch
Number of 10BASE-FL Ethernet Ports	48 (3 slots) Catalyst 6503 switch 120 (6 slots) Catalyst 6506 switch 192 (9 slots) Catalyst 6509 switch 288 (13 slots) Catalyst 6513 switch
Number of ATM OC-12 Ports	2 (3 slots) Catalyst 6503 switch 5 (6 slots) Catalyst 6506 switch 8 (9 slots) Catalyst 6509 switch 12 (13 slots) Catalyst 6513 switch
Number of FlexWAN Modules	2 (3 slots) Catalyst 6503 switch 5 (6 slots) Catalyst 6506 switch 8 (9 slots) Catalyst 6509 switch 12 (13 slots) Catalyst 6513 switch

Redundancy

Catalyst 6500 series switches have these redundancy features:

- Ability to house two hot-swappable supervisor engines
- Ability to house two fully redundant, AC-input or DC-input, load-sharing power supplies

---

Note In certain configurations, the power supplies are not fully redundant. Refer to the "Power Supply Redundancy" section.

- A hot-swappable fan assembly containing multiple fans
- Redundant backplane-mounted clock modules
- Redundant backplane-mounted voltage termination (VTT) modules

Component Hot Swapping

You can hot swap all modules (including the supervisor engine if you have a redundant supervisor engine) and the fan assembly. You can add, replace, or remove modules without interrupting the system power or causing other software or interfaces to shut down.

Fan Assembly

The system fan assembly is located in the chassis and provides cooling air for the supervisor engine and the switching modules. The following figures show the direction of airflow into and out of the switch: Figure 1-7 (Catalyst 6503 switch), Figure 1-8 (Catalyst 6506 switch), Figure 1-9 (Catalyst 6509 switch), Figure 1-10 (Catalyst 6509-NEB switch), and Figure 1-11 (Catalyst 6513 switch). Sensors on the supervisor engine monitor the internal air temperatures. If the air temperature exceeds a preset threshold, the environmental monitor displays warning messages.

ADS nº 01/2005 - CN - CPMI - CORREIOS
Fls Nº 840
3702
Doc:

16-946

Note We recommend that you maintain a minimum air space of 6 inches (15 cm) between walls and the chassis air vents and a minimum horizontal separation of 12 inches (30.5 cm) between two chassis to prevent overheating.

If an individual fan within the assembly fails, the FAN STATUS LED turns red. Individual fans cannot be replaced. To replace a fan assembly, see the "Removing and Replacing the Fan Assembly" section.

Refer to your software configuration guide for information on environmental monitoring.

Figure 1-7 Catalyst 6503 Switch Internal Airflow

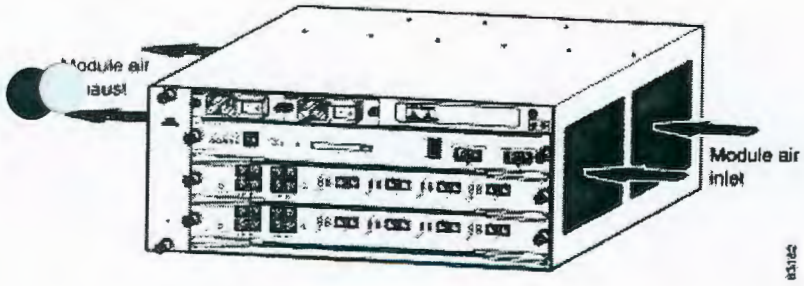


Figure 1-8 Catalyst 6506 Switch Internal Airflow

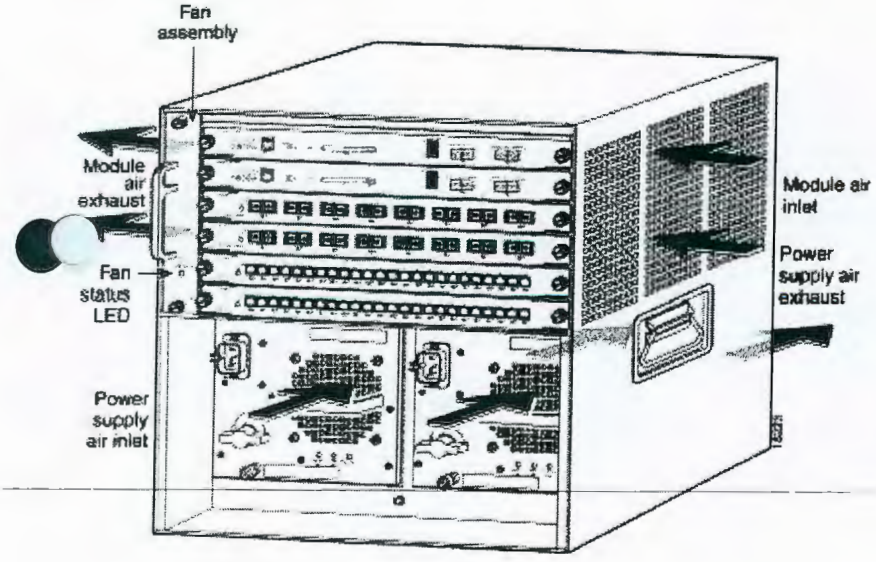


Figure 1-9 Catalyst 6509 Switch Internal Airflow

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 841
Nº Doc 3702

16.945
L

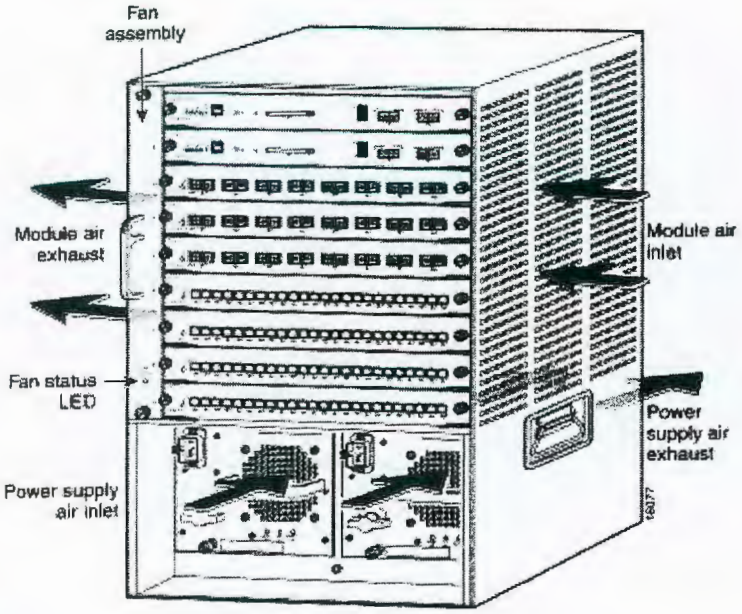


Figure 1-10 Catalyst 6509-NEB Switch Internal Airflow

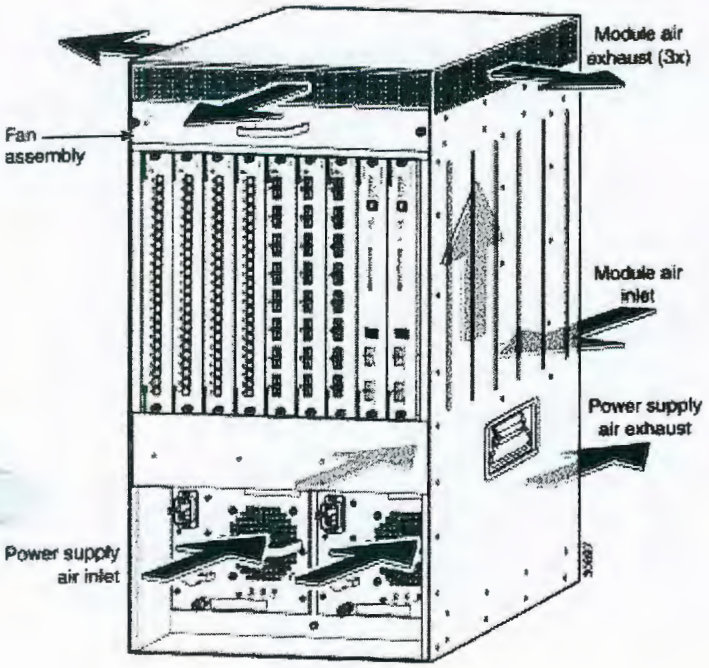
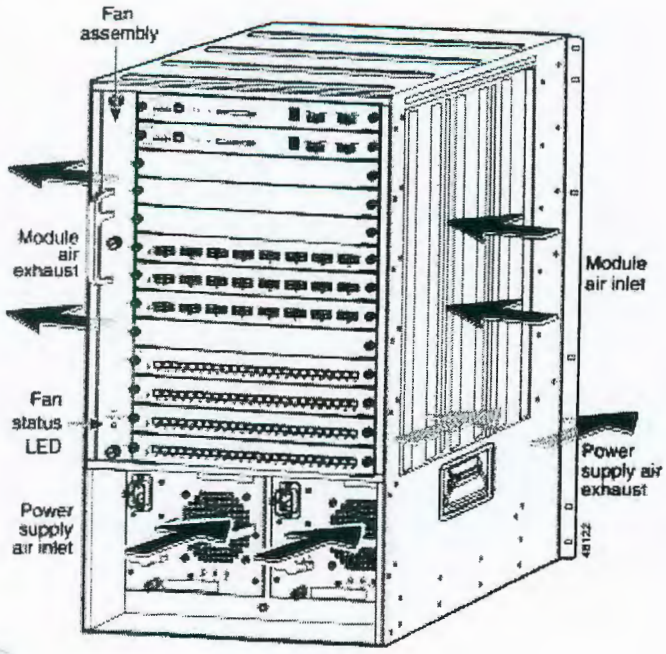


Figure 1-11 Catalyst 6513 Switch Internal Airflow

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 842
Nº Doc: 3702

J6 944 L



Power Supplies

Catalyst 6500 series switch power supplies are available in five power ratings:

- 950 W—AC and DC input (PWR-950-AC and PWR-950-DC) (for use with the Catalyst 6503 switch only)
- 1000 W—AC input only (WS-CAC-1000W)
- 1300 W—AC and DC input (WS-CAC-1300W and WS-CDC-1300W)
- 2500 W—AC and DC input (WS-CAC-2500W and WS-CDC-2500W)
- 4000 W—AC input only (WS-CAC-4000W-US1 or WS-CAC-4000W-INT)

950 W Power Supply (PWR-950-AC and PWR-950-DC)

Note The 950 W AC-input and DC-input power supplies can be installed in the Catalyst 6503 switch chassis only. They cannot be installed in any other Catalyst 6500 series switch chassis.

The 950 W power supplies (see Figure 1-12) do not connect directly to source AC but use a power entry module (PEM), located on the front of the chassis, to connect the site power source to the power supply located in the back of the chassis.

The AC-input PEM (shown in Figure 1-13) and DC-input PEM (shown in Figure 1-14) provide an input power connection on the front of the router chassis to connect the site power source to the power supply. You can connect the DC-input power supply to the power source with heavy gauge wiring connected to a terminal block. The wire gauge size is determined by local electrical codes and restrictions.

Note The power cord is not shown in Figure 1-13.

The PEMs have an illuminated power switch (AC-input only), current protection, surge and EMI suppression, and filtering functions.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 843
Nº Doc: 3702

16.943
2

Figure 1-12 Catalyst 6503 950 W AC- and DC-Input Power Supplies

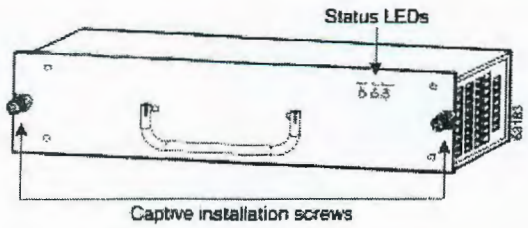


Figure 1-13 Catalyst 6503 AC Power Entry Module (PEM)

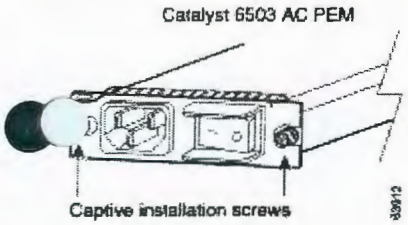
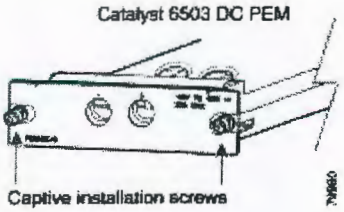


Figure 1-14 Catalyst 6503 DC Power Entry Module (PEM)



1000 W, 1300 W, 2500 W, and 4000 W Power Supplies

The 1000 W, 1300 W, 2500 W, and 4000 W AC-input and DC-input power supplies have the same form factor and designed for use in the Catalyst 6500 series switches.

Note The 1000 W, 1300 W, 2500 W, and 4000 W power supplies have a different form factor and cannot be used in the Catalyst 6503 series switch.

Catalyst 6500 series chassis power supply configurations for the 1000 W, 1300 W, 2500 W and 4000 W power supplies are shown in Table 1-3.

Table 1-3 Catalyst 6500 Series Power Supply Configurations

Catalyst 6500 Series Switch	Power Supply Configurations
Catalyst 6506	1000 W AC-input

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 844
Nº Doc 3702

16.942
L

	1300 W AC- and DC-input
	2500 W AC- and DC-input
Catalyst 6509	1300 W AC- and DC-input
	2500 W AC- and DC-input
	4000 W AC-input
Catalyst 6509-NEB	1300 W AC- and DC-input
	2500 W AC- and DC-input
	4000 W AC-input
Catalyst 6513	2500 W AC- and DC-input
	4000 W AC-input

Catalyst 6500 series switches support redundant AC-input and DC-input power supplies. Unlike the Catalyst 4000 family and Catalyst 5000 family switches, the Catalyst 6500 series switches allow you to mix AC-input and DC-input power supplies in the same chassis.

Many telco organizations require a -48 VDC power supply to accommodate their power distribution systems. From an operational perspective, the DC-input power supply has the same characteristics as the AC-input version.

The AC-input power supply (see Figure 1-15) has a detachable power cord (except for the WS-CAC-4000W) that allows you to connect each power supply to the site power source. You can connect the DC-input power supply (see Figure 1-16) to the power source with heavy gauge wiring connected to a terminal block. The wire gauge size is determined by local electrical codes and restrictions.

Note The power cord is not shown in Figure 1-15.

Note With a fully populated Catalyst 6513 switch, two 2500 W power supplies are not fully redundant. If you run the 2500 W power supply at the low range input (100 to 120 VAC), it is not redundant in a fully populated Catalyst 6509 or Catalyst 6509-NEB switch.

Note The 2500 W AC-input power supply needs 220 VAC to deliver 2500 W of power. When powered with 110 VAC, it delivers only 1300 W. In addition, the power supply needs 16 A, regardless of whether it is plugged into 110 VAC or 220 VAC.

For complete power specifications, see "Technical Specifications."

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 845
3702
Doc:

16 941

Figure 1-15 AC-Input Power Supply

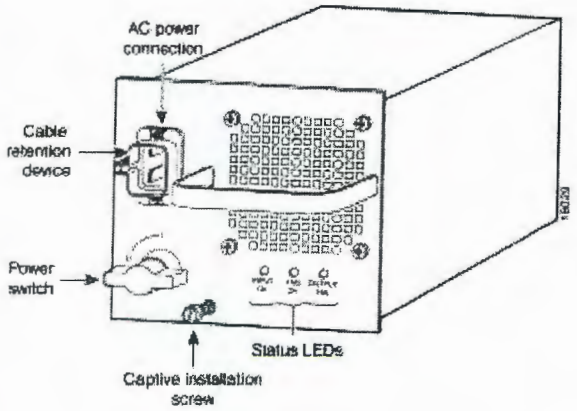
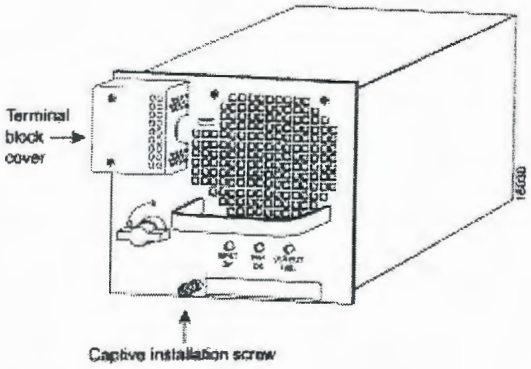


Figure 1-16 DC-Input Power Supply



Power Supply Redundancy

Catalyst 6500 series modules have different power requirements. Depending upon the wattage of the power supply, certain switch configurations might require more power than a single power supply can provide. Although the power management feature allows you to power all installed modules with two power supplies, redundancy is not supported in this configuration. Redundant and nonredundant power configurations are summarized in Table 1-4. The effects of changing the power supply configurations are summarized in Table 1-5.

Note For proper load-sharing operation in a redundant power supply configuration, you must install two modules in the chassis. If you fail to install two modules, you might receive spurious OUTPUT FAIL indications on the power supply.

Table 1-4 Power Supply Redundancy

If you have two power supplies of	and redundancy is	Then

RQS nº 03/2005 - CN
CPMI - CORREIO
Fls. Nº 84
3702
Rubr.

16 940

Equal wattage	Enabled	The total power drawn from both supplies is never greater than the capability of one supply. If one supply malfunctions, the other supply can take over the entire system load. Each power supply provides approximately half of the required power to the system. Load sharing and redundancy are enabled automatically; no software configuration is required.
Unequal wattage	Enabled	Both power supplies come online, but a syslog message displays that the lower wattage power supply will be disabled. If the active power supply fails, the system shuts down. The lower wattage power supply must then be manually turned on. The lower wattage power supply selectively powers up the modules so that the capacity of the power supply is not exceeded.
Equal or unequal wattage	Disabled	The total power available to the system is approximately 167 percent of the lower wattage power supply. The system powers up as many modules as the combined capacity allows. If the higher wattage power supply fails, the lower wattage supply might also shut down due to overcurrent protection, thus preventing damage to the lower wattage power supply.

Table 1-5 Effects of Power Supply Configuration Changes

Configuration Change	Effect
Redundant to nonredundant	• System log and syslog messages are generated. • System power is increased to approximately 167 percent of the lower wattage power supply. • The modules marked as *power-deny* in the **show module** Status field are brought up if there is sufficient power.
Nonredundant to redundant	• System log and syslog messages are generated. • System power is the power capability of the larger wattage supply. • If there is not enough power for all previously powered-up modules, some modules are powered down and marked as *power-deny* in the **show module** Status field.
Equal wattage power supply is inserted with redundancy enabled	• System log and syslog messages are generated. • System power equals the power capability of one supply (both supplies provide approximately one half of the total current). • No change in the module status because the power capability is unchanged.
Equal wattage power supply is	• System log and syslog messages are generated.

ROS nº 03/2005 - CN - CPMI - CORREIOS
847
Nº 3702
Doc

inserted with redundancy disabled	• System power is the combined power capability of both supplies. • The modules marked as *power-deny* in the **show module** Status field are brought up if there is sufficient power.
Higher wattage power supply is inserted with redundancy enabled	• System log and syslog messages are generated. • The system disables the lower wattage power supply; the higher wattage supply powers the system.
Lower wattage power supply is inserted with redundancy enabled	• System log and syslog messages are generated. • The system disables the lower wattage power supply; the higher wattage supply powers the system.
Higher or lower wattage power supply is inserted with redundancy disabled	• System log and syslog messages are generated. • System power is increased to the combined power capability of both supplies. • The modules marked as *power-deny* in the **show module** Status field are brought up if there is sufficient power.
Power supply is removed with redundancy enabled	• System log and syslog messages are generated. • If the power supplies are of equal wattage, there is no change in the module status because the power capability is unchanged. If the power supplies are of unequal wattage and the lower wattage supply is removed, there is no change in the module status. If the power supplies are of unequal wattage and the higher wattage supply is removed, the lower wattage power supply must be manually turned on. (The system had previously turned off the lower wattage power supply.)
Power supply is removed with redundancy disabled	• System log and syslog messages are generated. • System power is decreased to the power capability of one supply. • If there is not enough power for all previously powered-up modules, some modules are powered down and marked as *power-deny* in the **show module** Status field.
System is booted with power supplies of different wattage installed and redundancy enabled	• System log and syslog messages are generated. • The lower wattage supply is disabled.
System is booted with power	• System log and syslog messages are generated.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 848
Nº 3702
Doc.

supplies of equal or different wattage installed and redundancy disabled	• System power equals the combined power capability of both supplies. • The system powers up as many modules as the combined capacity allows.

You can change the configuration of the power supplies to redundant or nonredundant at any time. If you switch from a redundant to a nonredundant configuration, both power supplies are enabled (even a power supply that was disabled because it was of a lower wattage than the other power supply). If you change from a nonredundant to a redundant configuration, both power supplies are initially enabled, and if they are of the same wattage, remain enabled. If they are of different wattage, a syslog message displays and the lower wattage supply is disabled.

For additional information about the power management feature and individual module power consumption, refer to your software configuration guide.

Environmental Monitoring of the Power Supply

The environmental monitoring and reporting functions allow you to maintain normal system operation by resolving adverse environmental conditions prior to loss of operation.

The power supplies monitor their own internal temperature and voltages. In the event of excessive internal temperature, the power supply will shut down to prevent damage. When the power supply returns to a safe operating temperature, it will restart. In the event of an abnormal voltage on one or more outputs of the power supplies, the OUTPUT FAIL LED will light. Substantial overvoltage conditions can lead to a power supply shutdown.

The power supply front panel LEDs are described in Table 1-6.

For more information about the environmental monitoring feature, refer to your software configuration guide.

Table 1-6 Power Supply Front Panel LEDs

LED	Description
INPUT OK	AC-input power supplies: • Green when the input voltage is OK (85 VAC or greater) • Off when the input voltage falls below 70 VAC or if the power supply shuts down DC-input power supplies: • Green when the input voltage is OK (-40.5 VDC or greater) • Off when the input voltage falls below -33 VDC or if the power supply shuts down
FAN OK	Green when the power supply fan is operating properly. Red when a power supply fan failure is detected.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 849
Nº Doc. 3702

OUTPUT FAIL	Red when there is a problem with one or more of the DC-output voltages of the power supply

Power Supply Fan Assembly

The power supplies have a built-in fan; air enters the front of the fan (power-input end) and exits through the back. An air dam keeps the airflow separate from the rest of the chassis, which is cooled by the system fan assembly.

Power supply fans are not field-replaceable; the power supply must be replaced. To replace a power supply, see the "Removing and Replacing the 1000 W, 1300 W, 2500 W, and 4000 W Power Supplies" section.

HOME CONTENTS PREVIOUS NEXT GLOSSARY FEEDBACK SEARCH HELP

Posted: Wed Jun 11 10:35:00 PDT 2003
All contents are Copyright © 1992--2003 Cisco Systems, Inc. All rights reserved.
Important Notices and Privacy Statement.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 850
Doc: 3702

ANEXO (31)

16.936
L

Configuring EtherChannels

This chapter describes how to configure EtherChannels on the Catalyst 6500 series switch Layer 2 or Layer 3 LAN ports.

Note

- For complete syntax and usage information for the commands used in this chapter, refer to the *Catalyst 6500 Series Switch Cisco IOS Command Reference* publication.
- The commands in the following sections can be used on all LAN ports in Catalyst 6500 series switches, including the ports on the supervisor engine and a redundant supervisor engine.
- Release 12.1(13)E and later releases support the IEEE 802.3ad Link Aggregation Control Protocol (LACP).
- The WS-X6548-GE-TX and WS-X6548V-GE-TX fabric-enabled switching modules do not support more than 1 Gbps of traffic per EtherChannel, except when the switch is operating in truncated mode.
- The WS-X6148-GE-TX and WS-X6148V-GE-TX switching modules do not support more than 1 Gbps of traffic per EtherChannel.

This chapter consists of these sections:

- Understanding How EtherChannels Work, page 13-1
- EtherChannel Feature Configuration Guidelines and Restrictions, page 13-5
- Configuring EtherChannels, page 13-6

Understanding How EtherChannels Work

These sections describe how EtherChannels work:

- EtherChannel Feature Overview, page 13-1
- Understanding How EtherChannels Are Configured, page 13-2
- Understanding Port Channel Interfaces, page 13-4
- Understanding Load Balancing, page 13-5

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 851
Nº Doc: 3702

EtherChannel Feature Overview

An EtherChannel bundles individual Ethernet links into a single logical link that provides the aggregate bandwidth of up to eight physical links.

A Catalyst 6500 series switch supports a maximum of 64 EtherChannels (256 with Release 12.1(2)E and earlier). You can form an EtherChannel with up to eight compatibly configured LAN ports on any module in a Catalyst 6500 series switch. All LAN ports in each EtherChannel must be the same speed and must all be configured as either Layer 2 or Layer 3 LAN ports.

Note The network device to which a Catalyst 6500 series switch is connected may impose its own limits on the number of ports in an EtherChannel.

If a segment within an EtherChannel fails, traffic previously carried over the failed link switches to the remaining segments within the EtherChannel. When a failure occurs, the EtherChannel feature sends a trap that identifies the switch, the EtherChannel, and the failed link. Inbound broadcast and multicast packets on one segment in an EtherChannel are blocked from returning on any other segment of the EtherChannel.

Understanding How EtherChannels Are Configured

These sections describe how EtherChannels are configured:

- EtherChannel Configuration Overview, page 13-2
- Understanding Manual EtherChannel Configuration, page 13-3
- Understanding PAgP EtherChannel Configuration, page 13-3
- Understanding IEEE 802.3ad LACP EtherChannel Configuration, page 13-3

EtherChannel Configuration Overview

You can configure EtherChannels manually or you can use the Port Aggregation Control Protocol (PAgP) or, with Release 12.1(13)E and later, the Link Aggregation Control Protocol (LACP) to form EtherChannels. The EtherChannel protocols allow ports with similar characteristics to form an EtherChannel through dynamic negotiation with connected network devices. PAgP is a Cisco-proprietary protocol and LACP is defined in IEEE 802.3ad.

PAgP and LACP do not interoperate with each other. Ports configured to use PAgP cannot form EtherChannels with ports configured to use LACP. Ports configured to use LACP cannot form EtherChannels with ports configured to use PAgP.

Table 13-1 lists the user-configurable EtherChannel modes.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 852
Doc: 3702

Table 13-1 EtherChannel Modes

Mode	Description
on	Mode that forces the LAN port to channel unconditionally. In the **on** mode, a usable EtherChannel exists only when a LAN port group in the **on** mode is connected to another LAN port group in the **on** mode. Because ports configured in the **on** mode do not negotiate, there is no negotiation traffic between the ports. You cannot configure the **on** mode with an EtherChannel protocol.
auto	PAgP mode that places a LAN port into a passive negotiating state, in which the port responds to PAgP packets it receives but does not initiate PAgP negotiation. (Default)
desirable	PAgP mode that places a LAN port into an active negotiating state, in which the port initiates negotiations with other LAN ports by sending PAgP packets.
passive	LACP mode that places a port into a passive negotiating state, in which the port responds to LACP packets it receives but does not initiate LACP negotiation. (Default)
active	LACP mode that places a port into an active negotiating state, in which the port initiates negotiations with other ports by sending LACP packets.

Understanding Manual EtherChannel Configuration

Manually configured EtherChannel ports do not exchange EtherChannel protocol packets. A manually configured EtherChannel forms only when you enter configure all ports in the EtherChannel compatibly.

Understanding PAgP EtherChannel Configuration

PAgP supports the automatic creation of EtherChannels by exchanging PAgP packets between LAN ports. PAgP packets are exchanged only between ports in **auto** and **desirable** modes.

The protocol learns the capabilities of LAN port groups dynamically and informs the other LAN ports. Once PAgP identifies correctly matched Ethernet links, it facilitates grouping the links into an EtherChannel. The EtherChannel is then added to the spanning tree as a single bridge port.

Both the **auto** and **desirable** modes allow PAgP to negotiate between LAN ports to determine if they can form an EtherChannel, based on criteria such as port speed and trunking state. Layer 2 EtherChannels also use VLAN numbers.

LAN ports can form an EtherChannel when they are in different PAgP modes if the modes are compatible. For example:

- A LAN port in **desirable** mode can form an EtherChannel successfully with another LAN port that is in **desirable** mode.
- A LAN port in **desirable** mode can form an EtherChannel with another LAN port in **auto** mode.
- A LAN port in **auto** mode cannot form an EtherChannel with another LAN port that is also in **auto** mode, because neither port will initiate negotiation.

Understanding IEEE 802.3ad LACP EtherChannel Configuration

Release 12.1(13)E and later releases support IEEE 802.3ad LACP EtherChannels. LACP supports the automatic creation of EtherChannels by exchanging LACP packets between LAN ports. LACP packets are exchanged only between ports in **passive** and **active** modes.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 13-3 853
3702
Doc:

The protocol learns the capabilities of LAN port groups dynamically and informs the other LAN ports. Once LACP identifies correctly matched Ethernet links, it facilitates grouping the links into an EtherChannel. The EtherChannel is then added to the spanning tree as a single bridge port.

Both the **passive** and **active** modes allow LACP to negotiate between LAN ports to determine if they can form an EtherChannel, based on criteria such as port speed and trunking state. Layer 2 EtherChannels also use VLAN numbers.

LAN ports can form an EtherChannel when they are in different LACP modes as long as the modes are compatible. For example:

- A LAN port in **active** mode can form an EtherChannel successfully with another LAN port that is in **active** mode.
- A LAN port in **active** mode can form an EtherChannel with another LAN port in **passive** mode.
- A LAN port in **passive** mode cannot form an EtherChannel with another LAN port that is also in **passive** mode, because neither port will initiate negotiation.

LACP uses the following parameters:

- LACP system priority—You must configure an LACP system priority on each switch running LACP. The system priority can be configured automatically or through the CLI (see the "Configuring the LACP System Priority and System ID" section on page 13-9). LACP uses the system priority with the switch MAC address to form the system ID and also during negotiation with other systems.

Note The LACP system ID is the combination of the LACP system priority value and the MAC address of the switch.

- LACP port priority—You must configure an LACP port priority on each port configured to use LACP. The port priority can be configured automatically or through the CLI (see the "Configuring Channel Groups" section on page 13-7). LACP uses the port priority with the port number to form the port identifier. LACP uses the port priority to decide which ports should be put in standby mode when there is a hardware limitation that prevents all compatible ports from aggregating.
- LACP administrative key—LACP automatically configures an administrative key value equal to the channel group identification number on each port configured to use LACP. The administrative key defines the ability of a port to aggregate with other ports. A port's ability to aggregate with other ports is determined by these factors:
  - Port physical characteristics, such as data rate, duplex capability, and point-to-point or shared medium
  - Configuration restrictions that you establish

On ports configured to use LACP, LACP tries to configure the maximum number of compatible ports in an EtherChannel, up to the maximum allowed by the hardware (eight ports). If LACP cannot aggregate all the ports that are compatible (for example, the remote system might have more restrictive hardware limitations), then all the ports that cannot be actively included in the channel are put in hot standby state and are used only if one of the channeled ports fails. You can configure an additional 8 standby ports (total of 16 ports associated with the EtherChannel).

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 854
Doc: 3702

16.932
2

Understanding Port Channel Interfaces

Each EtherChannel has a numbered port channel interface. Release 12.1(5)E and later releases support a maximum of 64 port channel interfaces, numbered from 1 to 256.

Note Releases 12.1(4)E1, 12.1(3a)E4, and 12.1(3a)E3 support a maximum of 64 port channel interfaces, numbered from 1 to 64. Releases 12.1(2)E and earlier support a maximum of 256 port channel interfaces, numbered from 1 to 256.

The configuration that you apply to the port channel interface affects all LAN ports assigned to the port channel interface.

After you configure an EtherChannel, the configuration that you apply to the port channel interface affects the EtherChannel; the configuration that you apply to the LAN ports affects only the LAN port where you apply the configuration. To change the parameters of all ports in an EtherChannel, apply the configuration commands to the port channel interface, for example, Spanning Tree Protocol (STP) commands or commands to configure a Layer 2 EtherChannel as a trunk.

Understanding Load Balancing

An EtherChannel balances the traffic load across the links in an EtherChannel by reducing part of the binary pattern formed from the addresses in the frame to a numerical value that selects one of the links in the channel.

EtherChannel load balancing can use MAC addresses or IP addresses. With a PFC2, EtherChannel load balancing can also use Layer 4 port numbers. EtherChannel load balancing can use either source or destination or both source and destination addresses or ports. The selected mode applies to all EtherChannels configured on the switch.

Use the option that provides the balance criteria with the greatest variety in your configuration. For example, if the traffic on an EtherChannel is going only to a single MAC address and you use the destination MAC address as the basis of EtherChannel load balancing, the EtherChannel always chooses the same link in the EtherChannel; using source addresses or IP addresses might result in better load balancing.

EtherChannel Feature Configuration Guidelines and Restrictions

When EtherChannel interfaces are configured improperly, they are disabled automatically to avoid network loops and other problems. To avoid configuration problems, observe these guidelines and restrictions:

- All Ethernet LAN ports on all modules, including those on a redundant supervisor engine, support EtherChannels (maximum of eight LAN ports) with no requirement that the LAN ports be physically contiguous or on the same module.
- Configure all LAN ports in an EtherChannel to use the same EtherChannel protocol; you cannot run two EtherChannel protocols in one EtherChannel.
- Configure all LAN ports in an EtherChannel to operate at the same speed and in the same duplex mode.
- LACP does not support half-duplex. Half-duplex ports in an LACP EtherChannel are put in the suspended state.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
855
Fls Nº 13-5
3702
Doc:

- Enable all LAN ports in an EtherChannel. If you shut down a LAN port in an EtherChannel, it is treated as a link failure and its traffic is transferred to one of the remaining ports in the EtherChannel.
- An EtherChannel will not form if one of the LAN ports is a Switched Port Analyzer (SPAN) destination port.
- For Layer 3 EtherChannels, assign Layer 3 addresses to the port channel logical interface, not to the LAN ports in the channel.
- For Layer 2 EtherChannels:
  - Assign all LAN ports in the EtherChannel to the same VLAN or configure them as trunks.
  - If you configure an EtherChannel from trunking LAN ports, verify that the trunking mode is the same on all the trunks. LAN ports in an EtherChannel with different trunk modes can operate unpredictably.
  - An EtherChannel supports the same allowed range of VLANs on all the LAN ports in a trunking Layer 2 EtherChannel. If the allowed range of VLANs is not the same, the LAN ports do not form an EtherChannel.
  - LAN ports with different STP port path costs can form an EtherChannel as long they are compatibly configured with each other. If you set different STP port path costs, the LAN ports are not incompatible for the formation of an EtherChannel.
  - An EtherChannel will not form if protocol filtering is set differently on the LAN ports.
- After you configure an EtherChannel, the configuration that you apply to the port channel interface affects the EtherChannel. The configuration that you apply to the LAN ports affects only the LAN port where you apply the configuration.
- With Release 12.1(12c)E1 and later releases, when QoS is enabled, enter the **no mls qos channel-consistency** port-channel interface command to support EtherChannels that have ports with and without strict-priority queues.

Configuring EtherChannels

These sections describe how to configure EtherChannels:

- Configuring Port Channel Logical Interfaces for Layer 3 EtherChannels, page 13-6
- Configuring Channel Groups, page 13-7
- Configuring EtherChannel Load Balancing, page 13-10

Note

- Make sure that the LAN ports are configured correctly (see the "EtherChannel Feature Configuration Guidelines and Restrictions" section on page 13-5).
- With Release 12.1(11b)E and later, when you are in configuration mode you can enter EXEC mode commands by entering the **do** keyword before the EXEC mode command.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 856
Nº Doc: 3702

16.930
L

Configuring Port Channel Logical Interfaces for Layer 3 EtherChannels

Note

- When configuring Layer 2 EtherChannels, you cannot put Layer 2 LAN ports into manually created port channel logical interfaces. If you are configuring a Layer 2 EtherChannel, do not perform the procedures in this section (see the "Configuring Channel Groups" section on page 13-7).
- When configuring Layer 3 EtherChannels, you must manually create the port channel logical interface as described in this section, and then put the Layer 3 LAN ports into the channel group (see the "Configuring Channel Groups" section on page 13-7).
- To move an IP address from a Layer 3 LAN port to an EtherChannel, you must delete the IP address from the Layer 3 LAN port before configuring it on the port channel logical interface.

To create a port channel interface for a Layer 3 EtherChannel, perform this task:

	Command	Purpose
Step 1	`Router(config)# interface port-channel number`	Creates the port channel interface.
	`Router(config)# no interface port-channel number`	Deletes the port channel interface.
Step 2	`Router(config-if)# ip address ip_address mask`	Assigns an IP address and subnet mask to the EtherChannel.
Step 3	`Router(config-if)# end`	Exits configuration mode.
Step 4	`Router# show running-config interface port-channel number`	Verifies the configuration.

When creating the port channel interface, the *group* number can be one of the following:

- Release 12.1(5)E and later—1 through 256, up to a maximum of 64 port channel interfaces
- Releases 12.1(4)E1, 12.1(3a)E4, and 12.1(3a)E3—1 through 64
- Release 12.1(2)E and earlier—1 through 256

This example shows how to create port channel interface 1:

```
Router# configure terminal
Router(config)# interface port-channel 1
Router(config-if)# ip address 172.32.52.10 255.255.255.0
Router(config-if)# end
```

This example shows how to verify the configuration of port channel interface 1:

```
Router# show running-config interface port-channel 1
Building configuration...

Current configuration:
!
interface Port-channel1
 ip address 172.32.52.10 255.255.255.0
 no ip directed-broadcast
end
Router#
```

RQS nº 03/2005 - CN -
CPMI - CORREIOS
0857
Fls Nº 13-7
Doc: 3702

Configuring Channel Groups

Note

- When configuring Layer 3 EtherChannels, you must manually create the port channel logical interface first (see the "Configuring Port Channel Logical Interfaces for Layer 3 EtherChannels" section on page 13-6), and then put the Layer 3 LAN ports into the channel group as described in this section.
- When configuring Layer 2 EtherChannels, configure the LAN ports with the **channel-group** command as described in this section, which automatically creates the port channel logical interface. You cannot put Layer 2 LAN ports into a manually created port channel interface.
- For Cisco IOS to create port channel interfaces for Layer 2 EtherChannels, the Layer 2 LAN ports must be connected and functioning.

To configure channel groups, perform this task for each LAN port:

	Command	Purpose
Step 1	`Router(config)# interface` *type*[1] *slot/port*	Selects a LAN port to configure.
Step 2	`Router(config-if)# no ip address`	Ensures that there is no IP address assigned to the LAN port.
Step 3	`Router(config-if)# channel-protocol {lacp | pagp}`	(Optional) On the selected LAN port, restricts the **channel-group** command to the EtherChannel protocol configured with the **channel-protocol** command.
	`Router(config-if)# no channel-protocol`	Removes the restriction.
Step 4	`Router(config-if)# channel-group` *number* `mode {active | auto | desirable | on | passive}`	Configures the LAN port in a port channel and specifies the mode (see Table 13-1 on page 13-2). PAgP supports only the auto and desirable modes. LACP supports only the active and passive modes.
	`Router(config-if)# no channel-group`	Removes the LAN port from the channel group.
Step 5	`Router(config-if)# lacp port-priority` *priority_value*	(Optional for LACP) Valid values are 1 through 65535. Higher numbers have lower priority. The default is 32768.
	`Router(config-if)# no lacp port-priority`	Reverts to the default.
Step 6	`Router(config-if)# end`	Exits configuration mode.
Step 7	`Router# show running-config interface` *type*[1] *slot/port* `Router# show interfaces` *type*[1] *slot/port* `etherchannel`	Verifies the configuration.

1. *type* = **ethernet**, **fastethernet**, **gigabitethernet**, or **tengigabitethernet**

This example shows how to configure Fast Ethernet ports 5/6 and 5/7 into port channel 2 with PAgP mode **desirable**:

```
Router# configure terminal
Router(config)# interface range fastethernet 5/6 -7
Router(config-if)# channel-group 2 mode desirable
Router(config-if)# end
```


RQS nº 03/2005 - CN - CPMI - CORREIOS
78-14099-03 B0
Fls Nº 858
3702
Doc:

16.928
L.

Note See the "Configuring a Range of Interfaces" section on page 6-4 for information about the **range** keyword.

This example shows how to verify the configuration of port channel interface 2:

```
Router# show running-config interface port-channel 2
Building configuration...

Current configuration:
!
interface Port-channel2
 no ip address
 switchport
 switchport access vlan 10
 switchport mode access
end
Router#
```

This example shows how to verify the configuration of Fast Ethernet port 5/6:

```
Router# show running-config interface fastethernet 5/6
Building configuration...

Current configuration:
!
interface FastEthernet5/6
 no ip address
 switchport
 switchport access vlan 10
 switchport mode access
 channel-group 2 mode desirable
end
Router# show interfaces fastethernet 5/6 etherchannel
Port state    = Down Not-in-Bndl
Channel group = 12          Mode = Desirable-Sl     Gcchange = 0
Port-channel  = null        GC   = 0x00000000          Pseudo port-channel = Po1
2
Port index    = 0           Load = 0x00        Protocol =   PAgP

Flags:  S - Device is sending Slow hello.  C - Device is in Consistent state.
        A - Device is in Auto mode.        P - Device learns on physical port.
        d - PAgP is down.
Timers: H - Hello timer is running.        Q - Quit timer is running.
        S - Switching timer is running.    I - Interface timer is running.

Local information:
                                Hello    Partner  PAgP     Learning  Group
Port        Flags State   Timers Interval Count   Priority   Method  Ifindex
Fa5/2       d     U1/S1           1s       0        128        Any      0

Age of the port in the current state: 04d:18h:57m:19s
```


RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 859
Nº Doc: 3702

16927

This example shows how to verify the configuration of port channel interface 2 after the LAN ports have been configured:

```
Router# show etherchannel 12 port-channel
                Port-channels in the group:
                ----------------------

Port-channel: Po12
------------

Age of the Port-channel   = 04d:18h:58m:50s
Logical slot/port    = 14/1          Number of ports = 0
GC                   = 0x00000000      HotStandBy port = null
Port state           = Port-channel Ag-Not-Inuse
Protocol             =   PAgP

Router#
```

Configuring the LACP System Priority and System ID

The LACP system ID is the combination of the LACP system priority value and the MAC address of the switch.

To configure the LACP system priority and system ID, perform this task:

	Command	Purpose
Step 1	`Router(config)# lacp system-priority` *priority_value*	(Optional for LACP) Valid values are 1 through 65535. Higher numbers have lower priority. The default is 32768.
	`Router(config)# no lacp system-priority`	Reverts to the default.
Step 2	`Router(config)# end`	Exits configuration mode.
Step 3	`Router# show lacp sys-id`	Verifies the configuration.

This example shows how to configure the LACP system priority:

```
Router# configure terminal
Router(config)# lacp system-priority 23456
Router(config)# end
Router(config)#
```

This example shows how to verify the configuration:

```
Router# show lacp sys-id
23456,0050.3e8d.6400
Router#
```

The system priority is displayed first, followed by the MAC address of the switch.

RQS nº 03/2005 - CN - CPMI - CORREIOS
860
FIS Nº
3702
Nº Doc:

16-926
2

Configuring EtherChannel Load Balancing

To configure EtherChannel load balancing, perform this task:

	Command	Purpose
Step 1	`Router(config)# port-channel load-balance {src-mac | dst-mac | src-dst-mac | src-ip | dst-ip | src-dst-ip | src-port | dst-port | src-dst-port}`	Configures EtherChannel load balancing.
	`Router(config)# no port-channel load-balance`	Reverts to default EtherChannel load balancing.
Step 2	`Router(config)# end`	Exits configuration mode.
Step 3	`Router# show etherchannel load-balance`	Verifies the configuration.

The load-balancing keywords indicate the following information:

- With a PFC2:
  - **src-port**—Source Layer 4 port
  - **dst-port**—Destination Layer 4 port
  - **src-dst-port**—Source and destination Layer 4 port
- With a PFC or PFC2:
  - **src-ip**—Source IP addresses
  - **dst-ip**—Destination IP addresses
  - **src-dst-ip**—Source and destination IP addresses
  - **src-mac**—Source MAC addresses
  - **dst-mac**—Destination MAC addresses
  - **src-dst-mac**—Source and destination MAC addresses

This example shows how to configure EtherChannel to use source and destination IP addresses:

```
Router# configure terminal
Router(config)# port-channel load-balance src-dst-ip
Router(config)# end
Router(config)#
```

This example shows how to verify the configuration:

```
Router# show etherchannel load-balance
Source XOR Destination IP address
Router#
```


RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 861
Nº Doc: 3702

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 862
Nº Doc: 3702

ANEXO (32)

16.924
L

Configuring PFC QoS

This chapter describes how to configure quality of service (QoS) as implemented on the policy feature card (PFC) on the Catalyst 6500 series switches.

Note For complete syntax and usage information for the commands used in this publication, refer to the *Catalyst 6500 Series Switch Cisco IOS Command Reference* publication.

This chapter contains these sections:

- Understanding How PFC QoS Works, page 32-1
- PFC QoS Default Configuration, page 32-24
- PFC QoS Configuration Guidelines and Restrictions, page 32-29
- Configuring PFC QoS, page 32-31

Note

- With Release 12.1(13)E and later releases and with an MSFC2, you can configure Network-Based Application Recognition (NBAR) on LAN ports instead of using PFC QoS.
- All ingress and egress traffic on a port that is configured with NBAR is processed in software on the MSFC2.
- The PFC2 provides hardware support for input ACLs on ports where you configure NBAR.
- When PFC QoS is enabled, the traffic through ports where you configure NBAR passes through the ingress and egress queues and drop thresholds. When PFC QoS is enabled, the MSFC2 sets egress CoS equal to egress IP precedence.
- After passing through an ingress queue, all traffic is processed in software on the MSFC2 on ports where you configure NBAR.
- To configure NBAR, refer to this publication:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/dtnbarad.htm

Understanding How PFC QoS Works

Typically, networks operate on a *best-effort* delivery basis, which means that all traffic has equal priority and an equal chance of being delivered in a timely manner. When congestion occurs, all traffic has an equal chance of being dropped.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 863
Nº Doc: 3702

QoS selects network traffic (both unicast and multicast), prioritizes it according to its relative importance, and uses congestion avoidance to provide priority-indexed treatment; QoS can also limit the bandwidth used by network traffic. QoS makes network performance more predictable and bandwidth utilization more effective.

Note On the Catalyst 6500 series switches, queue architecture and QoS queueing features such as Weighted-Round Robin (WRR) and Weighted Random Early Detection (WRED) are implemented with a fixed configuration in Application Specific Integrated Circuits (ASICs). The queueing architecture cannot be reconfigured. For more information, see the "Receive Queues" section on page 32-13 and the "Transmit Queues" section on page 32-21.

These sections describe PFC QoS:

- Hardware Supported by PFC QoS, page 32-2
- QoS Terminology, page 32-3
- PFC QoS Feature Flowcharts, page 32-5
- PFC QoS Feature Summary, page 32-11
- Ingress LAN Port Features, page 32-12
- PFC Marking and Policing, page 32-16
- LAN Egress Port Features, page 32-21
- PFC QoS Statistics Data Export, page 32-24

Hardware Supported by PFC QoS

With Release 12.1(11a)E and later, PFC QoS supports both LAN ports and optical services module (OSM) ports:

- *LAN ports* are Ethernet ports on Ethernet switching modules, except for the 4-port Gigabit Ethernet WAN (GBIC) module (OSM-4GE-WAN). Except for the OSM-4GE-WAN module, OSMs have four Ethernet LAN ports in addition to WAN ports. With earlier releases, PFC QoS supports only LAN ports.
- *OSM ports* are the WAN ports on OSMs. The PFC provides ingress QoS for traffic from OSM ports. For more information, see the following sections:
  - "Ingress OSM Port Features" section on page 32-11
  - "Egress OSM Port Features" section on page 32-12
  - "PFC Marking and Policing" section on page 32-16
  - "Attaching Policy Maps" section on page 32-21
  - "Configuring the Trust State of Ethernet LAN and OSM Ingress Ports" section on page 32-51
- Refer to the following publication for information about additional OSM QoS features:

  http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/cfgnotes/osm_inst/index.htm
- The PFC does not provide QoS for FlexWAN module ports. Refer to the following publications for information about FlexWAN module QoS features:
  - *Cisco IOS Quality of Service Solutions Configuration Guide*, Release 12.1:

    http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/qos_c/index.htm

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 864
Doc: 3702

16.922
L

- *Cisco IOS Quality of Service Solutions Command Reference*, Release 12.1:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/qos_r/index.htm
- *Class-Based Marking*:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t5/cbpmark2.htm
- *Traffic Policing*:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t5/dtpoli.htm
- *Distributed Class-Based Weighted Fair Queueing and Distributed Weighted Random Early Detection*:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t5/dtcbwred.htm
- *Distributed Low Latency Queueing*:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t5/dtllqvip.htm
- *Configuring Burst Size in Low Latency Queueing*:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t3/dtcfgbst.htm
- *Distributed Traffic Shaping*:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t5/dtdts.htm
- MPLS QoS:

  http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/cfgnotes/osm_inst/mpls.htm

QoS Terminology

This section defines some QoS terminology:

- *Packets* carry traffic at Layer 3.
- *Frames* carry traffic at Layer 2. Layer 2 frames carry Layer 3 packets.
- *Labels* are prioritization values carried in Layer 3 packets and Layer 2 frames:
  - Layer 2 class of service (CoS) values, which range between zero for low priority and seven for high priority:

    Layer 2 Inter-Switch Link (ISL) frame headers have a 1-byte User field that carries an IEEE 802.1p CoS value in the three least significant bits.

    Layer 2 802.1Q frame headers have a 2-byte Tag Control Information field that carries the CoS value in the three most significant bits, which are called the User Priority bits.

    Other frame types cannot carry Layer 2 CoS values.

Note On LAN ports configured as Layer 2 ISL trunks, all traffic is in ISL frames. On LAN ports configured as Layer 2 802.1Q trunks, all traffic is in 802.1Q frames except for traffic in the native VLAN.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 865
3702
Doc:

ANEXO (33)

16.923
2

Configuring STP and IEEE 802.1s MST

This chapter describes how to configure the Spanning Tree Protocol (STP) and the IEEE 802.1s Multiple Spanning Tree (MST) protocol on Catalyst 6500 series switches.

Note For complete syntax and usage information for the commands used in this chapter, refer to the *Catalyst 6500 Series Switch Cisco IOS Command Reference* publication.

This chapter consists of these sections:

- Understanding How STP Works, page 15-2
- Understanding How IEEE 802.1w RSTP Works, page 15-13
- Understanding How IEEE 802.1s MST Works, page 15-14
- Default STP Configuration, page 15-21
- STP and MST Configuration Guidelines and Restrictions, page 15-21
- Configuring STP, page 15-22
- Configuring IEEE 802.1s MST, page 15-34

Note
- For information on configuring the PortFast, UplinkFast, and BackboneFast STP enhancements, see Chapter 16, "Configuring Optional STP Features."
- Release 12.1(13)E and later releases support IEEE 802.1s MST and IEEE 802.1w, rapid reconfiguration of spanning tree.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 866
3702
Doc:

16.920

Understanding How STP Works

These sections describe how STP works:

- STP Overview, page 15-2
- Understanding the Bridge ID, page 15-3
- Understanding Bridge Protocol Data Units, page 15-4
- Election of the Root Bridge, page 15-4
- STP Protocol Timers, page 15-5
- Creating the Spanning Tree Topology, page 15-5
- STP Port States, page 15-6
- STP and IEEE 802.1Q Trunks, page 15-12

STP Overview

STP is a Layer 2 link management protocol that provides path redundancy while preventing undesirable loops in the network. For a Layer 2 Ethernet network to function properly, only one active path can exist between any two stations. STP operation is transparent to end stations, which cannot detect whether they are connected to a single LAN segment or a switched LAN of multiple segments.

Catalyst 6500 series switches use STP (the IEEE 802.1D bridge protocol) on all VLANs. By default, a single instance of STP runs on each configured VLAN (provided you do not manually disable STP). You can enable and disable STP on a per-VLAN basis.

When you create fault-tolerant internetworks, you must have a loop-free path between all nodes in a network. The STP algorithm calculates the best loop-free path throughout a switched Layer 2 network. Layer 2 LAN ports send and receive STP frames at regular intervals. Network devices do not forward these frames, but use the frames to construct a loop-free path.

Multiple active paths between end stations cause loops in the network. If a loop exists in the network, end stations might receive duplicate messages and network devices might learn end station MAC addresses on multiple Layer 2 LAN ports. These conditions result in an unstable network.

STP defines a tree with a root bridge and a loop-free path from the root to all network devices in the Layer 2 network. STP forces redundant data paths into a standby (blocked) state. If a network segment in the spanning tree fails and a redundant path exists, the STP algorithm recalculates the spanning tree topology and activates the standby path.

When two Layer 2 LAN ports on a network device are part of a loop, the STP port priority and port path cost setting determine which port is put in the forwarding state and which port is put in the blocking state. The STP port priority value represents the location of a port in the network topology and how well located it is to pass traffic. The STP port path cost value represents media speed.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls 867
Doc: 3702

16.919

These sections describe Multiple Spanning Tree (MST):

- IEEE 802.1s MST Overview, page 15-15
- MST-to-PVST Interoperability, page 15-16
- Common Spanning Tree, page 15-18
- MST Instances, page 15-18
- MST Configuration Parameters, page 15-18
- MST Regions, page 15-19
- Message Age and Hop Count, page 15-20
- Default STP Configuration, page 15-21

IEEE 802.1s MST Overview

Releases 12.1(11b)EX and later releases support MST. MST in this release is based on the draft version of the IEEE standard. 802.1s for MST is an amendment to 802.1Q. MST extends the IEEE 802.1w rapid spanning tree (RST) algorithm to multiple spanning trees. This extension provides both rapid convergence and load balancing in a VLAN environment. MST converges faster than PVST+. MST is backward compatible with 802.1D STP, 802.1w (rapid spanning tree protocol [RSTP]), and the Cisco PVST+ architecture.

MST allows you to build multiple spanning trees over trunks. You can group and associate VLANs to spanning tree instances. Each instance can have a topology independent of other spanning tree instances. This new architecture provides multiple forwarding paths for data traffic and enables load balancing. Network fault tolerance is improved because a failure in one instance (forwarding path) does not affect other instances (forwarding paths).

In large networks, you can more easily administer the network and use redundant paths by locating different VLAN and spanning tree instance assignments in different parts of the network. A spanning tree instance can exist only on bridges that have compatible VLAN instance assignments. You must configure a set of bridges with the same MST configuration information, which allows them to participate in a specific set of spanning tree instances. Interconnected bridges that have the same MST configuration are referred to as an *MST region*.

MST uses the modified RSTP version called the Multiple Spanning Tree Protocol (MSTP). The MST feature has these characteristics:

- MST runs a variant of spanning tree called internal spanning tree (IST). IST augments the common spanning tree (CST) information with internal information about the MST region. The MST region appears as a single bridge to adjacent single spanning tree (SST) and MST regions.
- A bridge running MST provides interoperability with single spanning tree bridges as follows:
  - MST bridges run IST, which augments the common spanning tree (CST) information with internal information about the MST region.
  - IST connects all the MST bridges in the region and appears as a subtree in the CST that includes the whole bridged domain. The MST region appears as a virtual bridge to adjacent SST bridges and MST regions.
  - The common and internal spanning tree (CIST) is the collection of ISTs in each MST region, the CST that interconnects the MST regions, and the SST bridges. CIST is the same as an IST inside an MST region and the same as CST outside an MST region. The STP, RSTP, and MSTP together elect a single bridge as the root of the CIST.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 15-15
Nº Doc: 3702

ANEXO (34)

16.918

Configuring Local SPAN and RSPAN

This chapter describes how to configure local Switched Port Analyzer (SPAN) and remote SPAN (RSPAN) on the Catalyst 6500 series switches. The Catalyst 6500 series switches support RSPAN with Release 12.1(13)E and later releases.

This chapter consists of these sections:

- Understanding How Local SPAN and RSPAN Work, page 34-1
- Local SPAN and RSPAN Configuration Guidelines and Restrictions, page 34-5
- Configuring Local SPAN and RSPAN, page 34-8

Note For complete syntax and usage information for the commands used in this chapter, refer to the *Catalyst 6500 Series Switch Cisco IOS Command Reference* publication.

Understanding How Local SPAN and RSPAN Work

These sections describe how local SPAN and RSPAN work:

- Local SPAN and RSPAN Overview, page 34-1
- Local SPAN and RSPAN Sessions, page 34-3
- Monitored Traffic, page 34-4
- SPAN Sources, page 34-4
- Destination Ports, page 34-5

Local SPAN and RSPAN Overview

Local SPAN and RSPAN both select network traffic to send to a network analyzer such as a SwitchProbe device or other Remote Monitoring (RMON) probe. SPAN does not affect the switching of network traffic on source ports or VLANs. SPAN sends a copy of the packets received or transmitted by the source ports and VLANs to the destination port. You must dedicate the destination port for SPAN use.

These sections provide an overview of local SPAN and RSPAN:

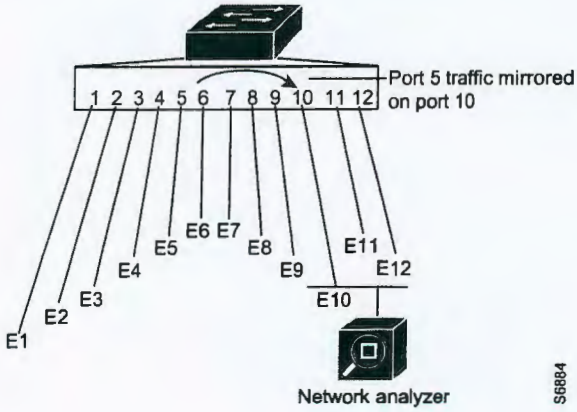
- Local SPAN Overview, page 34-2
- RSPAN Overview, page 34-3

RQS nº 03/2005 - CN - CPMI - CORREIOS
869
Fls Nº 34-1
3702
Doc:

Local SPAN Overview

Local SPAN supports source ports, source VLANs, and destination ports on the same Catalyst 6500 series switch. Local SPAN copies traffic from one or more source ports in any VLAN or from one or more VLANs to a destination port for analysis (see Figure 34-1). For example, as shown in Figure 34-1, all traffic on Ethernet port 5 (the source port) is copied to Ethernet port 10. A network analyzer on Ethernet port 10 receives all network traffic from Ethernet port 5 without being physically attached to Ethernet port 5.

Figure 34-1 Example SPAN Configuration



RQS nº 03/2005 - CN - CPMI - CORREIOS
870
FIS Nº 3702

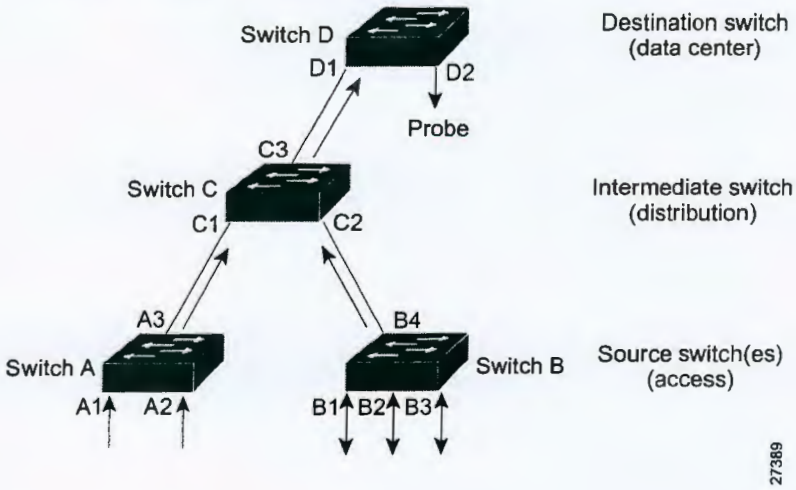
RSPAN Overview

RSPAN supports source ports, source VLANs, and destination ports on different switches, which provides remote monitoring of multiple switches across your network (see Figure 34-2). The traffic for each RSPAN session is carried over a user-specified RSPAN VLAN that is dedicated for that RSPAN session in all participating switches.

The RSPAN source ports can be trunks carrying the RSPAN VLAN. Local SPAN and RSPAN do not monitor the RSPAN traffic in the RSPAN VLAN seen on a source trunk.

The RSPAN traffic from the source ports or source VLANs is switched to the RSPAN VLAN and then forwarded to destination ports, which are in the RSPAN VLAN. The sources (ports or VLANs) in an RSPAN session can be different on different source switches but must be the same for all sources on each RSPAN source switch. Each RSPAN source switch must have either ports or VLANs as RSPAN sources.

Figure 34-2 RSPAN Configuration



Local SPAN and RSPAN Sessions

SPAN sessions (local or remote) allow you to monitor traffic on one or more ports, or one or more VLANs, and send the monitored traffic to one or more destination ports.

A local SPAN session is an association of a set of source ports and source VLANs with one or more destination ports. You configure a local SPAN session on a single network device. Local SPAN does not have separate source and destination sessions.

RSPAN consists of an RSPAN source session, an RSPAN VLAN, and an RSPAN destination session. You separately configure RSPAN source sessions and destination sessions on different network devices. To configure an RSPAN source session on one network device, you associate a set of source ports and VLANs with an RSPAN VLAN. To configure an RSPAN destination session on another device, you associate the destination port with the RSPAN VLAN.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 871
3702

Monitored Traffic

These sections describe the traffic that SPAN (local or remote) can monitor:

- Monitored Traffic Direction, page 34-4
- Monitored Traffic Type, page 34-4
- Duplicate Traffic, page 34-4

Monitored Traffic Direction

You can configure SPAN sessions to monitor ingress network traffic (called ingress SPAN), or to monitor egress network traffic (called egress SPAN), or to monitor traffic flowing in both directions.

Ingress SPAN copies network traffic received by the source ports and VLANs for analysis at the destination port. Egress SPAN copies network traffic transmitted from the source ports and VLANs. When you enter the **both** keyword, SPAN copies the network traffic received and transmitted by the source ports and VLANs to the destination port.

Monitored Traffic Type

By default, local SPAN monitors all network traffic, including multicast and bridge protocol data unit (BPDU) frames. RSPAN does not support BPDU monitoring.

Duplicate Traffic

In some configurations, SPAN sends multiple copies of the same source traffic to the destination port. For example, in a configuration with a bidirectional SPAN session (both ingress and egress) for two SPAN sources, called s1 and s2, to a SPAN destination port, called d1, if a packet enters the switch through s1 and is sent for egress from the switch to s2, ingress SPAN at s1 sends a copy of the packet to SPAN destination d1 and egress SPAN at s2 sends a copy of the packet to SPAN destination d1. If the packet was Layer 2 switched from s1 to s2, both SPAN packets would be the same. If the packet was Layer 3 switched from s1 to s2, the Layer-3 rewrite would alter the source and destination Layer 2 addresses, in which case the SPAN packets would be different.

SPAN Sources

These sections describe local SPAN and RSPAN sources:

- Source Ports, page 34-4
- Source VLANs, page 34-5

Source Ports

A source port is a port monitored for network traffic analysis. You can configure both switched and routed ports as SPAN source ports. SPAN can monitor one or more source ports in a single SPAN session. You can configure source ports in any VLAN. Trunk ports can be configured as source ports and mixed with nontrunk source ports, but SPAN does not copy the encapsulation from a source trunk port.

RQS nº 03/2005 - CN - CPMI - CORREIOS
872
Fls Nº
Doc 3702

16-915

Source VLANs

A source VLAN is a VLAN monitored for network traffic analysis. VLAN-based SPAN (VSPAN) uses a VLAN as the SPAN source. All the ports in the source VLANs become source ports.

Destination Ports

A destination port is a Layer 2 or Layer 3 LAN port to which SPAN sends traffic for analysis.

When you configure a port as a SPAN destination port, it can no longer receive any traffic. When you configure a port as a SPAN destination port, the port is dedicated for use only by the SPAN feature. A SPAN destination port does not forward any traffic except that required for the SPAN session.

With Release 12.1(13)E and later releases, you can configure trunk ports as destination ports, which allows destination trunk ports to transmit encapsulated traffic. With earlier releases, trunk ports stop trunking when you configure them as a destination port.

Local SPAN and RSPAN Configuration Guidelines and Restrictions

These sections describe local SPAN and RSPAN configuration guidelines and restrictions:

- Local SPAN and RSPAN Session Limits, page 34-5
- Local SPAN and RSPAN Source and Destination Limits, page 34-6
- Local SPAN and RSPAN Guidelines and Restrictions, page 34-6
- VSPAN Guidelines and Restrictions, page 34-7
- RSPAN Guidelines and Restrictions, page 34-7

Note

- Release 12.1(13)E and later releases support RSPAN.
- Ports on the WS-X6548-GE-TX and WS-X6548V-GE-TX switching modules cannot be ingress SPAN sources when the switch is operating in truncated mode.

Local SPAN and RSPAN Session Limits

These are the local SPAN and RSPAN session limits:

Total Sessions per Switch	Local SPAN Sessions	RSPAN Source Sessions	RSPAN Destination Sessions
66	2 (ingress or egress or both)	0	64
	1 ingress	1 (ingress or egress or both)	
	1 or 2 egress	0	

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 873
3702
Doc:

16.914

Local SPAN and RSPAN Source and Destination Limits

These are the local SPAN and RSPAN source and destination limits:

Sources and Destinations	Local SPAN Sessions	RSPAN Source Sessions	RSPAN Destination Sessions
Egress sources	1 (0 with a remote SPAN source session configured)	1 (0 with a local SPAN egress source session configured)	1 RSPAN VLAN
Ingress sources	64	64	
Destinations per session	64	1 RSPAN VLAN	64

Local SPAN and RSPAN Guidelines and Restrictions

These guidelines and restrictions apply to both local SPAN and RSPAN:

- You need a network analyzer to monitor destination ports.
- You can configure both Layer 2 LAN ports (LAN ports configured with the **switchport** command) and Layer 3 LAN ports (LAN ports not configured with the **switchport** command) as sources or destinations.
- With Release 12.1(13)E and later releases, you can configure destination ports as trunks to capture tagged traffic. With earlier releases, if you configure a trunk port as a destination port, SPAN suspends trunking on the port.
- A port specified as a destination port in one SPAN session cannot be a destination port for another SPAN session.
- A port configured as a destination port cannot be configured as a source port.
- A port channel interface (an EtherChannel) can be a source.
  - With Release 12.1(13)E and later releases, you cannot configure active member ports of an EtherChannel as source ports. Inactive member ports of an EtherChannel can be configured as sources but they are put into the suspended state and carry no traffic.
  - With releases earlier than 12.1(13)E, if you configure a member port of an EtherChannel as a SPAN source port, it is put into the suspended state and carries no traffic.
- A port channel interface (an EtherChannel) cannot be a destination.
  - With Release 12.1(13)E and later releases, you cannot configure active member ports of an EtherChannel as destination ports. Inactive member ports of an EtherChannel can be configured as destinations but they are put into the suspended state and carry no traffic.
  - With releases earlier than 12.1(13)E, if you configure a member port of an EtherChannel as a SPAN destination port, it is put into the suspended state and carries no traffic.
- You cannot mix individual source ports and source VLANs within a single session.
- If you specify multiple ingress source ports, the ports can belong to different VLANs.
- You cannot mix source VLANs and filter VLANs within a session. You can have source VLANs or filter VLANs, but not both at the same time.
- When enabled, local SPAN or RSPAN uses any previously entered configuration.
- When you specify sources and do not specify a traffic direction (ingress, egress, or both), "both" is used by default.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
874
Fls Nº 78-14099-03 B0
3702
Doc:

16-913

- You cannot configure destination ports to receive ingress traffic.
- Destination ports never participate in any spanning tree instance. Local SPAN includes BPDUs in the monitored traffic, so any BPDUs seen on the destination port are from the source port. RSPAN does not support BPDU monitoring.
- All packets sent through the switch for transmission from a port configured as an egress source are copied to the destination port, including packets that do not exit the switch through the port because STP has put the port into the blocking state, or on a trunk port because STP has put the VLAN into the blocking state on the trunk port.

VSPAN Guidelines and Restrictions

These are VSPAN guidelines and restrictions:

- For VSPAN sessions with both ingress and egress configured, two packets are forwarded from the destination port if the packets get switched on the same VLAN (one as ingress traffic from the ingress port and one as egress traffic from the egress port).
- VSPAN only monitors traffic that leaves or enters Layer 2 ports in the VLAN.
  - If you configure a VLAN as an ingress source and traffic gets routed into the monitored VLAN, the routed traffic is not monitored because it never appears as ingress traffic entering a Layer 2 port in the VLAN.
  - If you configure a VLAN as an egress source and traffic gets routed out of the monitored VLAN, the routed traffic is not monitored because it never appears as egress traffic leaving a Layer 2 port in the VLAN.

RSPAN Guidelines and Restrictions

These are RSPAN guidelines and restrictions:

- Any network device that supports RSPAN VLANs can be an RSPAN intermediate device.
- Networks impose no limit on the number of RSPAN VLANs that the networks carry.
- Intermediate switches might impose limits on the number of RSPAN VLANs that they can support.
- You must configure the RSPAN VLANs in all source, intermediate, and destination network devices. If enabled, the VLAN Trunking Protocol (VTP) can propagate configuration of VLANs numbered 1 through 1024 as RSPAN VLANs. You must manually configure VLANs numbered higher than 1024 as RSPAN VLANs on all source, intermediate, and destination network devices.
- If you enable VTP and VTP pruning, RSPAN traffic is pruned in the trunks to prevent the unwanted flooding of RSPAN traffic across the network.
- RSPAN VLANs can be used only for RSPAN traffic.
- Do not configure a VLAN used to carry management traffic as an RSPAN VLAN.
- Do not assign access ports to RSPAN VLANs. RSPAN puts access ports in an RSPAN VLAN into the suspended state.
- Do not configure any ports in an RSPAN VLAN except those selected to carry RSPAN traffic.
- MAC address learning is disabled on the RSPAN VLAN.
- You can use an output access control list (ACL) on the RSPAN VLAN in the RSPAN source switch to filter the traffic sent to an RSPAN destination.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 875
Doc: 3702

- RSPAN does not support BPDU monitoring.
- Do not configure RSPAN VLANs as sources in VSPAN sessions.
- You can configure any VLAN as an RSPAN VLAN as long as all participating network devices support configuration of RSPAN VLANs and you use the same RSPAN VLAN for each RSPAN session in all participating network devices.
- Entering SPAN configuration commands does not clear previously configured SPAN parameters. You must enter the **no monitor session** command to clear configured SPAN parameters.

Configuring Local SPAN and RSPAN

These sections describe how to configure local SPAN and RSPAN:

- Local SPAN and RSPAN Configuration Overview, page 34-8
- Configuring RSPAN VLANs, page 34-8
- Configuring Local or RSPAN Sources, page 34-9
- Monitoring Specific Source VLANs on a Source Trunk Port, page 34-10
- Configuring Local SPAN and RSPAN Destinations, page 34-10
- Verifying the Configuration, page 34-12
- Configuration Examples, page 34-12

Note With Release 12.1(11b)E and later releases, when you are in configuration mode you can enter EXEC mode-level commands by entering the **do** keyword before the EXEC mode-level command.

Local SPAN and RSPAN Configuration Overview

To configure a local SPAN session, use the same session number for the sources and the destination ports.

To configure an RSPAN source session, use the same session number for a source and a destination RSPAN VLAN.

To configure an RSPAN destination session, use the same session number for a source RSPAN VLAN and a destination port.

Configuring RSPAN VLANs

To configure a VLAN as an RSPAN VLAN, perform this task:

	Command	Purpose
Step 1	`Router(config)# vlan` *vlan_ID*`{[-`*vlan_ID*`]|[,`*vlan_ID*`]}`	Creates or modifies an Ethernet VLAN, a range of Ethernet VLANs, or several Ethernet VLANs specified in a comma-separated list (do not enter space characters).

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 876
Nº 3702
Doc:

	Command	Purpose
Step 2	`Router(config-vlan)# remote-span`	Configures the VLAN as an RSPAN VLAN.
	`Router(config-vlan)# no remote-span`	Clears the RSPAN VLAN configuration.
Step 3	`Router(config-vlan)# end`	Updates the VLAN database and returns to privileged EXEC mode.

Configuring Local or RSPAN Sources

Note To configure an RSPAN source session, configure a source with an RSPAN VLAN as the destination. To configure an RSPAN destination session, configure an RSPAN VLAN as the source and a port as the destination.

To configure a local SPAN or RSPAN source, perform this task:

Command	Purpose
`Router(config)# monitor session` *session_number* `source {{`*single_interface* `|` *interface_list* `|` *interface_range* `|` *mixed_interface_list* `|` *single_vlan* `|` *vlan_list* `|` *vlan_range* `|` *mixed_vlan_list*`} [rx | tx | both]} | {remote vlan` *rspan_vlan_ID*`}}`	Configures the session number, the source ports, VLANs, or RSPAN VLAN, and the traffic direction to be monitored.
`Router(config)# no monitor session {`*session_number* `| all | local | range` *session_range*`[[,`*session_range*`],...] | remote}`	Clears the monitor configuration.

When configuring monitor sessions, note the following syntax information:

- *single_interface* is **interface** *type slot/port*; *type* is **ethernet**, **fastethernet**, **gigabitethernet**, or **tengigabitethernet**.
- *interface_list* is *single_interface* , *single_interface* , *single_interface* ...

Note In lists, you must enter a space before and after the comma. In ranges, you must enter a space before and after the dash.

- *interface_range* is **interface** *type slot/first_port - last_port*
- *mixed_interface_list* is, in any order, *single_interface* , *interface_range* , ...
- *single_vlan* is a the ID number of a single VLAN.
- *vlan_list* is *single_vlan* , *single_vlan* , *single_vlan* ...
- *vlan_range* is *first_vlan_ID - last_vlan_ID*
- *mixed_vlan_list* is, in any order, *single_vlan* , *vlan_range* , ...

When clearing monitor sessions, note the following syntax information:

- The **no monitor session** *number* command entered with no other parameters clears session *session_number*.
- *session_range* is *first_session_number-last_session_number*

RQS nº 03/2005 - CN - CPMI - CORREIOS
877
Fls Nº 34-9
Nº 3702
Doc

Note In the **no monitor session range** command, do not enter spaces before or after the dash. If you enter multiple ranges, do not enter spaces before or after the commas.

This example shows how to configure session 1 to monitor bidirectional traffic from Fast Ethernet port 5/1:

```
Router(config)# monitor session 1 source interface fastethernet 5/1
```

Monitoring Specific Source VLANs on a Source Trunk Port

To monitor specific VLANs when the local or RSPAN source is a trunk port, perform this task:

Command	Purpose
`Router(config)# monitor session session_number filter {vlan_ID} [, | -]`	Monitors specific VLANs when the source is a trunk port.
`Router(config)# no monitor session session_number filter {vlan_ID}`	Clears trunk source configuration.

This example shows how to monitor VLANs 1 through 5 and VLAN 9 when the source is a trunk port:

```
Router(config)# monitor session 2 filter vlan 1 - 5 , 9
```

Configuring Local SPAN and RSPAN Destinations

These sections describe how to configure local SPAN and RSPAN destinations:

- Configuring a Destination Port as an Unconditional Trunk, page 34-10
- Configuring a Local or RSPAN Destination, page 34-11

Configuring a Destination Port as an Unconditional Trunk

To tag the monitored traffic with Release 12.1(13)E and later releases, configure the destination port as a trunk.

To configure the destination port as a trunk, perform this task:

	Command	Purpose
Step 1	`Router(config)# interface type[1] slot/port`	Selects the LAN port to configure.
Step 2	`Router(config-if)# switchport`	Configures the LAN port for Layer 2 switching (required only if the LAN port is not already configured for Layer 2 switching).
Step 3	`Router(config-if)# switchport trunk encapsulation {isl | dot1q}`	Configures the encapsulation, which configures the Layer 2 switching port as either an ISL or 802.1Q trunk.
Step 4	`Router(config-if)# switchport mode trunk`	Configures the port to trunk unconditionally.
Step 5	`Router(config-if)# switchport nonegotiate`	Configures the trunk not to use DTP.

1. *type* = **ethernet**, **fastethernet**, **gigabitethernet**, or **tengigabitethernet**

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 878
Doc: 3702

This example shows how to configure a port as an unconditional IEEE 802.1q trunk:

```
Router(config)# interface fastethernet 5/12
Router(config-if)# switchport
Router(config-if)# switchport trunk encapsulation dot1q
Router(config-if)# switchport mode trunk
Router(config-if)# switchport nonegotiate
```

Configuring a Local or RSPAN Destination

Note To configure an RSPAN source session, configure a source with an RSPAN VLAN as the destination. To configure an RSPAN destination session, configure an RSPAN VLAN as the source and a port as the destination.

To configure a local or RSPAN destination, perform this task:

Command	Purpose
Router(config)# **monitor session** *session_number* **destination** {*single_interface* | *interface_list* | *interface_range* | *mixed_interface_list*} | {**remote vlan** *rspan_vlan_ID*}}	Configures the session number and the destination ports or RSPAN VLAN.
Router(config)# **no monitor session** {*session_number* | **all** | **local** | **range** *session_range*[[,*session_range*],...] | **remote**}	Clears the monitor configuration.

Note To tag the monitored traffic, you must configure the port to trunk unconditionally before you configure it as a destination (see the "Configuring a Destination Port as an Unconditional Trunk" section on page 34-10).

When configuring monitor sessions, note the following syntax information:

- *single_interface* is **interface** *type slot/port*; *type* is **ethernet**, **fastethernet**, **gigabitethernet**, or **tengigabitethernet**.
- *interface_list* is *single_interface* , *single_interface* , *single_interface* ...

  Note In lists, you must enter a space before and after the comma. In ranges, you must enter a space before and after the dash.

- *interface_range* is **interface** *type slot/first_port - last_port*
- *mixed_interface_list* is, in any order, *single_interface* , *interface_range* , ...

When clearing monitor sessions, note the following syntax information:

- Enter the **no monitor session** *number* command with no other parameters to clear session *session_number*.
- *session_range* is *first_session_number-last_session_number*

RQS nº 03/2005 - CN - CPMI - CORREIOS
879
Fls Nº
Doc: 3702

Note In the **no monitor session range** command, do not enter spaces before or after the dash. If you enter multiple ranges, do not enter spaces before or after the commas.

This example shows how to configure Fast Ethernet port 5/48 as the destination for SPAN session 1:

```
Router(config)# monitor session 1 destination interface fastethernet 5/48
```

Verifying the Configuration

This example shows how to verify the configuration of session 2:

```
Router# show monitor session 2
Session 2
------------
Type : Remote Source Session

Source Ports:
    RX Only:        Fa3/1
Dest RSPAN VLAN:    901
Router#
```

This example shows how to display the full details of session 2:

```
Router# show monitor session 2 detail
Session 2
------------
Type : Remote Source Session

Source Ports:
    RX Only:        Fa1/1-3
    TX Only:        None
    Both:           None
Source VLANs:
    RX Only:        None
    TX Only:        None
    Both:           None
Source RSPAN VLAN: None
Destination Ports: None
Filter VLANs:       None
Dest RSPAN VLAN:    901
```

Configuration Examples

This example shows how to configure RSPAN source session 2:

```
Router(config)# monitor session 2 source interface fastethernet1/1 - 3 rx
Router(config)# monitor session 2 destination remote vlan 901
```

This example shows how to clear the configuration for sessions 1 and 2:

```
Router(config)# no monitor session range 1-2
```

This example shows how to configure an RSPAN source session with multiple sources:

```
Router(config)# monitor session 2 source interface fastethernet 5/15 , 7/3 rx
Router(config)# monitor session 2 source interface gigabitethernet 1/2 tx
Router(config)# monitor session 2 source interface port-channel 102
Router(config)# monitor session 2 source filter vlan 2 - 3
Router(config)# monitor session 2 destination remote vlan 901
```

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1880
Doc: 3702

This example shows how to remove sources for a session:

```
Router(config)# no monitor session 2 source interface fastethernet 5/15 , 7/3
```

This example shows how to remove options for sources for a session:

```
Router(config)# no monitor session 2 source interface gigabitethernet 1/2
Router(config)# no monitor session 2 source interface port-channel 102 tx
```

This example shows how to remove VLAN filtering for a session:

```
Router(config)# no monitor session 2 filter vlan 3
```

This example shows how to configure an RSPAN destination session:

```
Router(config)# monitor session 8 source remote vlan 901
Router(config)# monitor session 8 destination interface fastethernet 1/2 , 2/3
```


RQS nº 03/2005 - CN - CPMI - CORREIOS
881
Fls Nº
Doc: 3702

RQS nº 03/2005 - CN - CPMI - CORREIOS
882
Fls Nº
Doc: 3702

ANEXO (35)

16.405
L

Configuring VLANs

This chapter describes how to configure VLANs on the Catalyst 6500 series switches.

Note For complete syntax and usage information for the commands used in this chapter, refer to the *Catalyst 6500 Series Switch Cisco IOS Command Reference* publication.

This chapter consists of these sections:

- Understanding How VLANs Work, page 9-1
- VLAN Default Configuration, page 9-6
- VLAN Configuration Guidelines and Restrictions, page 9-8
- Configuring VLANs, page 9-8

Understanding How VLANs Work

The following sections describe how VLANs work:

- VLAN Overview, page 9-1
- VLAN Ranges, page 9-2
- Configurable VLAN Parameters, page 9-3
- Understanding Token Ring VLANs, page 9-3

VLAN Overview

A VLAN is a group of end stations with a common set of requirements, independent of physical location. VLANs have the same attributes as a physical LAN but allow you to group end stations even if they are not located physically on the same LAN segment.

VLANs are usually associated with IP subnetworks. For example, all the end stations in a particular IP subnet belong to the same VLAN. Traffic between VLANs must be routed. LAN port VLAN membership is assigned manually on an port-by-port basis.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 883
Doc: 3702

VLAN Ranges

Note You must enable the extended system ID to use 4096 VLANs (see the "Understanding the Bridge ID" section on page 15-3).

With Release 12.1(13)E and later releases, Catalyst 6500 series switches support 4096 VLANs in accordance with the IEEE 802.1Q standard. These VLANs are organized into several ranges; you use each range slightly differently. Some of these VLANs are propagated to other switches in the network when you use the VLAN Trunking Protocol (VTP). The extended-range VLANs are not propagated, so you must configure extended-range VLANs manually on each network device.

Table 9-1 describes the VLAN ranges.

Table 9-1 VLAN Ranges

VLANs	Range	Usage	Propagated by VTP
0, 4095	Reserved	For system use only. You cannot see or use these VLANs.	—
1	Normal	Cisco default. You can use this VLAN but you cannot delete it.	Yes
2–1001	Normal	For Ethernet VLANs; you can create, use, and delete these VLANs.	Yes
1002–1005	Normal	Cisco defaults for FDDI and Token Ring. You cannot delete VLANs 1002–1005.	Yes
1006–4094	Extended	For Ethernet VLANs only.	No

The following information applies to VLAN ranges:

- Layer 3 LAN ports, WAN interfaces and subinterfaces, and some software features use internal VLANs in the extended range. You cannot use an extended range VLAN that has been allocated for internal use.
- With Release 12.1(13)E and later releases, to display the VLANs used internally, enter the **show vlan internal usage** command. With earlier releases, enter the **show vlan internal usage** and **show cwan vlans** commands.
- With Release 12.1(13)E and later releases, you can configure ascending internal VLAN allocation (from 1006 and up) or descending internal VLAN allocation (from 4094 and down). In previous 12.1EX releases that support 4096 VLANs, internal VLANs are allocated from 1006 and up.
- Switches running the Catalyst operating system do not support configuration of VLANs 1006–1024. If you configure VLANs 1006–1024, ensure that the VLANs do not extend to any switches running Catalyst software.
- You must enable the extended system ID to use extended range VLANs (see the "Understanding the Bridge ID" section on page 15-3).

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 884
Doc: 3702

16.903
L

Configurable VLAN Parameters

Note

- Ethernet VLAN 1 uses only default values.
- Except for the VLAN name, Ethernet VLANs 1006 through 4094 use only default values.
- With Release 12.1(13)E and later releases, you can configure the VLAN name for Ethernet VLANs 1006 through 4094.

You can configure the following parameters for VLANs 2 through 1001:

- VLAN name
- VLAN type (Ethernet, FDDI, FDDI network entity title [NET], TrBRF, or TrCRF)
- VLAN state (active or suspended)
- Security Association Identifier (SAID)
- Bridge identification number for TrBRF VLANs
- Ring number for FDDI and TrCRF VLANs
- Parent VLAN number for TrCRF VLANs
- Spanning Tree Protocol (STP) type for TrCRF VLANs

Understanding Token Ring VLANs

The following section describes the two Token Ring VLAN types supported on network devices running VTP version 2:

- Token Ring TrBRF VLANs, page 9-3
- Token Ring TrCRF VLANs, page 9-4

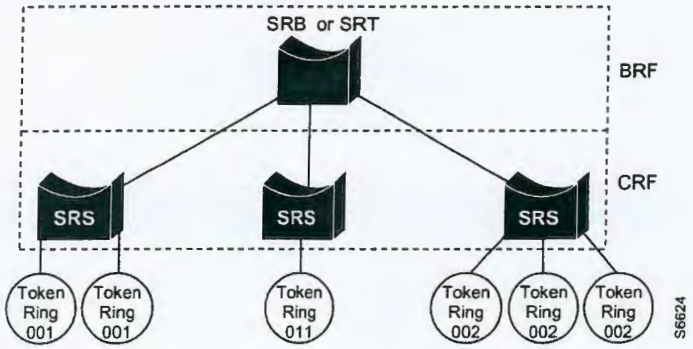
Note Catalyst 6500 series switches do not support Inter-Switch Link (ISL)-encapsulated Token Ring frames. When a Catalyst 6500 series switch is configured as a VTP server, you can configure Token Ring VLANs from the switch.

Token Ring TrBRF VLANs

Token Ring Bridge Relay Function (TrBRF) VLANs interconnect multiple Token Ring Concentrator Relay Function (TrCRF) VLANs in a switched Token Ring network (see Figure 9-1). The TrBRF can be extended across network devices interconnected with trunk links. The connection between the TrCRF and the TrBRF is referred to as a *logical port*.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 885
Doc: 3702

Figure 9-1 Interconnected Token Ring TrBRF and TrCRF VLANs



For source routing, the Catalyst 6500 series switch appears as a single bridge between the logical rings. The TrBRF can function as a source-route bridge (SRB) or a source-route transparent (SRT) bridge running either the IBM or IEEE STP. If an SRB is used, you can define duplicate MAC addresses on different logical rings.

The Token Ring software runs an instance of STP for each TrBRF VLAN and each TrCRF VLAN. For TrCRF VLANs, STP removes loops in the logical ring. For TrBRF VLANs, STP interacts with external bridges to remove loops from the bridge topology, similar to STP operation on Ethernet VLANs.

Caution Certain parent TrBRF STP and TrCRF bridge mode configurations can place the logical ports (the connection between the TrBRF and the TrCRF) of the TrBRF in a blocked state. For more information, see the "VLAN Configuration Guidelines and Restrictions" section on page 9-8.

To accommodate IBM System Network Architecture (SNA) traffic, you can use a combination of SRT and SRB modes. In a mixed mode, the TrBRF determines that some ports (logical ports connected to TrCRFs) operate in SRB mode while other ports operate in SRT mode

Token Ring TrCRF VLANs

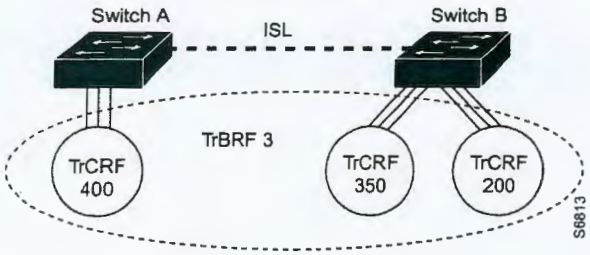
Token Ring Concentrator Relay Function (TrCRF) VLANs define port groups with the same logical ring number. You can configure two types of TrCRFs in your network: undistributed and backup.

TrCRFs typically are undistributed, which means each TrCRF is limited to the ports on a single network device. Multiple undistributed TrCRFs on the same or separate network devices can be associated with a single parent TrBRF (see Figure 9-2). The parent TrBRF acts as a multiport bridge, forwarding traffic between the undistributed TrCRFs.

Note To pass data between rings located on separate network devices, you can associate the rings to the same TrBRF and configure the TrBRF for an SRB.

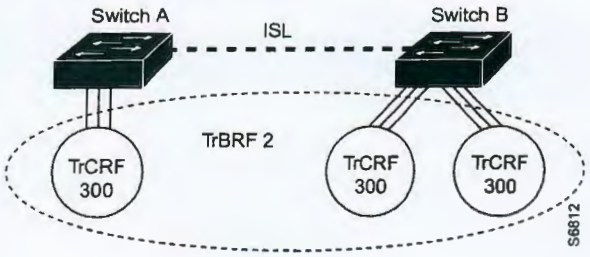
RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 886
Doc 3702

Figure 9-2 Undistributed TrCRFs



By default, Token Ring ports are associated with the default TrCRF (VLAN 1003, trcrf-default), which has the default TrBRF (VLAN 1005, trbrf-default) as its parent. In this configuration, a distributed TrCRF is possible (see Figure 9-3), and traffic is passed between the default TrCRFs located on separate network devices if the network devices are connected through an ISL trunk.

Figure 9-3 Distributed TrCRF



Within a TrCRF, source-route switching forwards frames based on either MAC addresses or route descriptors. The entire VLAN can operate as a single ring, with frames switched between ports within a single TrCRF.

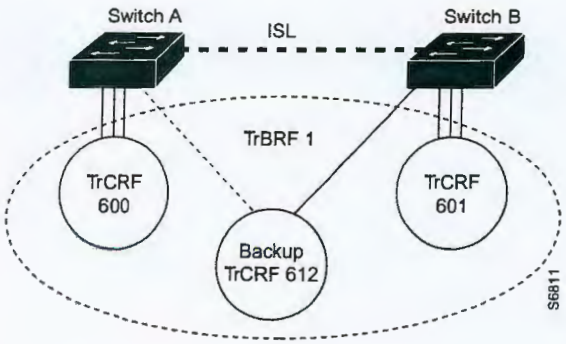
You can specify the maximum hop count for All-Routes and Spanning Tree Explorer frames for each TrCRF. When you specify the maximum hop count, you limit the maximum number of hops an explorer is allowed to traverse. If a port determines that the explorer frame it is receiving has traversed more than the number of hops specified, it does not forward the frame. The TrCRF determines the number of hops an explorer has traversed by the number of bridge hops in the route information field.

If the ISL connection between network devices fails, you can use a backup TrCRF to configure an alternate route for traffic between undistributed TrCRFs. Only one backup TrCRF for a TrBRF is allowed, and only one port per network device can belong to a backup TrCRF.

If the ISL connection between the network devices fails, the port in the backup TrCRF on each affected network device automatically becomes active, rerouting traffic between the undistributed TrCRFs through the backup TrCRF. When the ISL connection is reestablished, all but one port in the backup TrCRF is disabled. Figure 9-4 illustrates the backup TrCRF.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
887
Fls Nº 9-5
Doc: 3702

Figure 9-4 Backup TrCRF



VLAN Default Configuration

Tables 9-2 through 9-6 show the default configurations for the different VLAN media types.

Table 9-2 Ethernet VLAN Defaults and Ranges

Parameter	Default	Range
VLAN ID	1	1–4094
VLAN name	"default" for VLAN 1 "VLAN*vlan_ID*" for other Ethernet VLANs	—
802.10 SAID	10*vlan_ID*	100001–104094
MTU size	1500	1500–18190
Translational bridge 1	0	0–1005
Translational bridge 2	0	0–1005
VLAN state	active	active, suspend
Pruning eligibility	VLANs 2–1001 are pruning eligible; VLANs 1006–4094 are not pruning eligible.	—

Table 9-3 FDDI VLAN Defaults and Ranges

Parameter	Default	Range
VLAN ID	1002	1–1005
VLAN name	"fddi-default"	—
802.10 SAID	101002	1–4294967294
MTU size	1500	1500–18190
Ring number	0	1–4095
Parent VLAN	0	0–1005
Translational bridge 1	0	0–1005

ECT-14099-03
Nº Doc: 3702

16-849

Table 9-3 FDDI VLAN Defaults and Ranges (continued)

Parameter	Default	Range
Translational bridge 2	0	0–1005
VLAN state	active	active, suspend

Table 9-4 Token Ring (TrCRF) VLAN Defaults and Ranges

Parameter	Default	Range
VLAN ID	1003	1–1005
VLAN name	"token-ring-default"	—
802.10 SAID	101003	1–4294967294
Ring Number	0	1–4095
MTU size	VTPv1 default 1500 VTPv2 default 4472	1500–18190
Translational bridge 1	0	0–1005
Translational bridge 2	0	0–1005
VLAN state	active	active, suspend
Bridge mode	srb	srb, srt
ARE max hops	7	0–13
STE max hops	7	0–13
Backup CRF	disabled	disable; enable

Table 9-5 FDDI-Net VLAN Defaults and Ranges

Parameter	Default	Range
VLAN ID	1004	1–1005
VLAN name	"fddinet-default"	—
802.10 SAID	101004	1–4294967294
MTU size	1500	1500–18190
Bridge number	1	0–15
STP type	ieee	auto, ibm, ieee
VLAN state	active	active, suspend

Table 9-6 Token Ring (TrBRF) VLAN Defaults and Ranges

Parameter	Default	Range
VLAN ID	1005	1–1005
VLAN name	"trnet-default"	—
802.10 SAID	101005	1–4294967294

RQS nº 03/2005 - CN - CPMI - CORREIOS
889
Fls Nº
Doc: 3702

Table 9-6 Token Ring (TrBRF) VLAN Defaults and Ranges (continued)

Parameter	Default	Range
MTU size	VTPv1 1500; VTPv2 4472	1500–18190
Bridge number	1	0–15
STP type	ibm	auto, ibm, ieee
VLAN state	active	active, suspend

VLAN Configuration Guidelines and Restrictions

Follow these guidelines and restrictions when creating and modifying VLANs in your network:

- RPR+ redundancy (see Chapter 5, "Configuring RPR and RPR+ Supervisor Engine Redundancy") does not support a configuration entered in VLAN database mode. Use global configuration mode with RPR+ redundancy.
- You can configure extended-range VLANs only in global configuration mode. You cannot configure extended-range VLANs in VLAN database mode. See the "VLAN Configuration Options" section on page 9-9.
- Before you can create a VLAN, the Catalyst 6500 series switch must be in VTP server mode or VTP transparent mode. For information on configuring VTP, see Chapter 8, "Configuring VTP."
- The VLAN configuration is stored in the vlan.dat file, which is stored in nonvolatile memory. You can cause inconsistency in the VLAN database if you manually delete the vlan.dat file. If you want to modify the VLAN configuration or VTP, use the commands described in this guide and in the *Catalyst 6500 Series Switch Cisco IOS Command Reference* publication.
- To do a complete backup of your configuration, include the vlan.dat file in the backup.
- The Cisco IOS **end** command is not supported in VLAN database mode.
- You cannot enter **Ctrl-Z** to exit VLAN database mode.
- Catalyst 6500 series switches do not support Token Ring or FDDI media. The switch does not forward FDDI, FDDI-Net, TrCRF, or TrBRF traffic, but it can propagate the VLAN configuration through VTP.
- When a Catalyst 6500 series switch is configured as a VTP server, you can configure FDDI and Token Ring VLANs from the switch.
- You must configure a TrBRF before you configure the TrCRF (the parent TrBRF VLAN you specify must exist).
- In a Token Ring environment, the logical interfaces (the connection between the TrBRF and the TrCRF) of the TrBRF are placed in a blocked state if either of these conditions exists:
  - The TrBRF is running the IBM STP, and the TrCRF is in SRT mode.
  - The TrBRF is running the IEEE STP, and the TrCRF is in SRB mode.

RQS nº 03/2005 - CN - CPMI - CORREIOS
890
Nº 3702

Configuring VLANs

These sections describe how to configure VLANs:

- VLAN Configuration Options, page 9-9
- Creating or Modifying an Ethernet VLAN, page 9-10
- Assigning a Layer 2 LAN Interface to a VLAN, page 9-12
- Configuring the Internal VLAN Allocation Policy, page 9-12
- Mapping 802.1Q VLANs to ISL VLANs, page 9-12

Note

- With releases 12.1(11b)E and later, when you are in configuration mode you can enter EXEC mode commands by entering the **do** keyword before the EXEC mode command.
- VLANs support a number of parameters that are not discussed in detail in this section. For complete information, refer to the *Catalyst 6500 Series Switch Cisco IOS Command Reference* publication.

VLAN Configuration Options

These sections describe the VLAN configuration options:

- VLAN Configuration in Global Configuration Mode, page 9-9
- VLAN Configuration in VLAN Database Mode, page 9-9

VLAN Configuration in Global Configuration Mode

Note Releases 12.1(11b)E and later support VLAN configuration in global configuration mode.

If the switch is in VTP server or transparent mode (see the "Configuring VTP" section on page 8-6), you can configure VLANs in global and config-vlan configuration modes. When you configure VLANs in global and config-vlan configuration modes, the VLAN configuration is saved in the vlan.dat files. To display the VLAN configuration, enter the **show vlan** command.

If the switch is in VLAN transparent mode, use the copy **running-config startup-config** command to save the VLAN configuration to the startup-config file. After you save the running configuration as the startup configuration, use the **show running-config** and **show startup-config** commands to display the VLAN configuration.

Note

- When the switch boots, if the VTP domain name and VTP mode in the startup-config and vlan.dat files do not match, the switch uses the configuration in the vlan.dat file.
- You can configure extended-range VLANs only in global configuration mode. You cannot configure extended-range VLANs in VLAN database mode.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº [redacted] 891
Fls - Nº 3702
Doc

VLAN Configuration in VLAN Database Mode

Note You cannot configure extended-range VLANs in VLAN database mode. You can configure extended-range VLANs only in global configuration mode. RPR+ redundancy does not support configuration entered in VLAN database mode. Use global configuration mode with RPR+ redundancy.

If the switch is in VTP server or transparent mode, you can configure VLANs in the VLAN database mode. When you configure VLANs in VLAN database mode, the VLAN configuration is saved in the vlan.dat files. To display the VLAN configuration, enter the **show vlan** command.

You use the interface configuration command mode to define the port membership mode and add and remove ports from a VLAN. The results of these commands are written to the running-config file, and you can display the file by entering the **show running-config** command.

Creating or Modifying an Ethernet VLAN

User-configured VLANs have unique IDs from 1 to 4094, except for reserved VLANs (see Table 9-1 on page 9-2). Enter the **vlan** command with an unused ID to create a VLAN. Enter the **vlan** command for an existing VLAN to modify the VLAN (you cannot modify an existing VLAN that is being used by a Layer 3 port or a software feature).

See the "VLAN Default Configuration" section on page 9-6 for the list of default parameters that are assigned when you create a VLAN. If you do not specify the VLAN type with the **media** keyword, the VLAN is an Ethernet VLAN.

To create or modify a VLAN, perform this task:

	Command	Purpose

Step 1	`Router# configure terminal`
	or
	`Router# vlan database`
		Enters VLAN configuration mode.

Step 2	`Router(config)# vlan` *vlan_ID*`{[-`*vlan_ID*`]|[,`*vlan_ID*`]}`
	`Router(config-vlan)#`
	or
	`Router(vlan)# vlan` *vlan_ID*
		Creates or modifies an Ethernet VLAN, a range of Ethernet VLANs, or several Ethernet VLANs specified in a comma-separated list (do not enter space characters).

	`Router(config)# no vlan` *vlan_ID* `Router(config-vlan)#` or `Router(vlan)# no vlan` *vlan_ID*	Deletes a VLAN.

Step 3	`Router(config-vlan)# end`
	or
	`Router(vlan)# exit`
		Updates the VLAN database and returns to privileged EXEC mode.

Step 4	`Router# show vlan [id | name]` *vlan*	Verifies the VLAN configuration.

When you create or modify an Ethernet VLAN, note the following syntax information:

- Releases 12.1(11b)E and later support VLAN configuration in global configuration mode.
- Releases 12.1(13)E and later support extended-range VLANs.
- RPR+ redundancy does not support a configuration entered in VLAN database mode. Use global configuration mode with RPR+ redundancy.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 892
Nº Doc 3702

- Because Layer 3 ports and some software features require internal VLANs allocated from 1006 and up, configure extended-range VLANs starting with 4094.
- You can configure extended-range VLANs only in global configuration mode. You cannot configure extended-range VLANs in VLAN database mode.
- Layer 3 ports and some software features use extended-range VLANs. If the VLAN you are trying to create or modify is being used by a Layer 3 port or a software feature, the switch displays a message and does not modify the VLAN configuration.

When deleting VLANs, note the following syntax information:

- You cannot delete the default VLANs for the different media types: Ethernet VLAN 1 and FDDI or Token Ring VLANs 1002 to 1005.
- When you delete a VLAN, any LAN ports configured as access ports assigned to that VLAN become inactive. The ports remain associated with the VLAN (and inactive) until you assign them to a new VLAN.

This example shows how to create an Ethernet VLAN in global configuration mode and verify the configuration:

```
Router# configure terminal
Router(config)# vlan 3
Router(config-vlan)# end
Router# show vlan id 3

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------

3    VLAN0003                         active

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
3    enet  100003     1500  -      -      -        -    -        0      0

Primary Secondary Type              Interfaces
------- --------- ----------------- ------------------------------------------
```

This example shows how to create an Ethernet VLAN in VLAN database mode:

```
Router# vlan database
Router(vlan)# vlan 3
VLAN 3 added:
    Name: VLAN0003
Router(vlan)# exit
APPLY completed.
Exiting....
```

This example shows how to verify the configuration:

```
Router# show vlan name VLAN0003
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------

3    VLAN0003                         active

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- ------ ------
3    enet  100003     1500  -      -      -        -    0      0
Router#
```


RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 893
Nº Doc: 3702

Assigning a Layer 2 LAN Interface to a VLAN

A VLAN created in a management domain remains unused until you assign one or more LAN ports to the VLAN.

Note Make sure you assign LAN ports to a VLAN of the appropriate type. Assign Ethernet ports to Ethernet-type VLANs.

To assign one or more LAN ports to a VLAN, complete the procedures in the "Configuring LAN Interfaces for Layer 2 Switching" section on page 7-6.

Configuring the Internal VLAN Allocation Policy

Internal VLAN allocation policy is supported in Release 12.1(13)E and later releases. For more information about VLAN allocation, see the "VLAN Ranges" section on page 9-2.

Note The internal VLAN allocation policy is applied only following a reload.

To configure the internal VLAN allocation policy, perform this task:

	Command	Purpose
Step 1	`Router(config)# vlan internal allocation policy {ascending | descending}`	Configures the internal VLAN allocation policy.
	`Router(config)# no vlan internal allocation policy`	Returns to the default (ascending).
Step 2	`Router(config)# end`	Exits configuration mode.
Step 3	`Router# reload`	Applies the new internal VLAN allocation policy. **Caution** You do not need to enter the **reload** command immediately. Enter the **reload** command during a planned maintenance window.

When you configure the internal VLAN allocation policy, note the following syntax information:

- Enter the **ascending** keyword to allocate internal VLANs from 1006 and up.
- Enter the **descending** keyword to allocate internal VLAN from 4094 and down.

This example shows how to configure descending as the internal VLAN allocation policy:

```
Router# configure terminal
Router(config)# vlan internal allocation policy descending
```

Mapping 802.1Q VLANs to ISL VLANs

The valid range of user-configurable ISL VLANs is 1 through 1001 and 1006 through 4094. The valid range of VLANs specified in the IEEE 802.1Q standard is 1 to 4094. You can map 802.1Q VLAN numbers to ISL VLAN numbers.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 894
Nº 3702
Doc:

802.1Q VLANs in the range 1 through 1001 and 1006 through 4094 are automatically mapped to the corresponding ISL VLAN. 802.1Q VLAN numbers corresponding to reserved VLAN numbers must be mapped to an ISL VLAN in order to be recognized and forwarded by Cisco network devices.

These restrictions apply when mapping 802.1Q VLANs to ISL VLANs:

- You can configure up to eight 802.1Q-to-ISL VLAN mappings on the Catalyst 6500 series switch.
- You can only map 802.1Q VLANs to Ethernet-type ISL VLANs.
- Do not enter the native VLAN of any 802.1Q trunk in the mapping table.
- When you map an 802.1Q VLAN to an ISL VLAN, traffic on the 802.1Q VLAN corresponding to the mapped ISL VLAN is blocked. For example, if you map 802.1Q VLAN 1007 to ISL VLAN 200, traffic on 802.1Q VLAN 200 is blocked.
- VLAN mappings are local to each Catalyst 6500 series switch. Make sure you configure the same VLAN mappings on all appropriate network devices.

To map an 802.1Q VLAN to an ISL VLAN, perform this task:

	Command	Purpose
Step 1	`Router(config)# vlan mapping dot1q` *dot1q_vlan* `isl` *isl_vlan*	Maps an 802.1Q VLAN to an ISL Ethernet VLAN. The valid range for *dot1q_vlan* is 1001 to 4094. The valid range for *isl_vlan* is the same.
	`Router(config)# no vlan mapping dot1q {all |` *dot1q_vlan*`}`	Deletes the mapping.
Step 2	`Router(config)# end`	Exits configuration mode.
Step 3	`Router# show vlan`	Verifies the VLAN mapping.

This example shows how to map 802.1Q VLAN 1003 to ISL VLAN 200:

```
Router# configure terminal
Router(config)# vlan mapping dot1q 1003 isl 200
Router(config)# end
Router#
```

This example shows how to verify the configuration:

```
Router# show vlan
<...output truncated...>
802.1Q Trunk Remapped VLANs:
802.1Q VLAN     ISL VLAN
-----------     -----------
   1003           200
```


RQS nº 03/2005 - CI
CPMI - CORREIC
Fls 895
Doc: 3702

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 896
Nº 3702
Doc:

CISCO SERVICES MODULES

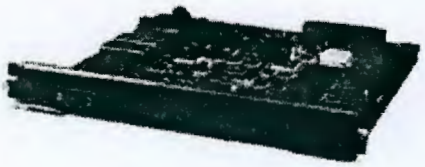
Cisco Content Switching Module

Downloads

Cisco Content Switching Mod

Data Sheet

Cisco Catalyst 6500 Series Content Switching Module



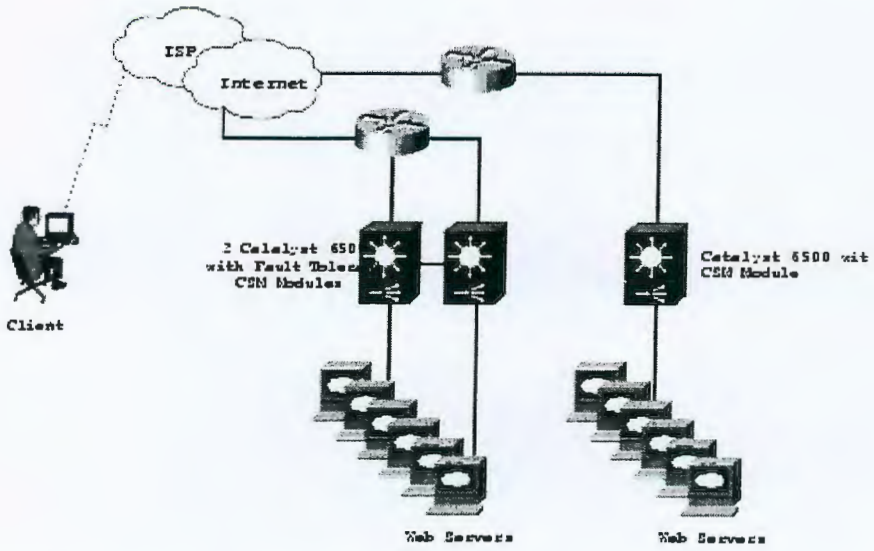
The Cisco Content Switching Module (CSM) is a Cisco Catalyst® 6500 line card that ba client traffic to farms of servers, firewalls, Secure Sockets Layer (SSL) devices, or virtu private network (VPN) termination devices. The Cisco CSM provides a high-performan effective load-balancing solution for enterprise and Internet service provider (ISP) netw The Cisco CSM meets the demands of high-speed content delivery networks, tracking sessions and server load conditions in real time and directing each session to the most appropriate server. Fault-tolerant Cisco CSM configurations maintain full state informat provide true hitless failover required for mission-critical functions.

The Cisco CSM provides the following key benefits (refer to Figure 1):

- Market-leading performance—The Cisco CSM establishes up to 165,000 Layer connections per second (depending on software version) and provides high-spe content switching while maintaining 1 million concurrent connections.
- Outstanding price/performance value for large data centers and ISPs—The Cis features a low connection cost and occupies a small footprint. It slides into a slo new or existing Cisco Catalyst 6500 and enables all ports in the Cisco Catalyst Layer 4-7 content switching.
- Multiple Cisco CSMs can be installed in the same Cisco Catalyst 6500.
- Ease of configuration—The Cisco CSM uses the same Cisco IOS® command-li interface (CLI) that is used to configure the Cisco Catalyst 6500 Switch.

Figure 1. The Cisco CSM

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 897
Doc: 3702



Content Switching Module Key Features

Firewall Load Balancing

The Cisco CSM allows you to scale firewall protection by distributing traffic across mult firewalls on a per-connection basis, while ensuring that all packets belonging to a partic connection go through the same firewall. Both stealth and regular firewalls are supporte

URL and Cookie-Based Load Balancing

The Cisco CSM allows full regular expression pattern matching for policies based on U cookies, and Hypertext Transfer Protocol (HTTP) header fields. The Cisco CSM suppo URL or cookie format—allowing it to load balance existing Web content without requirir URL/cookie format changes.

High Performance

The Cisco CSM performs up to 165,000 new Layer 4 TCP connection setups per secor depending on software version. These connections can be spread across 4096 virtual s (16,384 real servers) and all the ports in a Cisco Catalyst 6500, or they can be focused single port. This provides a benefit over competitors who use distributed architectures t require use of all the ports in order to gain maximum performance.

Network Configurations

The Cisco CSM supports many different network topology types. A Cisco CSM can ope a mixed bridged and routed configuration, allowing traffic to flow from the client side to server side on the same or on different IP subnets.

IP Protocol Support

The Cisco CSM accommodates a wide range of common IP protocols—including TCP User Datagram Protocol (UDP). Additionally, the Cisco CSM supports higher-level prot including HTTP, File Transfer Protocol (FTP), Telnet, Real-Time Streaming Protocol (R Domain Name System (DNS), and Simple Mail Transfer Protocol (SMTP).

User Session Stickiness

Whenever encryption or e-commerce is involved, it is important that the end user is consistently directed to the same server-that is, the server where the user's shopping c located or the encryption tunnel terminates. Cisco CSM User Session Stickiness provic ability to consistently bring users back to the same server-based on SSL session ID, IF address, cookie, or HTTP redirection.

Load-Balancing Algorithms

The Cisco CSM supports the following load-balancing algorithms:

- Round robin
- Weighted Round Robin
- Least connections
- Weighted least connections
- Source and/or destination IP hash (subnet mask also configurable)

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 898
Doc: 3702

16.890

- URL hashing

Quality of Service

Providing differentiated levels of service to end users is important when generating rev from content. The Cisco CSM takes advantage of the robust quality of service (QoS) of Cisco Catalyst 6500, enabling traffic differentiation as follows:

- Correctly prioritizes packets based on Layer 7 rules
- Directs users who are paying more for services to faster or less loaded servers

High Availability

The Cisco CSM continually monitors server and appliation availability using health mor probes, inband health monitoring, return code checking, and the Dynamic Feedback P (DFP). When a real server or gateway failure occurs, the Cisco CSM redirects traffic to different location. Servers can be added and removed without disrupting service—syst easily be scaled up or down.

Connection Redundancy

Optionally, two Cisco CSMs can be configured in a fault-tolerant configuration to share information about user sessions and provide connection redundancy. If the active Cisc fails, open connections are handled by the standby CSM without interruption, and user experience hitless failover—an important requirement for e-commerce sites and sites v encryption is used.

Global Server Load Balancing

The CSM offers multiple options for building a global or geographical load balanced environment. The CSM can act as an authoritative DNS and perform GSLB among geographically dispersed CSMs for the purposes of disaster recovery or for small GSLI environments with 2-4 locations. In addition, the CSM can report load information for it' IPs into the Global Site Selector (GSS), an appliance designed for advanced GSLB sc to 128 sites. With the many different GSLB options the CSM offers the ability to scale C capabilities as growth demands.

Configuration Limits

- Total virtual LANs (VLANs) (client and server): 256
- Virtual servers: 4000
- Server farms: 4000
- Real servers: 16,000
- Probes: 4000
- Access control list (ACL) items: 16,000

Performance Summary
Connections
1,000,000 concurrent TCP connections
165,000 connection setups per second—Layer 4
Throughput
Total combined throughput of 4 Gigabits per second (client to server and server to c
Cisco Catalyst Switch Platform Requirements
Cisco IOS Software only—Cisco Catalyst Operating System is not supported
Not fabric enabled—Functions as a bus-enabled line card

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 899
Doc: 3702

16.889
2

Multilayer Switch Feature Card (MSFC) or MSFC2
Physical Specifications
Occupies slot in the Cisco Catalyst 6500 chassis
Dimensions (H x W x D): 1.2 x 14.4 x 16 in. (3.0 x 35.6 x 40.6 cm)
Weight: 5 lb (2.27 kg)
Operating Environment
Operating temperature: 32 to 104.5°F (0 to 40°C)
Nonoperating temperature: -40 to 158°F (-40 to 70°C)
Operating relative humidity: 10 to 90% (noncondensing)
Nonoperating relative humidity: 5 to 95% (noncondensing)
Operating and nonoperating altitude: Sea level to 10,000 ft (3050m)
Agency Approvals
Emissions: FCC Part 15 (CFR 47) Class A, ICES-003 Class A, EN55022 Class A, CISPR22 Class A, AS NZS 3548 Class A
Safety: CE Marking according to UL 1950, CSA 22.2 No. 950, EN 60950, IEC 6095(001, AS/NZS 3260

Cisco Catalyst 6500 CSM Ordering Information

Product Number	Product Description
WS-X6066-SLB-APC	Cisco Catalyst 6500 Content Switching Module

© 1992-2003 Cisco Systems, Inc. All rights reserved. Important Notices, Privacy Statement, and Trademark

RQS nº 03/2005 - CN
CPMI - CORREIO
Fls Nº 900
Doc: 3702

COBRA TECNOLOGIA
Integradora de Soluções em TI e Serviços

16.888

ANEXO SWITCH TIPO 02
PARTE 1

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

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 901
Doc: 3702

SWITCH TIPO 2

ATRIBUTO	REQUISITOS DO EDITAL	ATRIBUTOS OFERTADOS	ATRIBUTOS OFERTADOS ADICIONALMENTE	CONFIRMA ATENDIMENTO (SIM / NÃO)	PÁGINA DA DOCUMENTAÇÃO TÉCNICA
1- Switch	Deverá ser do tipo Stackable (empilhável)	Conforme Edital	N/A	SIM	Anexo 14A - pág 1
	Deve permitir empilhamento de no mínimo 06 unidades por meio de links de no mínimo 1 Gbps redundantes, formando uma unidade gerenciável na rede através de um único endereço IP	Conforme Edital	Empilha até 09 unidades	SIM	Anexo 10 - pág. 2, 5, 7, 11 - Anexo 11 - pág. 1-1
	Deverão ser compatíveis com Rack 19¨ a ser fornecido	Conforme Edital	N/A	SIM	Anexo 14C (todas as páginas)
2- Interfaces Fast e Gigabit Ethernet	Possuir um mínimo de 48 portas 10/100TX , UTP, categoria 6, RJ-45 + 02 duas portas para interfaces de empilhamento e uplink	Conforme Edital	N/A	SIM	Anexo 10 - pág. 14, 17 - Anexo 11 - Anexo 10A
	Sinalização visual de funcionamento e de status das portas.	Conforme Edital	N/A	SIM	Anexo 10 - pág. 10 - Anexo 14 pág.10
	Compatível com os padrões IEEE 802.3u, IEEE 802.3Q e IEEE 802.3p.	Conforme Edital	N/A	SIM	Anexo 10 - pág. 14
	Deverá ser capaz de implementar espelhamento de tráfego de entrada e saída de interfaces ou de VLANs	Conforme Edital	N/A	SIM	Anexo 10B (todo o documento)
	Gerenciável via SNMP, com suporte a MIB II conforme RFC 1213 e 04 grupos de RMON.	Conforme Edital	N/A	SIM	Anexo 10 - pág. 1, 10, 13
	Controle de Broadcast Storm	Conforme Edital	N/A	SIM	Anexo 10 - pág. 7

RQS nº 03/2005 - CN
CPMI
CORREIOS
Fls Nº 902
Doc: 3702

16.887

3 - Gerais	Suporte a protocolo que permita limitar tráfego de IP Multicast.	Suporte a IGMP Snooping por hardware	N/A	SIM	Anexo 10 - pág. 5
	Deve implementar no mínimo 04 filas de prioridade em cada porta, permitindo a priorização do tráfego de rede e uma integração transparente de dadso, voz e vídeo através do protocolo IEEE 802.1p com CoS (Class of Services).	Conforme Edital	N/A	SIM	Anexo 10 - pág. 4, 14 Anexo 14 - pág 3
	Deverá possuir kits de fixação para instalação em racks de 19¨ e cabos de ligação lógica e elétrica necessária à instalação e perfeito funcionamento	Conforme Edital	N/A	SIM	Anexo 14C - pág. 2-9
	Deverão ser fornecidos todos os acessórios necessários à composição do empilhamento do Switch, tais como cabos, conectores e interfaces	Conforme Edital (Os cabos para empilhamento (50cm) são parte integrante das GBIC)	N/A	SIM	Anexo 14B - pág. 5 Ver propostas Técnica e Comercial
	Deverá implementar no mínimo, 200 VLANs no padrão IEEE 802.1Q, inclusive no empilhamento, isto é, deverá permitir o agrupamento em VLANs de portas de quaisquer Switches da pilha.	Conforme Edital	N/A	SIM	Anexo 14 - pág 4, 12 Anexo 14D (todas as páginas)
	Deverá implementar o protocolo STP (Spanning Tree Protocol) para cada VLAN configurada (uma sessão STP por grupo de portas)	Conforme Edital	N/A	SIM	Anexo 10 - pág. 2, 7, 8 - Anexo 14 - pág 7, 12 - Anexo 14E e Anexo 14F
	Deverá possui barramento para empilhamento igual ou superior a 1 Gbps	Conforme Edital	N/A	SIM	Anexo 10 - pág. 11

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 903
Doc. 3702

36.886

	A CONTRATADA deverá fornecer ferramentas que permitam o gerenciamento dos equipamentos e de todas as suas interfaces através de aplicação gráfica. Também deverão ser fornecidos servidores adicionais para instalação dessa gerência	Conforme Edital	N/A	SIM	Ver propostas Técnica e Comercial (Softwares de Gerenciamento)
4 - Fonte de Alimentação	Alimentação elétrica de acordo com a localidade onde serão instalados os equipamentos e frequência de 60Hz	Redundante interna ou externa independente. Frequência = 60Hz	N/A	SIM	Anexo 10 - pág. 16 - Anexo 13 - pág. 1, 3 e 4
	As fontes de alimentação deverão ser redundantes por fontes internas ou externas independentes com alimentação redundante de tal forma que, em caso de falha de uma das fontes por defeito ou por falta de alimentação elétrica em um dos 02 circuitos, o equipamento continue a funcionar sem prejuízo das aplicações	Conforme Edital	N/A	SIM	Anexo 13 - (todas as páginas)

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 904
Doc: 3702

1683
7

ANEXO (1º)

16-8
2

Cisco Systems

Data Sheet

Cisco Catalyst **2950** Series Switches—with Enhanced Image Software

Product Overview

Cisco® Catalyst® 2950 Series Switches are fixed-configuration, models that provide wire-speed Fast Ethernet and Gigabit Ethernet connectivity for small and midsize networks. The Cisco Catalyst 2950 Series is an affordable product line that brings intelligent services, such as enhanced security, high availability and advanced quality of service (QoS), to the network edge—while maintaining the simplicity of traditional LAN switching. When a Cisco Catalyst 2950 Switch is combined with a Cisco Catalyst 3550 Series Switch, the solution can enable IP routing from the edge to the core of the network.

Embedded in Cisco Catalyst 2950 Series switches is the Cisco Cluster Management Suite (CMS) Software, which allows users to simultaneously configure and troubleshoot multiple Cisco Catalyst desktop switches using a standard Web browser. In addition to CMS, Cisco Catalyst 2950 switches provide extensive management tools using Simple Network Management Protocol (SNMP) network management platforms such as CiscoWorks. With the newly launched Cisco Express Setup, users now have the option to set up the switch through a Web browser, eliminating the need for more complex terminal emulation programs and knowledge of the command-line interface (CLI). Cisco Express Setup reduces the cost of deployment by enabling less-skilled personnel to quickly and simply set up switches.

This product line offers two distinct sets of software features and a range of configurations to allow small, mid-sized, and enterprise branch offices to select the right combination for the network edge. The Standard Image (SI) software offers Cisco IOS® functionality for basic data, video, and voice services. For networks with requirements for additional security, advanced QoS and high availability, the Enhanced Image (EI) software delivers intelligent services such as rate limiting and security filtering for deployment at the network edge.

The Cisco Catalyst 2950 Series Switches consists of the following devices—which are only available with the EI Software for the Cisco Catalyst 2950 Series.

- *Cisco Catalyst 2950G-48*—48 10/100 ports and 2 Gigabit Interface Converter (GBIC)-based Gigabit Ethernet ports
- *Cisco Catalyst 2950G-24*—24 10/100 ports and 2 GBIC ports
- *Cisco Catalyst 2950G-24-DC*—24 10/100 ports, 2 GBIC ports, DC power
- *Cisco Catalyst 2950G-12*—12 10/100 ports and 2 GBIC ports

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 905
3702
Doc:

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

16.883

- *Cisco Catalyst 2950T-24*—24 10/100 ports and 2 fixed 10/100/1000BASE-T uplink ports
- *Cisco Catalyst 2950C-24*—24 10/100 ports and 2 fixed 100BASE-FX uplink ports

This complete set of switches offers network managers flexibility when selecting a migration path to Gigabit Ethernet. The two built-in Gigabit Ethernet ports on the Cisco Catalyst 2950G-12, 2950G-24, and 2950G-48 accommodate a range of GBIC transceivers, including the Cisco GigaStack® GBIC, 1000BASE-SX, 1000BASE-LX/LH, 1000BASE-ZX, 1000BASE-T, and CWDM GBICs. The dual GBIC-based Gigabit Ethernet implementation provides customers with tremendous deployment flexibility—allowing customers increased availability with the redundant uplinks. In sum, the configuration permits customers to implement one type of stacking and uplink configuration today, while preserving the option to migrate to another configuration in the future. High levels of stack resiliency can also be implemented by deploying dual redundant Gigabit Ethernet uplinks, a redundant GigaStack GBIC loopback cable, UplinkFast and CrossStack UplinkFast technologies for high-speed uplink and stack interconnection failover, and Per VLAN Spanning Tree Plus (PVST+) for uplink load balancing.

In addition, the Cisco Catalyst 2950T-24 offers small and mid-sized enterprises server connectivity and an easy migration path to Gigabit by using existing copper cabling infrastructure. Implementing Gigabit Ethernet over copper allows network managers to boost network performance and maximize infrastructure investments in Category 5 copper cabling.

Maximum power availability for a converged voice and data network is attainable when a Cisco Catalyst 2950 switch is combined with the Cisco Redundant Power System 300 (RPS 300) or 675 (RPS 675) for seamless protection against internal power supply failures and an uninterruptable power supply (UPS) system to safeguard against power outages.

Other Cisco Catalyst 2950 Series Switches

Cisco Catalyst 2950 Series with SI:

The Cisco Catalyst® 2950SX-24, 2950-24, and 2950-12 are also members of the Cisco Catalyst 2950 Series Switches. They are standalone, fixed-configuration, and managed 10/100 switches providing basic workgroup connectivity for small to mid-sized companies. These wire-speed desktop switches come with SI Software features and offer Cisco IOS® functionality for basic data, video, and voice services at the edge of the network.

Cisco Catalyst 2950 Long-Reach Ethernet (LRE) Switches:

- *Cisco Catalyst 2950ST-24-LRE*—24 LRE ports and 2 fixed 10/100/1000BASE-T ports and 2 Small Form-Factor Pluggable (SFP) ports (two of the four uplinks active at one time)
- *Cisco Catalyst 2950ST-8-LRE*—8 LRE ports and 2 fixed 10/100/1000BASE-T ports and 2 SFP ports (two of the four uplinks active at one time)

The Cisco Catalyst 2950 LRE solution delivers cost-effective, high-performance broadband access over existing phone wiring in enterprise campus environments and multitenant buildings (for example, hotels, apartment buildings, and office buildings). The Cisco Catalyst 2950 LRE switches come with the EI Software features enabling enterprise and service provider customers to extend intelligent services over traditional wiring (Category 1/2/3) to distances up to 5000 feet. Cisco is the only company with the breadth of technologies that allows customers to deliver intelligent network services across any combination of wired and wireless infrastructures. Refer to the Cisco Catalyst 2950 LRE Series Data Sheet for more information.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
906
Fls Nº
3702
Doc:

16-882
2

Intelligence in the Network

Networks of today are evolving to address four new developments at the network edge:

- Increase in desktop computing power
- Introduction of bandwidth-intensive applications
- Expansion of highly sensitive data on the network
- Presence of multiple device types, such as IP phones and wireless LAN access points

These new demands are contending for resources with many existing mission-critical applications. As a result, IT professionals must view the edge of the network as critical to effectively manage the delivery of information and applications.

As companies increasingly rely on networks as the strategic business infrastructure, it is more important than ever to ensure their high availability, security, scalability, and control. By adding Cisco intelligent functionality to the wiring closet, customers can now deploy network-wide intelligent services that address these requirements in a consistent way from the desktop to the core and through the WAN.

With Cisco Catalyst switches, Cisco enables companies to realize the full benefits of adding intelligent services into their networks. Deploying capabilities that make the network infrastructure highly available to accommodate time-critical needs, scalable to accommodate growth, secure enough to protect confidential information, and capable of differentiating and controlling traffic flows are key to further optimizing network operations.

Network Security Through Advanced Security Features

The Cisco Catalyst 2950 Series switches offer enhanced data security through a wide range of security features. These features allow customers to enhance LAN security with capabilities to secure network management traffic through the protection of passwords and configuration information; to provide options for network security based on users, ports and Media Access Control (MAC) addresses; and to enable more immediate reactions to intruder and hacker detection. The security enhancements are available free-of-charge by downloading the latest software release for the Cisco Catalyst 2950 switches.

Secure Shell (SSH) and Simple Network Management Protocol version 3 (SNMPv3) protects information from being tampered with or eavesdropped by encrypting information being passed along the network, thereby guarding administrative information. Private VLAN Edge isolates ports on a switch, ensuring that traffic travels directly from the entry point to the aggregation device through a virtual path and cannot be directed to another port. Local Proxy Address Resolution Protocol (ARP) works in conjunction with private VLAN edge to minimize broadcasts and maximize available bandwidth.

Port-based Access Control Parameters (ACPs) restrict sensitive portions of the network by denying packets based on source and destination MAC addresses, IP addresses, or TCP/UDP ports. ACP lookups are done in hardware; therefore, forwarding performance is not compromised when implementing this type of security in the network. In addition, Time-based ACLs allow configuration of differentiated services based on time periods. ACLs can also be applied to filter traffic based on differentiated services code point (DSCP) values. Port security provides another means to ensure the appropriate user is on the network by limiting access based on MAC addresses.

For authentication of users with a Terminal Access Controller Access Control System (TACACS+) or RADIUS server, 802.1x provides port-level security. 802.1x in conjunction with a RADIUS server allows for dynamic port-based user authentication. 802.1x-based user authentication can be extended to dynamically assign a VLAN based on a specific user regardless of where they connect on the network. This intelligent adaptability allows IT departments to offer

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 907
Doc: 3702

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

16-881

greater flexibility and mobility to their stratified user populations. By combining access control and user profiles with secure network connectivity, services, and applications, enterprises can more effectively manage user mobility and drastically reduce the overhead associated with granting and managing access to network resources.

With the multilayer Cisco Catalyst 2950 switches, network managers can implement high levels of console security. Multilevel access security on the switch console and the web-based management interface prevents unauthorized users from accessing or altering switch configuration TACACS+ or RADIUS authentication enables centralized access control of the switch and restricts unauthorized users from altering the configuration. Deploying security can be done through Cisco CMS Software Security Wizards, which ease the deployment of security features that restrict user access to a server, a portion of the network, or access to the network.

Network Control Through Advanced Quality of Service and Rate Limiting

The Cisco Catalyst 2950 Series Switches offer superior and highly granular QoS based on Layer 2–4 information, to ensure that network traffic is classified, prioritized, and congestion is avoided in the best possible manner. Configuration of QoS is greatly simplified through automatic QoS (auto-QoS), a feature that detects Cisco IP phones and automatically configures the switch for the appropriate classification and egress queuing. This optimizes traffic prioritization and network availability without the challenge of a complex configuration.

The Cisco Catalyst 2950 Series Switches can classify, reclassify, police (determine if the packet is in or out of predetermined profiles and affect actions on the packet), and mark or drop the incoming packets before the packet is placed in the shared buffer. Packet classification allows the network elements to discriminate between various traffic flows and enforce policies based on Layer 2 and Layer 3 QoS fields.

To implement QoS, these switches first identify traffic flows, or packet groups, and classify or reclassify these groups using the DiffServ Code Point (DSCP) field in the IP packet and/or the 802.1p class of service (CoS) field in the Ethernet packet. Classification and reclassification can also be based on criteria as specific as the source/destination IP address, source/destination MAC address or the Layer 4 Transmission Control Protocol (TCP)/User Datagram Protocol (UDP) ports. At the ingress (incoming port) level, the Cisco Catalyst switches will also perform policing and marking of the packet.

After the packet goes through classification, policing, and marking, it is then assigned to the appropriate queue before exiting the switch. The Cisco Catalyst 2950 Series Switches support four egress (outgoing port) queues per port, which allows the network administrator to be more discriminating and specific in assigning priorities for the various applications on the LAN. At the egress level, the switch performs scheduling, which is an algorithm/process that determines the order in which the queues are processed. The switches support Weighted Round Robin (WRR) scheduling or strict priority scheduling. The WRR scheduling algorithm ensures that the lower priority packets are not entirely starved for bandwidth and are serviced without compromising the priority settings administered by the network manager. Strict priority scheduling ensures that the highest priority packets will always get serviced first, ahead of all other traffic, and that the other three queues will be serviced using WRR best effort.

These features allow network administrators to prioritize mission-critical and/or bandwidth-intensive traffic, such as ERP (Oracle, SAP, and so on), voice (IP telephony traffic) and CAD/CAM over less time-sensitive applications such as FTP or e-mail (SMTP). For example, it would be highly undesirable to have a large file download destined to one port on a wiring closet switch and have quality implications such as increased latency in voice traffic, destined to another port on this switch. This condition is avoided by ensuring that voice traffic is properly classified and prioritized throughout the network. Other applications, such as Web browsing, can be treated as low priority and handled on a best-efforts basis.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 908
3702
Doc:

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

16.830
2

The Cisco Catalyst 2950 Series Switches are capable of allocating bandwidth based on several criteria including MAC source address, MAC destination address, IP source address, IP destination address, and TCP/UDP port number. Bandwidth allocation is essential in network environments requiring service-level agreements or when it is necessary for the network manager to control the bandwidth given to certain users. The Cisco Catalyst 2950 Series Switches support up to 6 policers per Fast Ethernet port and up to 60 policers on a Gigabit Ethernet port. This gives the network administrator very granular control of LAN bandwidth.

Network Availability

To provide efficient use of resources for bandwidth-hungry applications like multicasts, the Cisco Catalyst 2950 Series Intelligent Switches support Internet Group Management Protocol (IGMP) snooping in hardware. Through the support and configuration of IGMP snooping via the Cisco CMS Software, Cisco Catalyst 2950 Series Switches deliver outstanding performance and ease of use in administering and managing multicast applications on the LAN.

The IGMP snooping feature allows the switch to "listen in" on the IGMP conversation between hosts and routers. When a switch hears an IGMP join request from a host for a given multicast group, the switch adds the host's port number to the Group Destination Address (GDA) list for that group. And, when the switch hears an IGMP leave request, it removes the host's port from the Content Addressable Memory (CAM) table entry.

PVST+ allows users to implement redundant uplinks while also distributing traffic loads across multiple links. This is not possible with standard Spanning-Tree Protocol implementations. Cisco UplinkFast technology ensures immediate transfer to the secondary uplink, much better than the traditional 30 to 60 second convergence time. This is yet another enhancement of the Spanning-Tree Protocol implementation. An additional feature that enhances performance is Voice VLAN. This feature allows network administrators to assign voice traffic to a VLAN dedicated to IP telephony—simplifying phone installations and providing easier network traffic administration and troubleshooting.

Multicast VLAN Registration (MVR) is designed for applications using wide-scale deployment of multicast traffic across an Ethernet ring-based service provider network (for example, the broadcast of multiple television channels over a service-provider network). MVR allows a subscriber on a port to subscribe and unsubscribe to a multicast stream on the network-wide multicast VLAN.

Network Management

The Cisco CMS is Web-based software that is embedded in Cisco Catalyst 3750, 3550, 2970, 2950, 2940, 3500 XL, 2900 XL, and 2900 LRE XL switches. Through Cisco Switch Clustering technology, users access Cisco CMS with any standard Web browser to manage up to 16 of these switches at once, regardless of their geographic proximity—with the option of using a single IP address for the entire cluster if desired. With the addition of the Cisco Catalyst 3550 switches, Cisco CMS Software can now extend beyond routed boundaries for even more flexibility in managing a Cisco cluster.

Cisco CMS provides an integrated management interface for delivering intelligent services, such as multilayer switching, QoS, multicast and security access control lists (ACLs). Thus, CMS allows administrators to take advantage of benefits formerly reserved for only the most advance networks without having to learn the CLI or even the details of the technology.

The new Guide Mode in Cisco CMS leads the user step-by-step through the configuration of advanced features and provides enhanced online help for context-sensitive assistance. In addition, Cisco AVVID (Architecture for Voice, Video and Integrated Data) Wizards provide automated configuration of the switch to optimally support video

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

PROC. nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 909
Doc: 3702

16 879
2

streaming or video conferencing, voice over IP (VoIP) and mission-critical applications. These Wizards can save hours of time for network administrators, eliminate human errors, and ensure that the configuration of the switch is optimized for these applications.

Cisco CMS Software supports standards-based connectivity options such as Ethernet, Fast Ethernet, Fast EtherChannel®, Gigabit Ethernet, and Gigabit EtherChannel connectivity. Because Cisco Switch Clustering technology is not limited to a single stack of switches, Cisco CMS Software expands the traditional cluster domain beyond a single wiring closet and saves time and effort for network administrators.

Cisco Catalyst 2950 switches can be configured either as "command" or "member" switches in a Cisco switch cluster. Cisco CMS also allows the network administrator to designate a standby or redundant command switch, which takes the commander duties should the primary command switch fail. Other key features include the ability to configure multiple ports and switches simultaneously, as well as perform software updates across the entire cluster at once, and clone configurations to other clustered switches for rapid network deployments. Bandwidth graphs and link reports provide useful diagnostic information and the topology map gives network administrators a quick view of the network status.

In addition to CMS, Cisco Catalyst 2950 switches provide extensive management tools using SNMP network management platforms such as CiscoWorks for Switched Internetworks.

The Cisco Catalyst 2950 Switches deliver a comprehensive set of management tools to provide the required visibility and control in the network. Managed with CiscoWorks, Cisco Catalyst family switches can be configured and managed to deliver end-to-end device, VLAN, traffic, and policy management. Coupled with CiscoWorks, Cisco Resource Manager Essentials, a Web-based management tool, offers automated inventory collection, software deployment, easy tracking of network changes, views into device availability, and quick isolation of error conditions.

Cisco Express Setup is a new feature that simplifies initial configuration of a switch. Users now have the option to set up the switch through a Web browser, eliminating the need for more complex terminal emulation programs and knowledge of the CLI. Cisco Express Setup reduces the cost of deployment by enabling less-skilled personnel to quickly and simply set up switches.

Figure 1
Cisco Catalyst 2950 Switches

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 910
Doc: 3702

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

16.878

Product Features and Benefits

Feature	Benefit
Availability	
Superior Redundancy for Fault Backup	• IEEE 802.1D Spanning-Tree Protocol support for redundant backbone connections and loop-free networks simplifies network configuration and improves fault tolerance. • Support for Cisco Spanning-Tree Protocol enhancements such as UplinkFast, BackboneFast, and PortFast technologies ensure quick fail-over recovery enhancing overall network stability and availability. • IEEE 802.1w Rapid Spanning-Tree Protocol (RSTP) provides rapid convergence of the spanning tree independent of spanning-tree timers. • Cisco CrossStack UplinkFast technology extends UplinkFast to a stack to ensure quick fail-over recovery enhancing network stability and availability. • Support for Cisco's optional, 300W or 675W redundant AC power system provides a backup power source for up to 4 units or 6 units, respectively, for improved fault tolerance and network uptime. • Redundant stacking connections provide support for a redundant loopback connection for top and bottom switches in an independent stack backplane cascaded configuration. • Command switch redundancy enabled in the Cisco CMS Software allows customers to designate a backup command switch that takes over cluster management functions if the primary command switch fails. • Provides unidirectional link detection (UDLD) and Aggressive UDLD for detecting and disabling unidirectional links on fiber-optic interfaces caused by incorrect fiber-optic wiring or port faults.
Integrated Cisco IOS Features for Bandwidth Optimization	• Bandwidth aggregation up to 4 Gbps (2 ports full duplex) through Gigabit EtherChannel technology and up to 16 Gbps (8 ports full duplex) through Fast EtherChannel technology enhances fault tolerance and offers higher-speed aggregated bandwidth between switches, to routers and individual servers. Port Aggregation Protocol (PAgP) is available to simplify configuration. • VLAN1 minimization allows VLAN1 to be disabled on any individual VLAN trunk link. • Per-port broadcast, multicast, and unicast storm control prevents faulty end stations from degrading overall systems performance. • Per virtual LAN (VLAN) PVST+ allows for Layer 2 load sharing on redundant links to efficiently utilize the extra capacity inherent in a redundant design. • IEEE 802.1s Multiple Spanning-Tree Protocol (MSTP) allows a spanning tree instance per VLAN enabling Layer 2 load sharing on redundant links. • VLAN Trunking Protocol (VTP) pruning limits bandwidth consumption on VTP trunks by flooding broadcast traffic only on trunk links required to reach the destination devices. Dynamic Trunking Protocol (DTP) enables dynamic trunk configuration across all ports in the switch • IGMP snooping provides for fast client joins and leaves of multicast streams and limits bandwidth-intensive video traffic to only the requestors. MVR, IGMP filtering and fast-join and immediate leave are available as enhancements. • MVR continuously sends multicast streams in a multicast VLAN while isolating the streams from subscriber VLANs for bandwidth and security reasons. • Supports additional frame formats: Ethernet II (tagged and untagged), 802.3 (SNAP encapsulated tagged and untagged frames)

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 911
Doc: 3702

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

16·847
L

Feature	Benefit
Security	
Network-Wide Security Features	• Filtering of incoming traffic flows based on Layer 2, Layer 3, or Layer 4 ACPs prevents unauthorized data flows. – The following Layer 2 ACPs or a combination can be used for security classification of incoming packets: source MAC address, destination MAC address, and 16-bit Ethertype. – The following Layer 3 and Layer 4 fields or a combination can be used for security classification of incoming packets: source IP address, destination IP address, TCP source or destination port number, UDP source, or destination port number. ACLs can also be applied to filter based on DSCP-values. – Time-based ACLs allow configuration of differentiated services based on time-periods. • A private VLAN edge provides security and isolation between ports on a switch, ensuring that voice traffic travels directly from its entry point to the aggregation device through a virtual path and cannot be directed to a different port. • Support for the 802.1x standard allows users to be authenticated regardless of which LAN port they are accessing, and provides unique benefits to customers who have a large base of mobile (wireless) users accessing the network. – 802.1x with VLAN assignment allows a dynamic VLAN assignment for a specific user regardless of where the user is connected. – 802.1x with an ACL assignment allows for specific security policies based on a user regardless of where the user is connected. – 802.1x with voice VLAN to permit an IP phone access to the voice VLAN irrespective of the authorized or unauthorized state of the port – 802.1x with port security for authenticating the port and managing network access for all addresses, including that of the client. • SSH and SNMPv3 provides network security by encrypting administrator traffic during Telnet and SNMP sessions—SSH and the crypto version of SNMPv3 require a special crypto software image due to US export restrictions. • Port Security secures the access to a port based on the MAC address of a users device. The aging feature removes the MAC address from the switch after a specific timeframe to allow another device to connect to the same port. • MAC Address Notification allows administrators to be notified of new users added or removed from the network. • Spanning-tree root guard (STRG) prevents edge devices not in the network administrator's control from becoming Spanning-Tree Protocol root nodes. • The Spanning-Tree Protocol PortFast/bridge protocol data unit (BPDU) guard feature disables access ports with Spanning-Tree Protocol PortFast-enabled upon reception of a BPDU, and increases network reliability, manageability, and security. Multilevel security on console access prevents unauthorized users from altering the switch configuration. • TACACS+ and RADIUS authentication to enable centralized control of the switch and restrict unauthorized users from altering the configuration. • The user-selectable address-learning mode simplifies configuration and enhances security. • Trusted Boundary provides the ability to trust the QoS priority settings if an IP phone is present and disable the trust setting in the event that the IP phone is removed, thereby preventing a rogue user from overriding prioritization policies in the network. • IGMP Filtering provides multicast authentication by filtering out non-subscribers and limits the number of concurrent multicast streams available per port.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 912
3702

Cisco Systems, Inc.
All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

16.876

Feature	Benefit
	• Support for dynamic VLAN assignment through implementation of VLAN Membership Policy Server (VMPS) client functionality provides flexibility in assigning ports to VLANs. Dynamic VLAN enables fast assignment of IP address. • Cisco CMS Software Security Wizards ease the deployment of security features for restricting user access to a server, a portion of the network or access to the network.
QoS	
	Overview • The switches support the aggregate QoS model by enabling classification, policing/metering, and marking functions on a per-port basis at ingress and queuing/scheduling function at egress. • The switches support configuring QoS ACPs on all ports to ensure proper policing and marking on a per-packet basis using ACPs. Up to 4 ACPs per switch are supported in configuring either QoS ACPs or security filters. • Automatic QoS (Auto-QoS) greatly simplifies the configuration of QoS in VoIP networks by issuing interface and global switch commands that allow the detection of Cisco IP phones, the classification of traffic, and egress queue configuration.
	QoS Classification Support at Ingress • The switches support QoS classification of incoming packets for QoS flows based on Layer 2, Layer 3, and Layer 4 fields. • The following Layer 2 fields or a combination can be used for classifying incoming packets to define QoS flows: source MAC address, destination MAC address, 16-bit Ethertype. • The switches support identification of traffic based on Layer 3 ToS field—DSCP values. • The following Layer 3 and 4 fields or a combination can be used to classify incoming packets to define QoS flows: source IP address, destination IP address, TCP source or destination port number, UDP source or destination port number.
	QoS Metering/Policing at Ingress • Support for metering/policing of incoming packets restricts incoming traffic flows to a certain rate. • The switches support up to 6 policers per Fast Ethernet port, and 60 policers on a Gigabit Ethernet port. • The switches offer granularity of traffic flows at 1 Mbps on Fast Ethernet ports, and 8 Mbps on Gigabit Ethernet ports.
	QoS Marking at Ingress • The switches support marking/re-marking packets based on state of policers/meters. • The switches support marking/re-marking based on the following mappings: from DSCP to 802.1p, and 802.1p to DSCP. • The switches support 14 well-known and widely used DSCP values. • The switches support classifying or reclassifying packets based on default DSCP per port. Also support classification based on DSCP-values in ACL. • The switches support classifying or reclassifying frames based on default 802.1p value per port. • The switches support 802.1p override at ingress.
	QoS Scheduling Support at Egress • 4 queues per egress port are supported in hardware. • The WRR queuing algorithm ensures that low-priority queues are not starved. • Strict-priority queue configuration via Strict Priority Scheduling ensures that time-sensitive applications such as voice always follow an expedited path through the switch fabric.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 913
Doc: 3702

16-875
L

Feature	Benefit
Sophisticated Traffic Management	• The switch supports up to 6 policers per Fast Ethernet port and up to 60 policers on a Gigabit Ethernet port. • The switch offers granularity of traffic flows at 1 Mbps on Fast Ethernet ports and 8 Mbps on Gigabit Ethernet ports. • The switch offers the ability to limit data flows based on MAC source/destination address, IP source/destination address, TCP/UDP port numbers, or any combination of these fields. • The switch offers the ability to manage data flows asynchronously upstream and downstream from the end station or on the uplink.
Management	
Superior Manageability	• An embedded Remote Monitoring (RMON) software agent supports 4 RMON groups (history, statistics, alarms, and events) for enhanced traffic management, monitoring, and analysis. • The switch supports all 9 RMON groups through the use of a Cisco SwitchProbe® Analyzer (Switched Port Analyzer [SPAN]) port, permitting traffic monitoring of a single port, a group of ports, or the entire switch from a single network analyzer or RMON probe. • A SPAN port monitors traffic of a single port from a single network analyzer or RMON probe. • Remote Switch Port Analyzer (RSPAN) allows network administrators to locally monitor ports in a Layer 2 switch network from any other switch in the same network. • The Domain Name System (DNS) provides IP address resolution with user-defined device names. • Trivial File Transfer Protocol (TFTP) reduces the cost of administering software upgrades by downloading from a centralized location. • Network Timing Protocol (NTP) provides an accurate and consistent timestamp to all switches within the intranet. • Layer 2 traceroute eases troubleshooting by identifying the physical path that a packet takes from the source device to a destination device. • Crash Information support enables switch to generate a crash file for improved troubleshooting. • Show-interface-capabilities provides information on configuration capabilities of any interface. • RTTMON-MIB allows users to monitor network performance between a Cisco Catalyst switch and a remote device. • Multifunction LEDs per port for port status, half-duplex/full-duplex, 10BASE-T/100BASE-TX/1000BASE-T indication, as well as switch-level status LEDs for system, redundant power supply, and bandwidth utilization provide a comprehensive and convenient visual management system. • Layer 2 traceroute eases troubleshooting by identifying the physical path that a packet takes from the source device to a destination device.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 914
Doc 3702

16.875

Feature	Benefit
Cisco CMS	• Cisco CMS Software allows the user to manage up to 16 inter-connected Cisco Catalyst 3750, 3550, 2970, 2950, 2940, 3500 XL, 2900 XL, and 2900 LRE XL switches without the limitation of being physically located in the same wiring closet, and with the option of using a single IP address for the entire cluster if desired. Full backward compatibility ensures any combination of the above switches can be managed with a Cisco Catalyst 2950 switch. • Cisco AVVID Wizards use just a few user inputs to automatically configure the switch to optimally handle different types of traffic: voice, video, multicast, and/or high-priority data. • A security wizard is provided to restrict unauthorized access to servers and networks, and restrict certain applications on the network. • One-click software upgrades can be performed across the entire cluster simultaneously, and configuration cloning enables rapid deployment of networks. • Cisco CMS Software has been extended to include multilayer feature configurations such as ACPs and QoS parameters. • Cisco CMS Guide Mode assists users in the configuration of powerful advanced features by providing step-by-step instructions. • Cisco CMS provides enhanced online help for context-sensitive assistance. • Easy-to-use graphical interface provides both a topology map and front panel view of the cluster. • Multi-device and multi-port configuration capabilities allow network administrators to save time by configuring features across multiple switches and ports simultaneously. • Ability to launch the Web-based management for a Cisco Aironet Wireless Access Point by simply clicking on its icon in the topology map. • User-personalized interface allows users to modify polling intervals, table views, and other settings within CMS and retain these settings the next time they use CMS. • Alarm notification provides automated e-mail notification of network errors and alarm thresholds.
Support for CiscoWorks	• Manageable through CiscoWorks network management software on a per-port and per-switch basis providing a common management interface for Cisco routers, switches, and hubs. • SNMP v1, v2, and v3 (non-crypto) and Telnet interface support delivers comprehensive in-band management, and a CLI-based management console provides detailed out-of-band management. • Cisco Discovery Protocol (CDP) Versions 1 and 2 enable a CiscoWorks network management station to automatically discover the switch in a network topology. • Supported by the CiscoWorks 2000 LAN Management Solution.
Ease of Use and Ease of Deployment	• Cisco Express Setup – Simplifies initial configuration of a switch via a Web browser, eliminating the need for more complex terminal emulation programs and CLI knowledge. – Reduces the cost of deployment by enabling less-skilled personnel to quickly and simply set up switches. • The Cisco GigaStack GBIC delivers a hardware-based, independent stacking bus with up to 2-Gbps forwarding rate in a point-to-point configuration, or 1-Gbps forwarding bandwidth when daisy chained with up to 9 switches. • Auto-configuration eases deployment of switches in the network by automatically configuring multiple switches across a network via a boot server. • Auto-QoS greatly simplifies the configuration of QoS in VoIP networks by issuing interface and global switch commands that allow the detection of Cisco IP phones, the classification of traffic, and egress queue configuration.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 915
Doc 3702

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

16.874

Feature	Benefit
	• Auto-sensing on each non-GBIC port detects the speed of the attached device and automatically configures the port for 10-, 100-, or 1000-Mbps operation, easing the deployment of the switch in mixed 10, 100, and 1000BASE-T environments. • Auto-negotiating on all ports automatically selects half- or full-duplex transmission mode to optimize bandwidth. • Cisco VTP supports dynamic VLANs and dynamic trunk configuration across all switches. • Voice VLAN simplifies telephony installations by keeping voice traffic on a separate VLAN for easier network administration and troubleshooting. • DTP enables dynamic trunk configuration across all ports in the switch. • PAgP automates the creation of Cisco Fast EtherChannel or Gigabit EtherChannel groups, enabling linking to another switch, router, or server. • Link Aggregation Control Protocol (LACP) allows the creation of Ethernet channeling with devices that conform to IEEE 802.3ad. This is similar to Cisco's EtherChannel and PAgP. • IEEE 802.3z-compliant 1000BASE-SX, 1000BASE-LX/LH, 1000BASE-ZX, and 1000BASE-T physical interface support through a field-replaceable GBIC module provides customers unprecedented flexibility in switch deployment. • The default configuration stored in Flash ensures that the switch can be quickly connected to the network and can pass traffic with minimal user intervention. • The switches support non-standard Ethernet frame sizes (mini-giants) up to 1542 bytes (configurations with GBIC ports only).

Product Specifications

Feature	Description
Performance	• 13.6-Gbps switching fabric • Cisco Catalyst 2950G-48: 13.6-Gbps maximum forwarding bandwidth • Cisco Catalyst 2950G-24: 8.8-Gbps maximum forwarding bandwidth • Cisco Catalyst 2950G-24-DC: 8.8-Gbps maximum forwarding bandwidth • Cisco Catalyst 2950G-12: 6.4-Gbps maximum forwarding bandwidth • Cisco Catalyst 2950T-24: 8.8-Gbps maximum forwarding bandwidth • Cisco Catalyst 2950C-24: 5.2-Gbps maximum forwarding bandwidth (Forwarding rates based on 64-byte packets) • Cisco Catalyst 2950G-48: 10.1-Mpps wire-speed forwarding rate • Cisco Catalyst 2950G-24: 6.6-Mpps wire-speed forwarding rate • Cisco Catalyst 2950G-24-DC: 6.6-Mpps wire-speed forwarding rate • Cisco Catalyst 2950G-12: 4.8-Mpps wire-speed forwarding rate • Cisco Catalyst 2950T-24: 6.6-Mpps wire-speed forwarding rate • Cisco Catalyst 2950C-24: 3.9-Mpps wire-speed forwarding rate • 8-MB memory architecture shared by all ports • Up to 16-MB SDRAM and 8-MB Flash memory • Configurable up to 8000 MAC addresses • Configurable maximum transmission unit (MTU) of up to 1,530 bytes (Cisco Catalyst 2950G switches only)

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 916
Nº Doc: 3702

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

16.873
L

Feature	Description
Management	• BRIDGE-MIB • CISCO-BULK-FILE-MIB • CISCO-2900-MIB • CISCO-CDP-MIB • CISCO-CLASS-BASED-QOS-MIB • CISCO-CLUSTER-MIB • CISCO-CONFIG-COPY-MIB • CISCO-CONFIG-MAN-MIB • CISCO-ENVMON-MIB • CISCO-FLASH-MIB • CISCO-FTP-CLIENT-MIB • CISCO-IMAGE-MIB • CISCO-IPMROUTE-MIB • CISCO-MAC-NOTIFICATION-MIB • CISCO-MEMORY-POOL-MIB • CISCO-PAGP-MIB • CISCO-PING-MIB • CISCO-PROCESS-MIB • CISCO-PRODUCTS-MIB • CISCO-RTTMON-MIB • CISCO-SMI • CISCO-STACKMAKER-MIB • CISCO-STP-EXTENSIONS-MIB • CISCO-SYSLOG-MIB • CISCO-TC • CISCO-TCP-MIB • CISCO-VLAN-MEMBERSHIP-MIB • CISCO-VTP-MIB • ENTITY-MIB • IANAifType-MIB • IF-MIB (RFC 1573) • OLD-CISCO-CHASSIS-MIB • OLD-CISCO-CPU-MIB • OLD-CISCO-INTERFACES-MIB • OLD-CISCO-IP-MIB • OLD-CISCO-MEMORY-MIB • OLD-CISCO-SYSTEM-MIB • OLD-CISCO-TCP-MIB • OLD-CISCO-TS-MIB • RFC1213-MIB (MIB-II) • RFC1398-MIB (ETHERNET-MIB) • RMON-MIB (RFC 1757) • RS-232-MIB • SNMPv2-MIB • SNMPv2-SMI • SNMPv2-TC • TCP-MIB • UDP-MIB

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
917
Fls Nº
3702
Doc:

16-872
2

Feature	Description
Standards	• IEEE 802.1x support • IEEE 802.1w • IEEE 802.1s • IEEE 802.3x full duplex on 10BASE-T, 100BASE-TX, and 1000BASE-T ports • IEEE 802.1D Spanning-Tree Protocol • IEEE 802.1p CoS prioritization • IEEE 802.1Q VLAN • IEEE 802.3 10BASE-T specification • IEEE 802.3u 100BASE-TX specification • IEEE 802.3ab 1000BASE-T specification • IEEE 802.3ad • IEEE 802.3z 1000BASE-X specification • 1000BASE-X (GBIC) • 1000BASE-T (GBIC) • 1000BASE-SX • 1000BASE-LX/LH • 1000BASE-ZX • 1000BASE-CWDM GBIC 1470 nm • 1000BASE-CWDM GBIC 1490 nm • 1000BASE-CWDM GBIC 1510 nm • 1000BASE-CWDM GBIC 1530 nm • 1000BASE-CWDM GBIC 1550 nm • 1000BASE-CWDM GBIC 1570 nm • 1000BASE-CWDM GBIC 1590 nm • 1000BASE-CWDM GBIC 1610 nm • RMON I and II standards • SNMPv1, SNMPv2c, SNMPv3 (planned future support for v3)
Y2K	• Y2K compliant
Connectors and Cabling	• 10BASE-T ports: RJ-45 connectors; 2-pair Category 3, 4, or 5 unshielded twisted-pair (UTP) cabling • 100BASE-TX ports: RJ-45 connectors; two-pair Category 5 UTP cabling • 1000BASE-T ports: RJ-45 connectors; two-pair Category 5 UTP cabling • 100BASE-FX ports: MT-RJ connectors, 50/125 or 62.5/125 micron multimode fiber-optic cabling • 1000BASE-T, 1000BASE-SX, -LX/LH, -ZX GBIC-based ports: SC fiber connectors, single-mode or multimode fiber • Cisco GigaStack GBIC ports: copper-based Cisco GigaStack cabling • Management console port: 8-pin RJ-45 connector, RJ-45-to-RJ-45 rollover cable with RJ-45-to-DB9 adapter for PC connections; for terminal connections, use RJ-45-to-DB25 female data-terminal-equipment (DTE) adapter (can be ordered separately from Cisco, part number ACS-DSBUASYN=)
MT-RJ Patch Cables for Cisco Catalyst 2950C-24 Switch	*Type of Cable, Cisco Part Number* • 1-meter, MT-RJ-to-SC multimode cable, CAB-MTRJ-SC-MM-1M • 3-meter, MT-RJ-to-SC multimode cable, CAB-MTRJ-SC-MM-3M • 5-meter, MT-RJ-to-SC multimode cable, CAB-MTRJ-SC-MM-5M • 1-meter, MT-RJ-to-ST multimode cable, CAB-MTRJ-ST-MM-1M • 3-meter, MT-RJ-to-ST multimode cable, CAB-MTRJ-ST-MM-3M • 5-meter, MT-RJ-to-ST multimode cable, CAB-MTRJ-ST-MM-5M

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 918
3702
Doc:

16.871
L

Feature	Description
Power Connectors	Customers can provide power to a switch by using either the internal power supply or the Cisco RPS 300. The connectors are located at the back of the switch. **Internal Power Supply Connector** • The internal power supply is an auto-ranging unit. • The internal power supply supports input voltages between 100 and 240 VAC. • Use the supplied AC power cord to connect the AC power connector to an AC power outlet. **Cisco RPS 675 Connector** • The connector offers connection for an optional Cisco RPS 675 that uses AC input and supplies DC output to the switch. • The connector offers a 675W RPS that supports 6 external network devices and provides power to 1 failed device at a time. • The connector automatically senses when the internal power supply of a connected device fails and provides power to the failed device, preventing loss of network traffic. • Attach only the Cisco RPS 675 (model PWR675-AC-RPS-NI=) to the redundant power supply receptacle with this connector. **Cisco RPS Connector (Cisco RPS 300)** • The connector offers connection for an optional Cisco RPS 300 that uses AC input and supplies DC output to the switch. • The connector offers a 300W RPS that can support 6 external network devices and provides power to 1 failed device at a time. • The connector automatically senses when the internal power supply of a connected device fails and provides power to the failed device, preventing loss of network traffic. • Attach only the Cisco RPS 300 (model PWR300-AC-RPS-N1) to the redundant-power-supply receptacle.
Indicators	• Per-port status LEDs: link integrity, disabled, activity, speed, and full-duplex indications. • System status LEDs: system, RPS, and bandwidth utilization indications.
Dimensions and Weight (H x W x D)	• 1.72 x 17.5 x 9.52 in. (4.36 x 44.5 x 24.18 cm) (Cisco Catalyst 2950T-24, 2950C-24, 2950G-12, and 2950G-24) • 1.72 x 17.5 x 13 in. (4.36 x 44.5 x 33.02 cm) (Cisco Catalyst 2950G-48) • 1.0 rack-unit high • 6.5 lb (3.0 kg) (Cisco Catalyst 2950T-24, 2950C-24, 2950G-12 and 2950G-24) • 10 lb (4.5 kg) (Cisco Catalyst 2950G-48)
Environmental Ranges	• Operating temperature: 32 to 113 F (0 to 45 C) • Storage temperature: –13 to 158 F (–25 to 70 C) • Operating relative humidity: 10 to 85% (non-condensing) • Operating altitude: Up to 10,000 ft (3000 m) • Storage altitude: Up to 15,000 ft (4500 m) • Not intended for use on top of desktops or in open office environments

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 919
3702
Doc:

16.870
2

Feature	Description
Power Requirements	• Power consumption: 30W maximum, 102 BTUs per hour (Cisco Catalyst 2950T-24, 2950C-24, 2950G-12, and 2950G-24) • Power consumption: 45W maximum, 154 BTUs per hour (Cisco Catalyst 2950G-48) • AC input voltage/frequency: 100 to 127/200 to 240 VAC (auto-ranging), 50 to 60 Hz • DC Input Voltages for Cisco RPS 300 RPS: +12V @ 4.5A
Acoustic Noise	• ISO 7770, bystander position—operating to an ambient temperature of 30 degrees Celsius: • WS-C2950-24, WS-C2950-12, WS-C2950C-24, WS-C2950T-24: 46 dBa • WS-C2950G-12, WS-C2950G-24: 46 dBa • WS-C2950G-48: 48 dBa
Mean Time Between Failure (MTBF) **– Predicted**	• 482,776 hours (Cisco Catalyst 2950G-12) • 468,884 hours (Cisco Catalyst 2950G-24) • 479,086 hours (Cisco Catalyst 2950G-24-DC) • 159,026 hours (Cisco Catalyst 2950G-48) • 297,144 hours (Cisco Catalyst 2950T-24) • 268,292 hours (Cisco Catalyst 2950C-24)
Fiber-Port Specifications for Cisco Catalyst 2950C-24 Switch	Fiber-Port Power Levels: • Optical transmitter wavelength: 1300 nanometers • Optical receiver sensibility: –14 dBm2 • Optical transmitter power: –19 dBm to –14 dBm • Transmit: –19 dBm to –14 dBm
Regulatory Agency Approvals	
Safety Certifications	• UL 1950/CSA 22.2 No. 950 • IEC 950-EN 60950 • AS/NZS 3260, TS001 • CE Marking
Electromagnetic Emissions Certifications	• FCC Part 15 Class A • EN 55022: 1998 Class A (CISPR22 Class A) • EN 55024: 1998 (CISPR24) • VCCI Class A • AS/NZS 3548 Class A • CE Marking • CNS 13438 • BSMI Class A • MIC

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 920
3702
Doc:

16.869

Feature	Description
NEBS (For WS-C2950G-24-EI-DC only)	• Bellcore • GR-1089-CORE • GR-63-CORE • SR-3580 Level 3
Warranty	• Limited lifetime warranty

Service and Support

The services and support programs described in the table below are available as part of the Cisco Desktop Switching Service and Support solution, and are available directly from Cisco and through resellers.

Service and Support	Features	Benefits
Advanced Services		
Total Implementation Solutions (TIS)— available direct from Cisco *Packaged Total Implementation Solutions (Packaged TIS)*— available through resellers	• Project management • Site survey, configuration deployment • Installation, text, and cutover • Training • Major Moves, Adds, Changes (MAC) • Design review and product staging	• Supplements existing staff • Ensures functionality meets needs • Mitigates risk
Technical Support Services		
SMARTnet and SMARTnet Onsite (OS)— available direct from Cisco *Packaged SMARTnet*— available through resellers	• 24x7 access to software updates • Web access to technical repositories • Telephone support through the Technical Assistance Center • Advance replacement of hardware parts	• Enables proactive or expedited issue resolution • Lowers cost of ownership by utilizing Cisco expertise and knowledge • Minimize network downtime

Ordering Information

Model Numbers	Configuration
WS-C2950G-48-EI	• 48 10/100 ports + 2 1000BASE-X ports • EI installed
WS-C2950G-24-EI	• 24 10/100 ports + 2 1000BASE-X ports • EI installed
WS-C2950G-24-EI-DC	• 24 10/100 ports + 2 1000BASE-X ports, DC power • EI installed
WS-C2950G-12-EI	• 12 10/100 ports + 2 1000BASE-X ports • EI installed
WS-C2950T-24	• 24 10/100 ports + 2 1000BASE-T ports • EI installed

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 921
3702
Doc:

16 868
2

Model Numbers	Configuration
WS-C2950C-24	• 24 10/100 ports + 2 100BASE-FX ports • EI installed
WS-C2950ST-24-LRE	• 24 Long-Reach Ethernet (LRE) ports and 2 fixed 10/100/1000BASE-T ports and 2 Form Factor Pluggable (SFP) ports • EI installed
WS-C2950ST-8-LRE	• 8 LRE ports and 2 fixed 10/100/1000BASE-T ports and 2 SFP ports • EI installed

For More Information on Cisco Products, Contact:

- US and Canada: 800 553-NETS (6387)
- Europe: 32 2 778 4242
- Australia: 612 9935 4107
- Other: 408 526-7209
- World Wide Web URL:

  http://www.cisco.com

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the **Cisco Web site at www.cisco.com/go/offices**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Catalyst, cisco, Cisco IOS, Cisco Systems, the Cisco Systems logo, EtherChannel, GigaStack, and SwitchProbe are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0304R)

WH/LW4736 06/03

ROS II 03/2005 CN - CPMI - CORREIOS
Fls N° 922
3702
Doc

ANEXO 10A

16.867
2

GIGABIT ETHERNET OVER COPPER (802.3AB)

Introduction

Gigabit ethernet over Copper (also known as 1000BaseT) is an extension of the existing Fast Ethernet standard. It specifies Gigabit Ethernet operation over the Category 5e/6 cabling systems already installed, making it a highly cost effective solution. As a result, most copper-based environments that run Fast Ethernet can also run Gigabit Ethernet over the existing network infrastructure in order to dramatically boost network performance for demanding applications.

© 1992-2003 Cisco Systems, Inc. All rights reserved. Important Notices, Privacy Statement, and Trademark

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 923
Doc: 3702

ANEXO (10B)

16.866
L

Configuring SPAN and RSPAN

This chapter describes how to configure Switched Port Analyzer (SPAN) and Remote SPAN (RSPAN) on your Catalyst 2950 or Catalyst 2955 switch.

Note For complete syntax and usage information for the commands used in this chapter, refer to the command reference for this release.

This chapter consists of these sections:

- Understanding SPAN and RSPAN, page 22-1
- Configuring SPAN, page 22-7
- Configuring RSPAN, page 22-12
- Displaying SPAN and RSPAN Status, page 22-16

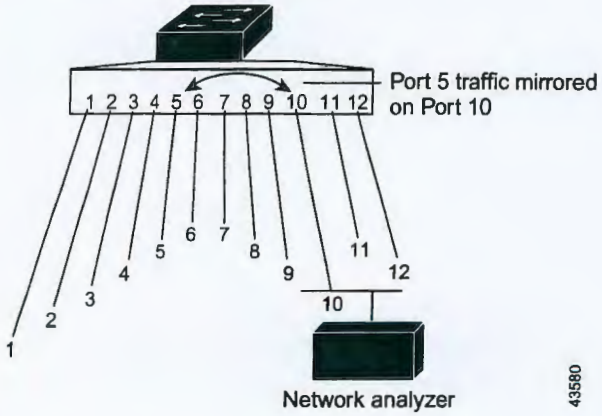
Understanding SPAN and RSPAN

You can analyze network traffic passing through ports by using SPAN to send a copy of the traffic to another port on the switch that has been connected to a SwitchProbe device or other Remote Monitoring (RMON) probe or security device. SPAN mirrors received or transmitted (or both) traffic on one or more source ports to a destination port for analysis.

For example, in Figure 22-1, all traffic on port 5 (the source port) is mirrored to port 10 (the destination port). A network analyzer on port 10 receives all network traffic from port 5 without being physically attached to port 5.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls' Nº 924
3702
Data

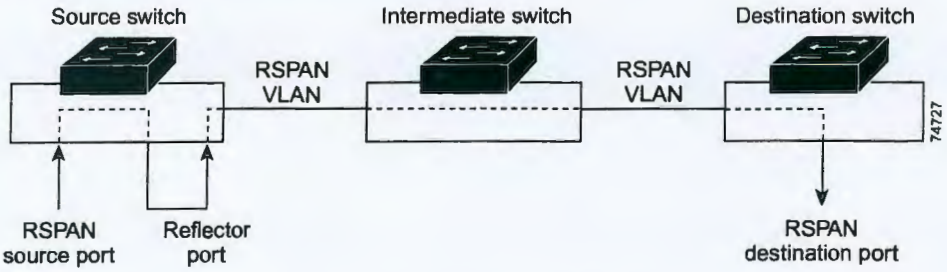
Figure 22-1 Example SPAN Configuration



Only traffic that enters or leaves source ports can be monitored by using SPAN.

RSPAN extends SPAN by enabling remote monitoring of multiple switches across your network. The traffic for each RSPAN session is carried over a user-specified RSPAN VLAN that is dedicated for that RSPAN session in all participating switches. The SPAN traffic from the sources is copied onto the RSPAN VLAN through a reflector port and then forwarded over trunk ports that are carrying the RSPAN VLAN to any RSPAN destination session monitoring the RSPAN VLAN, as shown in Figure 22-2.

Figure 22-2 Example of RSPAN Configuration



SPAN and RSPAN do not affect the switching of network traffic on source ports; a copy of the packets received or sent by the source interfaces are sent to the destination interface. Except for traffic that is required for the SPAN or RSPAN session, reflector ports and destination ports do not receive or forward traffic.

You can use the SPAN destination port to inject traffic from a network security device. For example, if you connect a Cisco Intrusion Detection System (IDS) Sensor Appliance to a destination port, the IDS device can send TCP Reset packets to close down the TCP session of a suspected attacker.

Note You cannot use the RSPAN destination port to inject traffic from a network security device. The switch does not support ingress forwarding on an RSPAN destination port.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 925
Nº Doc: 3702

16.864
2

SPAN and RSPAN Concepts and Terminology

This section describes concepts and terminology associated with SPAN and RSPAN configuration.

SPAN Session

A local SPAN session is an association of a destination port with source ports. You can monitor incoming or outgoing traffic on a series or range of ports.

An RSPAN session is an association of source ports across your network with an RSPAN VLAN. The destination source is the RSPAN VLAN.

SPAN sessions do not interfere with the normal operation of the switch. However, an oversubscribed SPAN destination, for example, a 10-Mbps port monitoring a 100-Mbps port, results in dropped or lost packets.

You can configure SPAN sessions on disabled ports; however, a SPAN session does not become active unless you enable the destination port and at least one source port for that session. The **show monitor session** *session_number* privileged EXEC command displays the operational status of a SPAN session.

A SPAN session remains inactive after system power-on until the destination port is operational.

Traffic Types

SPAN sessions include these traffic types:

- Receive (Rx) SPAN—The goal of receive (or ingress) SPAN is to monitor as much as possible all the packets received by the source interface. A copy of each packet received by the source is sent to the destination port for that SPAN session. You can monitor a series or range of ingress ports in a SPAN session.

  At the destination port, if tagging is enabled, the packets appear with the 802.1Q header. If no tagging is specified, packets appear in the native format.

  Packets that are modified because of quality of service (QoS)—for example, modified Differentiated Services Code Point (DSCP)—are copied with modification for Rx SPAN.

- Transmit (Tx) SPAN—The goal of transmit (or egress) SPAN is to monitor as much as possible all the packets sent by the source interface after all modification and processing is performed by the switch. A copy of each packet sent by the source is sent to the destination port for that SPAN session. The copy is provided after the packet is modified. You can monitor a range of egress ports in a SPAN session.

  Packets that are modified because of QoS, the modified packet might not have the same DSCP (IP packet) or CoS (non-IP packet) as the SPAN source.

  Some features that can cause a packet to be dropped during transmit processing might also affect the duplicated copy for SPAN. These features include IP standard and extended output ACLs on multicast packets, and egress QoS policing. In the case of output ACLs, if the SPAN source drops the packet, the SPAN destination would also drop the packet. If the source port is oversubscribed, the destination ports will have different dropping behavior.

- Both—In a SPAN session, you can monitor a series or range of ports for both received and sent packets.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
926
Fls Nº
3702
Doc:

16-863
2

Source Port

A source port (also called a *monitored port*) is a switched port that you monitor for network traffic analysis. In a single local SPAN session or RSPAN source session, you can monitor source port traffic such as received (Rx), transmitted (Tx), or bidirectional (both). The switch supports any number of source ports (up to the maximum number of available ports on the switch).

A source port has these characteristics:

- It can be any port type (for example, EtherChannel, Fast Ethernet, Gigabit Ethernet, and so forth).
- It cannot be a destination port.
- Each source port can be configured with a direction (ingress, egress, or both) to monitor. For EtherChannel sources, the monitored direction would apply to all the physical ports in the group.
- Source ports can be in the same or different VLANs.

You can configure a trunk port as a source port. All VLANs active on the trunk are monitored.

Destination Port

Each local SPAN session or RSPAN destination session must have a destination port (also called a *monitoring port*) that receives a copy of traffic from the source port.

The destination port has these characteristics:

- It must reside on the same switch as the source port (for a local SPAN session).
- It can be any Ethernet physical port.
- It cannot be a source port or a reflector port.
- It cannot be an EtherChannel group or a VLAN.
- It can be a physical port that is assigned to an EtherChannel group, even if the EtherChannel group has been specified as a SPAN source. The port is removed from the group while it is configured as a SPAN destination port.
- The port does not transmit any traffic except that required for the SPAN session.
- If ingress traffic forwarding is enabled for a network security device, the destination port forwards traffic at Layer 2.
- It does not participate in spanning tree while the SPAN session is active.
- When it is a destination port, it does not participate in any of the Layer 2 protocols (STP, VTP, CDP, DTP, PagP, LACP).
- No address learning occurs on the destination port.
- A destination port receives copies of sent and received traffic for all monitored source ports. If a destination port is oversubscribed, it could become congested. This could affect traffic forwarding on one or more of the source ports.

Reflector Port

The reflector port is the mechanism that copies packets onto an RSPAN VLAN. The reflector port forwards only the traffic from the RSPAN source session with which it is affiliated. Any device connected to a port set as a reflector port loses connectivity until the RSPAN source session is disabled.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 927
3702
Doc:

The reflector port has these characteristics:

- It is a port set to loopback.
- It cannot be an EtherChannel group, it does not trunk, and it cannot do protocol filtering.
- It can be a physical port that is assigned to an EtherChannel group, even if the EtherChannel group is specified as a SPAN source. The port is removed from the group while it is configured as a reflector port.
- A port used as a reflector port cannot be a SPAN source or destination port, nor can a port be a reflector port for more than one session at a time.
- It is invisible to all VLANs.
- The native VLAN for looped-back traffic on a reflector port is the RSPAN VLAN.
- The reflector port loops back untagged traffic to the switch. The traffic is then placed on the RSPAN VLAN and flooded to any trunk ports that carry the RSPAN VLAN.
- Spanning tree is automatically disabled on a reflector port.
- A reflector port receives copies of sent and received traffic for all monitored source ports. If a reflector port is oversubscribed, it could become congested. This could affect traffic forwarding on one or more of the source ports.

If the bandwidth of the reflector port is not sufficient for the traffic volume from the corresponding source ports, the excess packets are dropped. A 10/100 port reflects at 100 Mbps. A Gigabit port reflects at 1 Gbps.

SPAN Traffic

You can use local SPAN to monitor all network traffic, including multicast and bridge protocol data unit (BPDU) packets, and Cisco Discovery Protocol (CDP), VLAN Trunk Protocol (VTP), Dynamic Trunking Protocol (DTP), Spanning Tree Protocol (STP), Port Aggregation Protocol (PagP), and Link Aggregation Control Protocol (LACP) packets. You cannot use RSPAN to monitor Layer 2 protocols. See the "RSPAN Configuration Guidelines" section on page 22-12 for more information.

In some SPAN configurations, multiple copies of the same source packet are sent to the SPAN destination port. For example, a bidirectional (both Rx and Tx) SPAN session is configured for the sources a1 Rx monitor and the a2 Rx and Tx monitor to destination port d1. If a packet enters the switch through a1 and is switched to a2, both incoming and outgoing packets are sent to destination port d1.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 928
3702
Doc:

16-861
L

SPAN and RSPAN Interaction with Other Features

SPAN interacts with these features:

- Spanning Tree Protocol (STP)—A destination port or a reflector port does not participate in STP while its SPAN or RSPAN session is active. The destination or reflector port can participate in STP after the SPAN or RSPAN session is disabled. On a source port, SPAN does not affect the STP status. STP can be active on trunk ports carrying an RSPAN VLAN.
- Cisco Discovery Protocol (CDP)—A SPAN destination port does not participate in CDP while the SPAN session is active. After the SPAN session is disabled, the port again participates in CDP.
- VLAN Trunking Protocol (VTP)—You can use VTP to prune an RSPAN VLAN between switches.
- VLAN and trunking—You can modify VLAN membership or trunk settings for source, destination, or reflector ports at any time. However, changes in VLAN membership or trunk settings for a destination or reflector port do not take effect until you disable the SPAN or RSPAN session. Changes in VLAN membership or trunk settings for a source port immediately take effect, and the SPAN session automatically adjusts accordingly.
- EtherChannel—You can configure an EtherChannel group as a source port but not as a SPAN destination port. When a group is configured as a SPAN source, the entire group is monitored.

  If a port is added to a monitored EtherChannel group, the new port is added to the SPAN source port list. If a port is removed from a monitored EtherChannel group, it is automatically removed from the source port list. If the port is the only port in the EtherChannel group, the EtherChannel group is removed from SPAN.

  If a physical port that belongs to an EtherChannel group is configured as a SPAN source, destination, or reflector port, it is removed from the group. After the port is removed from the SPAN session, it rejoins the EtherChannel group. Ports removed from an EtherChannel group remain members of the group, but they are in the *down* or *standalone* state.

  If a physical port that belongs to an EtherChannel group is a destination or reflector port and the EtherChannel group is a source, the port is removed from the EtherChannel group and from the list of monitored ports.
- QoS—For ingress monitoring, the packets sent to the SPAN destination port might be different from the packets actually received at the SPAN source port because the packets are forwarded after ingress QoS classification and policing. The packet DSCP might not be the same as the received packet.
- Multicast traffic can be monitored. For egress and ingress port monitoring, only a single unedited packet is sent to the SPAN destination port. It does not reflect the number of times the multicast packet is sent.
- Port security—A secure port cannot be a SPAN destination port.

SPAN and RSPAN Session Limits

You can configure (and store in NVRAM) one local SPAN session or multiple RSPAN sessions on a switch. The number of active sessions and combinations are subject to these restrictions:

- SPAN or RSPAN source (rx, tx, both): 1 active session limit. (SPAN and RSPAN are mutually exclusive on a source switch).
- RSPAN source sessions have one destination per session with an RSPAN VLAN associated for that session.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
1929
Fls. Nº
3702
Doc.

- Each RSPAN destination session has one or more destination interfaces for each RSPAN VLAN that they support.
- RSPAN destination sessions are limited to two, or one if a local SPAN or a source RSPAN session is configured on the same switch.

Default SPAN and RSPAN Configuration

Table 22-1 shows the default SPAN and RSPAN configuration.

Table 22-1 Default SPAN and RSPAN Configuration

Feature	Default Setting
SPAN state	Disabled.
Source port traffic to monitor	Both received and sent traffic (**both**).
Encapsulation type (destination port)	Native form (no encapsulation type header).
Ingress forwarding (destination port)	Disabled.

Configuring SPAN

This section describes how to configure SPAN on your switch. It contains this configuration information:

- SPAN Configuration Guidelines, page 22-7
- Creating a SPAN Session and Specifying Ports to Monitor, page 22-8
- Creating a SPAN Session and Enabling Ingress Traffic, page 22-9
- Removing Ports from a SPAN Session, page 22-11

SPAN Configuration Guidelines

Follow these guidelines when configuring SPAN:

- SPAN sessions can coexist with RSPAN sessions within the limits described in the "SPAN and RSPAN Session Limits" section on page 22-6.
- The destination port cannot be a source port; a source port cannot be a destination port.
- You can have only one destination port.
- An EtherChannel port can be a SPAN source port; it cannot be a SPAN destination port.
- For SPAN source ports, you can monitor sent and received traffic for a single port or for a series or range of ports.
- When you configure a switch port as a SPAN destination port, it is no longer a normal switch port; only monitored traffic passes through the SPAN destination port.
- You can configure a disabled port to be a source or destination port, but the SPAN function does not start until the destination port and at least one source port is enabled.
- A SPAN destination port never participates in any VLAN spanning tree. SPAN does include BPDUs in the monitored traffic, so any spanning-tree BPDUs received on the SPAN destination port for a SPAN session were copied from the SPAN source ports.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 930
3702
Doc:

- When SPAN is enabled, configuration changes have these results:
  - If you change the VLAN configuration of a destination port, the change is not effective until SPAN is disabled.
  - If you disable all source ports or the destination port, the SPAN function stops until both a source and the destination port are enabled.

Creating a SPAN Session and Specifying Ports to Monitor

Beginning in privileged EXEC mode, follow these steps to create a SPAN session and specify the source (monitored) and destination (monitoring) ports:

	Command	Purpose
1	**configure terminal**	Enter global configuration mode.
Step 2	**no monitor session** {*session_number* | **all** | **local** | **remote**}	Clear any existing SPAN configuration for the session. For *session_number*, specify 1. Specify **all** to remove all SPAN sessions, **local** to remove all local sessions, or **remote** to remove all remote SPAN sessions.
Step 3	**monitor session** *session_number* **source interface** *interface-id* [**,** | **-**] [**both** | **rx** | **tx**]	Specify the SPAN session and the source port (monitored port). For *session_number*, specify 1. For *interface-id*, specify the source port to monitor. Valid interfaces include physical interfaces and port-channel logical interfaces (**port-channel** *port-channel-number*). (Optional) [**,** | **-**] Specify a series or range of interfaces. Enter a space before and after the comma; enter a space before and after the hyphen. (Optional) Specify the direction of traffic to monitor. If you do not specify a traffic direction, the source interface sends both sent and received traffic. • **both**—Monitor both received and sent traffic. • **rx**—Monitor received traffic. • **tx**—Monitor sent traffic.
Step 4	**monitor session** *session_number* **destination interface** *interface-id* [**encapsulation** {**dot1q**}]	Specify the SPAN session and the destination port (monitoring port). For *session_number*, specify 1. For *interface-id*, specify the destination port. Valid interfaces include physical interfaces. (Optional) Specify the encapsulation header for outgoing packets. If not specified, packets are sent in native form. • **dot1q**—Use 802.1Q encapsulation.
Step 5	**end**	Return to privileged EXEC mode.
Step 6	**show monitor** [**session** *session_number*]	Verify your entries.
Step 7	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 931
3702
Doc:

This example shows how to set up a SPAN session, session 1, for monitoring source port traffic to a destination port. First, any existing SPAN configuration for session 1 is cleared, and then bidirectional traffic is mirrored from source port 1 to destination port 10.

```
Switch(config)# no monitor session 1
Switch(config)# monitor session 1 source interface fastEthernet0/1
Switch(config)# monitor session 1 destination interface fastEthernet0/10
encapsulation dot1q
Switch(config)# end
```

Creating a SPAN Session and Enabling Ingress Traffic

Beginning in privileged EXEC mode, follow these steps to create a SPAN session, to specify the source and destination ports, and to enable ingress traffic on the destination port for a network security device (such as a Cisco IDS Sensor Appliance):

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**no monitor session** {*session_number* | **all** | **local** | **remote**}	Clear any existing SPAN configuration for the session. For *session_number*, specify 1. Specify **all** to remove all SPAN sessions, **local** to remove all local sessions, or **remote** to remove all remote SPAN sessions.
Step 3	**monitor session** *session_number* **source interface** *interface-id* [, | -] [**both** | **rx** | **tx**]	Specify the SPAN session and the source port (monitored port). For *session_number*, specify 1. For *interface-id*, specify the source port to monitor. Valid interfaces include physical interfaces and port-channel logical interfaces (**port-channel** *port-channel-number*). (Optional) [, | -] Specify a series or range of interfaces. Enter a space before and after the comma; enter a space before and after the hyphen. (Optional) Specify the direction of traffic to monitor. If you do not specify a traffic direction, the source interface sends both sent and received traffic. • **both**—Monitor both received and sent traffic. • **rx**—Monitor received traffic. • **tx**—Monitor sent traffic.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 932
Doc: 3702

Nº 857

	Command	Purpose
Step 4	**monitor session** *session_number* **destination interface** *interface-id* [**encapsulation** {**dot1q**}] [**ingress vlan** *vlan id*]	Specify the SPAN session, the destination port (monitoring port), the packet encapsulation, and the ingress VLAN. For *session_number*, specify 1. For *interface-id*, specify the destination port. Valid interfaces include physical interfaces. (Optional) Specify the encapsulation header for outgoing packets. If not specified, packets are sent in native form. • **dot1q**—Use 802.1Q encapsulation. (Optional) Enter **ingress vlan** *vlan id* to enable ingress forwarding and specify a default VLAN.
Step 5	**end**	Return to privileged EXEC mode.
Step 6	**show monitor** [**session** *session_number*]	Verify your entries.
Step 7	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

This example shows how to configure the destination port for ingress traffic on VLAN 5 by using a security device that does not support 802.1Q encapsulation.

```
Switch(config)# monitor session 1 destination interface Fa 0/5 ingress vlan 5
```

This example shows how to configure the destination port for ingress traffic on VLAN 5 by using a security device that supports 802.1Q encapsulation.

```
Switch(config)# monitor session 1 destination interface Fa 0/5 encapsulation dot1q ingress
vlan 5
```

This example shows how to disable ingress traffic forwarding on the destination port.

```
Switch(config)# monitor session 1 destination interface Fa 0/5 encapsulation dot1q
```


RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 933
Nº 3702
Doc:

Removing Ports from a SPAN Session

Beginning in privileged EXEC mode, follow these steps to remove a port as a SPAN source for a session:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**no monitor session** *session_number* **source interface** *interface-id* [**,** | **-**] [**both** | **rx** | **tx**]	Specify the characteristics of the source port (monitored port) and SPAN session to remove. For *session*, specify 1. For *interface-id*, specify the source port to no longer monitor. Valid interfaces include physical interfaces and port-channel logical interfaces (**port-channel** *port-channel-number*). (Optional) Use [**,** | **-**] to specify a series or range of interfaces if they were configured. This option is valid when monitoring only received traffic. Enter a space before and after the comma; enter a space before and after the hyphen. (Optional) Specify the direction of traffic (**both**, **rx**, or **tx**) to no longer monitor. If you do not specify a traffic direction, both transmit and receive are disabled.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show monitor** [**session** *session_number*]	Verify your entries.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To remove a source or destination port from the SPAN session, use the **no monitor session** *session_number* **source interface** *interface-id* global configuration command or the **no monitor session** *session_number* **destination interface** *interface-id* global configuration command. To change the encapsulation type back to the default (native), use the **monitor session** *session_number* **destination interface** *interface-id* without the **encapsulation** keyword.

This example shows how to remove port 1 as a SPAN source for SPAN session 1:

```
Switch(config)# no monitor session 1 source interface fastEthernet0/1
Switch(config)# end
```

This example shows how to disable received traffic monitoring on port 1, which was configured for bidirectional monitoring:

```
Switch(config)# no monitor session 1 source interface fastEthernet0/1 rx
```

The monitoring of traffic received on port 1 is disabled, but traffic sent from this port continues to be monitored.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls' Nº 934
3702
Doc:

Configuring RSPAN

This section describes how to configure RSPAN on your switch. It contains this configuration information:

- RSPAN Configuration Guidelines, page 22-12
- Creating an RSPAN Session, page 22-13
- Creating an RSPAN Destination Session, page 22-14
- Removing Ports from an RSPAN Session, page 22-15

RSPAN Configuration Guidelines

To use the RSPAN feature described in this section, you must have the EI installed on your switch. Follow these guidelines when configuring RSPAN:

- All the items in the "SPAN Configuration Guidelines" section on page 22-7 apply to RSPAN.

Note As RSPAN VLANs have special properties, you should reserve a few VLANs across your network for use as RSPAN VLANs; do not assign access ports to these VLANs.

- RSPAN sessions can coexist with SPAN sessions within the limits described in the "SPAN and RSPAN Session Limits" section on page 22-6.
- For RSPAN configuration, you can distribute the source ports and the destination ports across multiple switches in your network.
- A port cannot serve as an RSPAN source port or RSPAN destination port while designated as an RSPAN reflector port.
- When you configure a switch port as a reflector port, it is no longer a normal switch port; only looped-back traffic passes through the reflector port.
- RSPAN does not support BPDU packet monitoring or other Layer 2 switch protocols.
- In a network consisting of only Catalyst 2950 or Catalyst 2955 switches, you must use a unique RSPAN VLAN session on each source switch. If more than one source switch uses the same RSPAN VLAN, the switches are limited to act only as source switches to ensure the delivery of all monitored traffic to the destination switch.
- You can configure any VLAN as an RSPAN VLAN as long as these conditions are met:
  - The RSPAN VLAN is not configured as a native VLAN.
  - Extended range RSPAN VLANs will not be propagated to other switches using VTP.
  - No access port is configured in the RSPAN VLAN.
  - All participating switches support RSPAN.

Note The RSPAN VLAN cannot be VLAN 1 (the default VLAN) or VLAN IDs 1002 through 1005 (reserved to Token Ring and FDDI VLANs).

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 935
Nº 3702
Doc:

- You should create an RSPAN VLAN before configuring an RSPAN source or destination session.
- If you enable VTP and VTP pruning, RSPAN traffic is pruned in the trunks to prevent the unwanted flooding of RSPAN traffic across the network for VLAN-IDs that are lower than 1005.

Creating an RSPAN Session

First create an RSPAN VLAN that *does not* exist for the RSPAN session in any of the switches that will participate in RSPAN. With VTP enabled in the network, you can create the RSPAN VLAN in one switch, and VTP propagates it to the other switches in the VTP domain for VLAN-IDs that are lower than 1005. See the "Creating or Modifying an Ethernet VLAN" section on page 15-8 for more information about creating an RSPAN VLAN.

Use VTP pruning to get efficient flow of RSPAN traffic, or manually delete the RSPAN VLAN from all trunks that do not need to carry the RSPAN traffic.

After creating the RSPAN VLAN, begin in privileged EXEC mode, and follow these steps to start an RSPAN source session and to specify the source (monitored) ports and the destination RSPAN VLAN.

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**no monitor session** {*session_number* | **all** | **local** | **remote**}	Clear any existing RSPAN configuration for the session. For *session_number*, specify the session number identified with this RSPAN session. Specify **all** to remove all RSPAN sessions, **local** to remove all local sessions, or **remote** to remove all remote SPAN sessions.
Step 3	**monitor session** *session_number* **source interface** *interface-id* [, | -] [**both** | **rx** | **tx**]	Specify the RSPAN session and the source port (monitored port). For *session_number*, specify the session number identified with this RSPAN session. For *interface-id*, specify the source port to monitor. Valid interfaces include physical interfaces and port-channel logical interfaces (**port-channel** *port-channel-number*). (Optional) [, | -] Specify a series or range of interfaces. Enter a space before and after the comma; enter a space before and after the hyphen. (Optional) Specify the direction of traffic to monitor. If you do not specify a traffic direction, the source interface sends both sent and received traffic. • **both**—Monitor both received and sent traffic. • **rx**—Monitor received traffic. • **tx**—Monitor sent traffic.

RQS nº 03/2005 - CN - CPMI - CORREIOS
22-13
Fls Nº 936
Doc 3702

16.853
2

	Command	Purpose
Step 4	**monitor session** *session_number* **destination remote vlan** *vlan-id* **reflector-port** *interface*	Specify the RSPAN session, the destination remote VLAN, and the reflector port. For *session_number*, enter the session number identified with this RSPAN session. For *vlan-id*, specify the RSPAN VLAN to carry the monitored traffic to the destination port. (See the "Creating or Modifying an Ethernet VLAN" section on page 15-8 for more information about creating an RSPAN VLAN.) For *interface*, specify the interface that will flood the RSPAN traffic onto the RSPAN VLAN.
Step 5	**end**	Return to privileged EXEC mode.
Step 6	**show monitor** [**session** *session_number*]	Verify your entries.
Step 7	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

This example shows how to clear any existing RSPAN configuration for session 1, configure RSPAN session 1 to monitor multiple source interfaces, and configure the destination RSPAN VLAN and the reflector-port.

```
Switch(config)# no monitor session 1
Switch(config)# monitor session 1 source interface fastEthernet0/10 tx
Switch(config)# monitor session 1 source interface fastEthernet0/2 rx
Switch(config)# monitor session 1 source interface fastEthernet0/3 rx
Switch(config)# monitor session 1 source interface port-channel 102 rx
Switch(config)# monitor session 1 destination remote vlan 901 reflector-port
fastEthernet0/1
Switch(config)# end
```

Creating an RSPAN Destination Session

Beginning in privileged EXEC mode, follow these steps to create an RSPAN destination session and to specify the source RSPAN VLAN and the destination port:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**monitor session** *session_number* **source remote vlan** *vlan-id*	Specify the RSPAN session and the source RSPAN VLAN. For *session_number*, specify the session number identified with this RSPAN session. For *vlan-id*, specify the source RSPAN VLAN to monitor.
Step 3	**monitor session** *session_number* **destination interface** *interface-id* [**encapsulation** {**dot1q**}]	Specify the RSPAN session and the destination interface. For *session_number*, specify the session number identified with this RSPAN session. For *interface-id*, specify the destination interface. (Optional) Specify the encapsulation header for outgoing packets. If not specified, packets are sent in native form. • **dot1q**—Use 802.1Q encapsulation.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 937
Nº 3702 Doc

16.852

	Command	Purpose
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show monitor** [**session** *session_number*]	Verify your entries.
Step 6	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

This example shows how to configure VLAN 901 as the source remote VLAN and port 5 as the destination interface:

```
Switch(config)# monitor session 1 source remote vlan 901
Switch(config)# monitor session 1 destination interface fastEthernet0/5
Switch(config)# end
```

Removing Ports from an RSPAN Session

Beginning in privileged EXEC mode, follow these steps to remove a port as an RSPAN source for a session:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**no monitor session** *session_number* **source interface** *interface-id* [**,** | **-**] [**both** | **rx** | **tx**]	Specify the characteristics of the RSPAN source port (monitored port) to remove. For *session_number*, specify the session number identified with this RSPAN session. For *interface-id*, specify the source port to no longer monitor. Valid interfaces include physical interfaces and port-channel logical interfaces (**port-channel** *port-channel-number*). (Optional) Use [**,** | **-**] to specify a series or range of interfaces if they were configured. Enter a space before and after the comma; enter a space before and after the hyphen. (Optional) Specify the direction of traffic (**both**, **rx**, or **tx**) to no longer monitor. If you do not specify a traffic direction, both transmit and receive are disabled.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show monitor** [**session** *session_number*]	Verify your entries.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

This example shows how to remove port 1 as an RSPAN source for RSPAN session 1:

```
Switch(config)# no monitor session 1 source interface fastEthernet0/1
Switch(config)# end
```

This example shows how to disable received traffic monitoring on port 1, which was configured for bidirectional monitoring:

```
Switch(config)# no monitor session 1 source interface fastEthernet0/1 rx
```

The monitoring of traffic received on port 1 is disabled, but traffic sent from this port continues to be monitored.

RQS nº 03/2005 - CN - CPMI - CORREIOS
22-15
Fls Nº 938
3702
Doc:

Displaying SPAN and RSPAN Status

To display the status of the current SPAN or RSPAN configuration, use the **show monitor** privileged EXEC command.

This is an example of output for the **show monitor** privileged EXEC command for SPAN source session 1:

```
Switch# show monitor session 1
Session 1
---------
Type                : Local Session
Source Ports        :
    RX Only         : None
    TX Only         : None
    Both            : Fa0/4
Source VLANs        :
    RX Only         : None
    TX Only         : None
    Both            : None
Source RSPAN VLAN   : None
Destination Ports   : Fa0/5
    Encapsulation: DOT1Q
          Ingress: Enabled, default VLAN = 5
Reflector Port      : None
Filter VLANs        : None
Dest RSPAN VLAN     : None
```


RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 939
3702

ANEXO (11)

16.850

Overview

The GigaStack GBIC (model WS-X3500-XL) adds port density and high-performance connectivity to supporting switches. When installed in a supporting switch, the GigaStack GBIC supports Gigabit connections in a cascaded stack or point-to-point configuration. The GigaStack GBIC autonegotiates the duplex setting of each port to maximize the bandwidth for your configuration.

Features

This section describes the GigaStack GBIC features:

- Half-duplex stacking using only one GBIC slot for each switch

  Stack up to nine switches to form an independent backbone that can be managed with a single IP address. This stack gives the appearance of a single large switch for network management purposes. For this kind of connectivity, see the "Example 1: Cascaded Stack Connection" section on page 1-9.

- Full-duplex connectivity between two switches

  You can also form a point-to-point link between two switches. The GigaStack GBIC supports one full-duplex link (in a point-to-point configuration) or up to eight half-duplex links (in a stack configuration) to other Gigabit Ethernet devices. For this kind of connectivity, see the "Example 2: Point-to-Point Connection" section on page 1-10.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 940
3702
Doc:

16 849

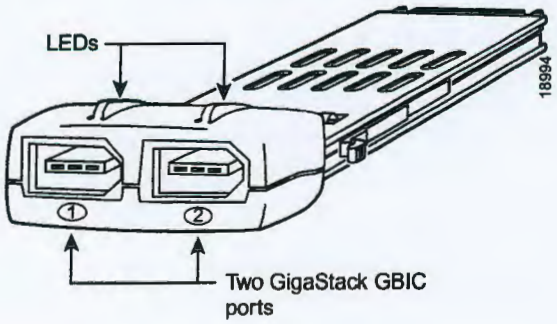
- Support for redundant loop configurations in a GigaStack GBIC stack

  For more information, see the "Minimum IOS Release for Redundant Loop Configurations" section on page 1-7 and the "Cascaded Stack Connections with a Redundant Link" section on page 2-12
- Support for IOS Release 12.0(5)XU or later for Catalyst 2900 XL and 3500 XL switches, support for Release 12.1(6)EA2 or later for Catalyst 2950 switches, and support for Release 12.1(4)EA1 or later for Catalyst 3550 multilayer switches
- Management through the Cisco IOS command-line interface (CLI) or the web-based Cluster Management Suite (CMS)
- Field-replaceable

GigaStack GBIC LEDs

Figure 1-1 shows the LED locations on the GigaStack GBIC, and Table 1-1 describes the LED colors and their meanings.

Figure 1-1 GigaStack GBIC LEDs and Ports



RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 941
Doc 3702

16 848
2

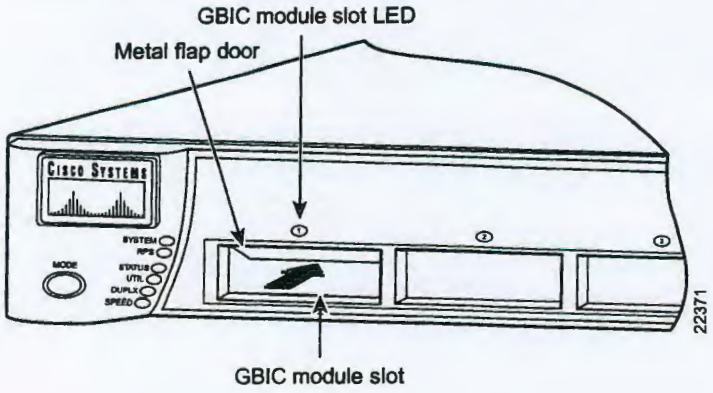
Table 1-1 GigaStack GBIC LEDs

Color	Meaning
Off	No link.
Green	Link present. This link occurs if there is connectivity with another network device and the GigaStack GBIC port.
Amber	Power-on self-test (POST) failure or use of an incorrect cable.
Flashing amber	Loop detection activated.

GBIC Module Slot LEDs

Figure 1-2 shows the GBIC module slot LED on the front of a supporting switch, and Figure 1-3 shows the GBIC LED location when the GigaStack GBIC is installed in the 1000BASE-X module.

Figure 1-2 GBIC Module Slot LED Location on a Switch



RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 942
Doc: 3702

16 817
L

Figure 1-3 GBIC LED Location on a 1000BASE-X Module

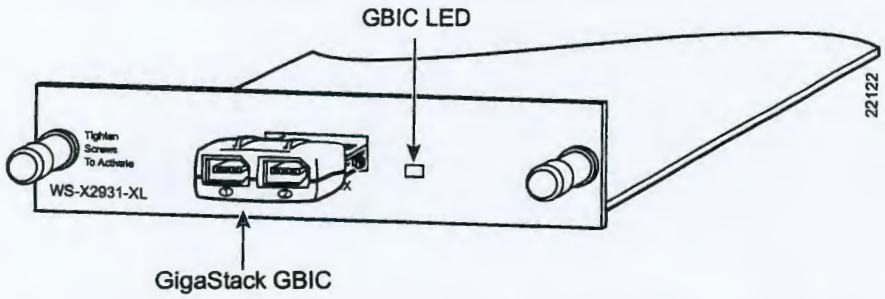


Table 1-2 describes the switch and 1000BASE-X module GBIC slot LED colors and port status.

Table 1-2 Switch and 1000BASE-X Module GBIC Slot LEDs

Color	Meaning
Off	No link, or port was administratively shut down.
Green	Link present.
Flashing green	Activity. Port is transmitting or receiving data.
Alternating green-amber	Link fault. Error frames can affect connectivity, and errors such as excessive collisions, cyclic redundancy check (CRC) errors, and alignment and jabber errors are monitored for a link-fault indication.
Solid amber	Port is blocked by Spanning Tree Protocol (STP) and is not forwarding data. **Note** After a port is reconfigured, the port LED can remain amber for up to 30 seconds as STP checks the switch for possible loops.
Flashing amber	Port is blocked by STP and is sending or receiving packets.

Cabling Guidelines

The GigaStack GBIC uses the following Cisco proprietary cables. See Figure 1-4 and Table 1-3 for more information.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 943
Doc: 3702

16.346
L

The maximum distance for a GBIC-to-GBIC connection is 1 meter. The GigaStack GBIC requires Cisco proprietary signaling and cabling. For more information about cabling, see Appendix B, "Connectors and Cables."

Figure 1-4 GigaStack GBIC Cables

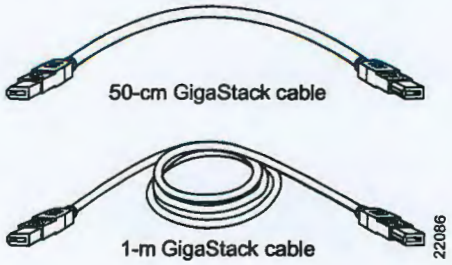


Table 1-3 GigaStack GBIC Cable Part Numbers

Part Number	Cable Length
CAB-GS-50CM	50 cm
CAB-GS-1M	1 m

The 50-cm cable comes with the GigaStack GBIC. You can order additional cables.

Caution Do not use standard IEEE 1394 cables with the GigaStack GBIC. You must use one of the Cisco proprietary cables (CAB-GS-50CM or CAB-GS-1M). If you use any other cable, you will not have connectivity.

Caution Do not use the GigaStack GBIC with standard IEEE 1394 equipment. You might damage the equipment or lose data.

RQS nº 03/2005 - CN - CPMI - CORREIOS
944
Nº Fls Nº 3702
Doc:

16.845
2

Switches Supporting the GBIC

Refer to the online *GigaStack Gigabit Interface Converter Switch Compatibility Matrix* listed with the GBIC documentation on www.cisco.com for the most current list of products supporting the GBIC.

Caution Installing the GBIC in or connecting it to an unauthorized device might cause damage to the GBIC, the other device, or both.

Table 1-4 lists the switches and the module supporting the GigaStack GBIC.

Table 1-4 Switches and Module Supporting the GigaStack GBIC

Switch Series or Module	Model Number	Description
WS-X2931-XL module for Catalyst 2900 series XL switches	WS-X2931-XL	1 1000BASE-X port[1]
Catalyst 2900 XL switches	Catalyst 2912MF XL	12 100BASE-FX ports and 2 module slots
	Catalyst 2924M XL	24 autosensing 10/100 Ethernet ports and 2 module slots
Catalyst 2950 switches	Catalyst 2950G-12-EI	12 autosensing 10/100 Ethernet ports and 2 GBIC module slots
	Catalyst 2950G-24-EI	24 autosensing 10/100 Ethernet ports and 2 GBIC module slots
	Catalyst 2950G-24-EI-DC	24 autosensing 10/100 Ethernet ports and 2 GBIC module slots with DC-input power
	Catalyst 2950G-48-EI	48 autosensing 10/100 Ethernet ports and 2 GBIC module slots

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 945
Nº 3702
Doc:

16.845
2

Switch Series or Module	Model Number	Description
Catalyst 3500 XL switches	Catalyst 3508G XL	8 GBIC module slots
	Catalyst 3512 XL	12 autosensing 10/100 Ethernet ports and 2 GBIC module slots
	Catalyst 3524 XL	24 autosensing 10/100 Ethernet ports and 2 GBIC module slots
	Catalyst 3524 PWR XL	24 autosensing 10/100 inline-power Ethernet ports and 2 GBIC module slots
	Catalyst 3548 XL	48 autosensing 10/100 Ethernet ports and 2 GBIC module slots
Catalyst 3550 switches	Catalyst 3550-12G	2 autosensing 10/100/1000 Ethernet ports and 10 GBIC module slots
	Catalyst 3550-12T	10 autosensing 10/100/1000 Ethernet ports and 2 GBIC module slots
	Catalyst 3550-24-SMI Catalyst 3550-24-EMI	24 autosensing 10/100 Ethernet ports and 2 GBIC module slots
	Catalyst 3550-48-SMI Catalyst 3550-48-EMI	48 autosensing 10/100 Ethernet ports and 2 GBIC module slots

1. The 1000BASE-X module provides one switched 1000-Mbps port in half-duplex, full-duplex, or autonegotiation mode for a GigaStack GBIC. The port supports the IEEE 802.3Z 1000BASE-X standard.

Minimum IOS Release for Redundant Loop Configurations

To ensure support for redundant loop configurations when using the GigaStack GBIC in a cascaded stack configuration, make sure that every switch in the stack is running at least the minimum IOS Release listed in Table 1-5.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
946
Fls Nº
3702
Doc:

16.844
L

Table 1-5 Minimum IOS Release for Redundant Loop Configurations

Supported Switch	Minimum IOS Release
Modular 2900 XL switches	12.0(5)XU (April 2000)
2950 switches	12.1(6)EA2 (December 2000)
3500 XL switches	12.0(5)XU (April 2000)
3550 multilayer switches	12.1(4)EA1 (May 2001)

Note All switches in a series must run the same software version. For example, if the stack includes only Catalyst 2900 series XL and 3500 series XL switches, they must run Release 12.0(5)XU or later. If the stack includes a mixture of Catalyst 2900 series XL, 3500 series XL, 2950, and 3550 switches, all the 2900 XL and 3500 XL switches must run Release 12.0(5)XW or later, all the Catalyst 2950 switches must run Release 12.1(6)EA2 or later, and all the Catalyst 2950 switches must run Release 12.1(4)EA1 or later.

For more information, see the "Cascaded Stack Connections with a Redundant Link" section on page 2-12. For switch software upgrade information, refer to the release notes for your switch.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 947
Nº 3702

16.843

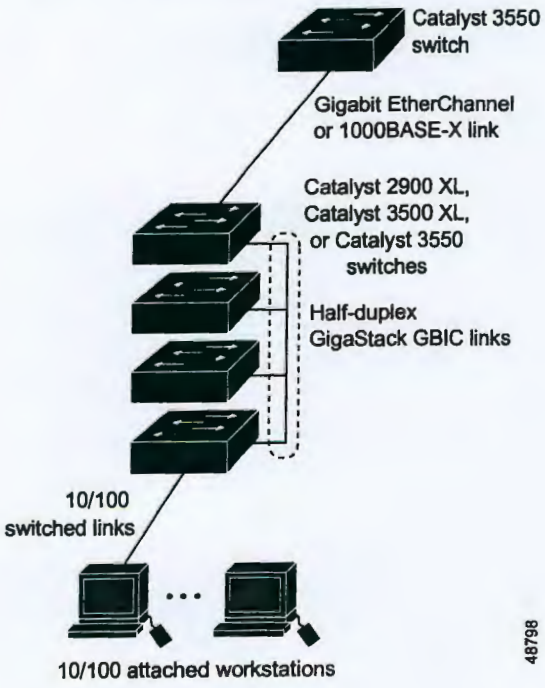
Deployment Examples

This section contains examples that use the GigaStack GBIC as a Gigabit uplink to aggregate traffic in a switched and shared network.

Example 1: Cascaded Stack Connection

Figure 1-5 shows the GigaStack GBIC cascaded in a half-duplex stack configuration.

Figure 1-5 Cascaded Stack Connection



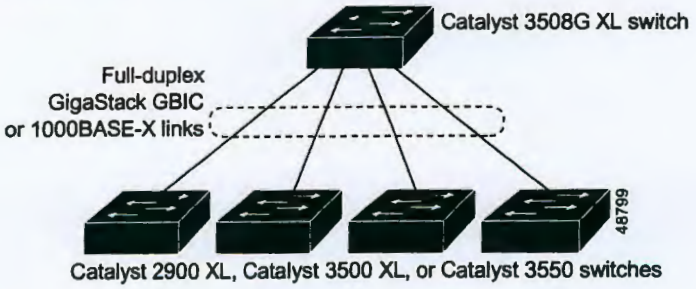
RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 948
3702
Doc

16 842

Example 2: Point-to-Point Connection

Figure 1-6 shows the 3500 XL switch aggregating traffic by using a GigaStack GBIC as a full-duplex, point-to-point uplink connection.

Figure 1-6 Point-to-Point Connection



RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 949
Doc: 3702

16 841
i

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems Europe
11, Rue Camille Desmoulins
92782 Issy-les-Moulineaux
Cedex 9
France
www.cisco.com
Tel: 33 1 58 04 60 00
Fax: 33 1 58 04 61 00

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems Australia, Pty., Ltd
Level 9, 80 Pacific Highway
P.O. Box 469
North Sydney
NSW 2060 Australia
www.cisco.com
Tel: +61 2 8448 7100
Fax: +61 2 9957 4350

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the **Cisco.com Web site at www.cisco.com/go/offices.**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Czech Republic
Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel
Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal
Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden

All contents are Copyright © 1992-2001 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement. Printed in the USA. Catalyst, Cisco, Cisco IOS, Cisco Systems, the Cisco Systems logo, and EtherChannel are registered trademarks of Cisco Systems, Inc. or its affiliates in the U.S. and certain other countries.

All other brands, names, or trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0103R)

05/01 BW7243

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 950
Nº Doc: 3702

ANEXO (12)

16.840
2

Cisco Systems

Product Selector Guide:
Cisco Catalyst 3550 and 2950 Series Intelligent Ethernet Switches

Intelligent Switching for the **Evolving** Network

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 951
Doc 3702

16.859
L

An agent that precipitates
or accelerates a reaction,
development, or change.

Don't fear change, embrace it. With Cisco Catalyst Intelligent Ethernet switches, you can. By extending intelligent services to the network edge, they make it easy to adapt to changing requirements, so networks and network administrators can be ready for anything. Keep reading.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls 'Nº 952
Nº 3702

16.838

Q: Who needs intelligent services at the network edge?

A: Any organization that wants to grow.

Everything changes. People, organizations, and networks, too. Fortunately, it's now easier than ever to adjust and adapt to new networking requirements. The key is to extend intelligent services, beyond basic connectivity, to the network edge, where the users are. That way, a network is ready for whatever comes along, including:

- Increases in desktop computing power
- The emergence of more bandwidth-intensive applications
- The need to safeguard sensitive data
- The addition of wireless access points, IP phones, video equipment, and other network devices

Q: How do intelligent services ease network growth?

A: By delivering high availability, advanced quality of service, and enhanced security.

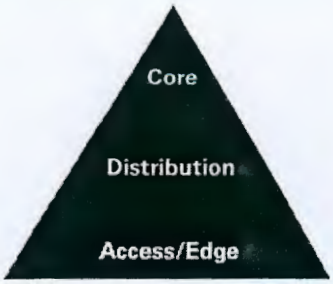
These three areas of network performance become more vital as networks grow and evolve. Consider the role they each play:

- High availability ensures users can access the network whenever necessary, keeping productivity at a maximum even as the demands on the network rise
- Advanced quality of service (QoS) classifies, prioritizes, and controls network traffic, so time-sensitive applications like voice and video are handled first, without leaving less urgent applications starved for bandwidth
- Enhanced security protects the network from internal and external threats by authenticating users, restricting access to data and controls, and isolating traffic en route to its destination

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 953
Nº Doc. 3702

16.837
L

The Local-Area Network (LAN)



Core (or Backbone) This serves as the primary path for traffic moving between, rather than within, local-area networks. Layer 3 and 4–7 services are usually required to meet the core's rigorous performance, density, and functionality demands. Seen here at the top of the hierarchical model, the core is often physically located in a separate building from the rest of the network, requiring fiber connectivity.

Distribution/Aggregation Layer As the name suggests, this serves as a point of aggregation and distribution between the network core and the access layer, or edge. In other words, it is the layer of the network through which the core and the access layer communicate. In most networks, Layer 2–7 services are needed here as well.

In some networks, there may not be a clear separation between the network layers. The functions will be consolidated in an area sometimes referred to as a "collapsed backbone." A multilayer switch with intelligent services is generally introduced to enhance performance of small and medium-sized networks.

Access Layer (or Edge) As the outermost part of the network, the access layer directly connects users to the network, and typically consists of several switches located in a nearby wiring closet. The only network devices beyond the access layer would be IP phones, wireless access points, or other customer premises equipment. Layer 2 switching is most often found here, though Layer 3 and 4 services delivered by an intelligent switch are increasingly common.

Deploying intelligent services at the network edge is the focus of this guide.

The OSI Model

The Open System Interconnection (OSI) model uses seven layers to define a networking framework for implementing protocols. Two are commonly referenced when describing a type of switch and are relevant to this discussion of LAN switching at the network edge: Layer 2 and Layer 3.

Layer 2: The data link layer in the OSI model is concerned with procedures and protocols for operating the communications lines.

Layer 3: The network layer in the OSI model determines how data is transferred between computers. It also addresses routing within and between individual networks.

Multilayer Switching

Layer 2 and Layer 3 are terms that are often used to describe the types of functions performed by switches. Switching technology had previously been limited to the processing of information contained in Layer 2. Current technology has progressed to yield a more advanced switch labeled as a "multilayer switch." These switches are able to look deeper into the packet and make decisions based on Layer 2, Layer 3, and even Layer 4 (the transport layer in the OSI model) information. Cisco has implemented this technology to provide sophisticated intelligent services such as security, availability, and QoS that are easy for IT managers to deploy in a Layer 2 device.

Intelligent multilayer switching means that access layer switches can now perform more than basic broadcasting and store-and-forward functions. In fact, Cisco Catalyst desktop switches can now perform security filtering, highly granular rate-limiting, and advanced QoS—in addition to IP routing at Layer 3, in some products. As a result, traffic flows more efficiently through the network, helping to prevent bottlenecks. Intelligent switching also provides a superior level of control over network traffic, making it easier to adjust to changing requirements and priorities.

Recommendations

The requirements for Layer 2–4 intelligent services vary based on the location in the network. It is recommended that small and medium-sized networks deploy intelligent services such as security filtering, QoS, multicast management, and rate-limiting, beginning at the network edge or access layer. Additionally, in small and medium-sized networks with enterprise-class requirements—such as maximum availability, greater deployment flexibility, and heightened network control, routed uplinks from the access layer are recommended.

To meet the availability and performance demands of the core and distribution layers of the network, multilayer intelligent services are recommended, including IP routing. Gigabit connectivity is often required, and can be delivered either through fixed 10/100/1000 ports or gigabit interface card (GBIC) slots.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 954
Doc: 3702

16.836
2

Q: Why focus on the network edge?

A: To complete the picture.

Until now, network intelligence has been limited to the core. As the demands on *small and medium-sized networks* increase, so does the need for high availability, advanced QoS, and enhanced security at the network edge.

When intelligent services are extended to the edge, data traffic can be classified and marked at the source, allowing both upstream and downstream traffic to be prioritized to minimize congestion and optimize the network for time-sensitive applications such as IP telephony or videoconferencing.

Extending intelligence to the network edge also makes it possible for network administrators to set up policies on a per-user basis, and frees up router processing power.

Q: Beyond intelligent services, what else should be considered when choosing a switch?

A: Keep future requirements and applications in mind.

The switches you deploy today must support the organization's needs tomorrow. So it's worth taking a minute to evaluate likely future requirements, not only in terms of bandwidth, but also with regard to any new technologies or applications on the horizon. For many organizations, IP telephony and wireless access are at the top of the list.

IP Telephony

The integration of IP telephony services into the data network has the potential to drive major changes in institutions by delivering information more efficiently than today's dual-network approach. A converged voice, video, and data network improves customer care capabilities, increases employee productivity, and enhances corporate agility by simplifying moves, adds, and changes.

To accommodate IP telephony, switches should support:

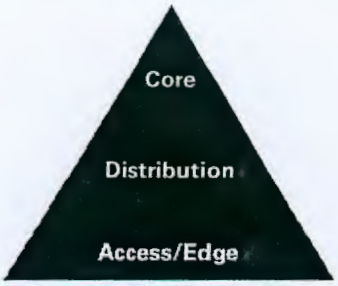
- Network-based inline power, which eliminates the need to connect each IP phone to a wall outlet or other power source
- Voice virtual LANs (VLANs) to create a separate path for voice traffic, simplifying network administration and troubleshooting
- Advanced QoS so voice traffic can be prioritized over less delay-sensitive traffic
- Port security to isolate voice traffic and prevent eavesdropping

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 955
Doc: 3702

16.835
2

Intelligence at the Edge

The Local-Area Network (LAN)



Core (or Backbone) This serves as the primary path for traffic moving between, rather than within, local-area networks. Layer 3 and 4–7 services are usually required to meet the core's rigorous performance, density, and functionality demands. Seen here at the top of the hierarchical model, the core is often physically located in a separate building from the rest of the network, requiring fiber connectivity.

Distribution/Aggregation Layer As the name suggests, this serves as a point of aggregation and distribution between the network core and the access layer, or edge. In other words, it is the layer of the network through which the core and the access layer communicate. In most networks, Layer 2–7 services are needed here as well.

In some networks, there may not be a clear separation between the network layers. The functions will be consolidated in an area sometimes referred to as a "collapsed backbone." A multilayer switch with intelligent services is generally introduced to enhance performance of small and medium-sized networks.

Access Layer (or Edge) As the outermost part of the network, the access layer directly connects users to the network, and typically consists of several switches located in a nearby wiring closet. The only network devices beyond the access layer would be IP phones, wireless access points, or other customer premises equipment. Layer 2 switching is most often found here, though Layer 3 and 4 services delivered by an intelligent switch are increasingly common.

Deploying intelligent services at the network edge is the focus of this guide.

The OSI Model

The Open System Interconnection (OSI) model uses seven layers to define a networking framework for implementing protocols. Two are commonly referenced when describing a type of switch and are relevant to this discussion of LAN switching at the network edge: Layer 2 and Layer 3.

Layer 2: The data link layer in the OSI model is concerned with procedures and protocols for operating the communications lines.

Layer 3: The network layer in the OSI model determines how data is transferred between computers. It also addresses routing within and between individual networks.

Multilayer Switching

Layer 2 and Layer 3 are terms that are often used to describe the types of functions performed by switches. Switching technology had previously been limited to the processing of information contained in Layer 2. Current technology has progressed to yield a more advanced switch labeled as a "multilayer switch." These switches are able to look deeper into the packet and make decisions based on Layer 2, Layer 3, and even Layer 4 (the transport layer in the OSI model) information. Cisco has implemented this technology to provide sophisticated intelligent services such as security, availability, and QoS that are easy for IT managers to deploy in a Layer 2 device.

Intelligent multilayer switching means that access layer switches can now perform more than basic broadcasting and store-and-forward functions. In fact, Cisco Catalyst desktop switches can now perform security filtering, highly granular rate-limiting, and advanced QoS—in addition to IP routing at Layer 3, in some products. As a result, traffic flows more efficiently through the network, helping to prevent bottlenecks. Intelligent switching also provides a superior level of control over network traffic, making it easier to adjust to changing requirements and priorities.

Recommendations

The requirements for Layer 2–4 intelligent services vary based on the location in the network. It is recommended that small and medium-sized networks deploy intelligent services such as security filtering, QoS, multicast management, and rate-limiting, beginning at the network edge or access layer. Additionally, in small and medium-sized networks with enterprise-class requirements—such as maximum availability, greater deployment flexibility, and heightened network control, routed uplinks from the access layer are recommended.

To meet the availability and performance demands of the core and distribution layers of the network, multilayer intelligent services are recommended, including IP routing. Gigabit connectivity is often required, and can be delivered either through fixed 10/100/1000 ports or gigabit interface converter (GBIC) slots.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 956
Nº Doc: 3702

16.834
2

Q: Why use Cisco Catalyst 3550 and 2950 Series switches to deploy intelligent services at the network edge?

A: There are several reasons why they stand above the competition.

- Cisco Catalyst 3550 and 2950 Series switches are part of a larger family of switches that also includes Cisco Catalyst 6500 and 4000 Series switches, offering industry-leading performance, functionality, scalability, and flexibility in a range of standalone, stackable, and chassis configurations
- Cisco Catalyst 3550 and 2950 Series switches support advanced features and services which can help you differentiate your business by bringing valuable enhancements to your network operations
- Cisco Cluster Management Suite (CMS) Software is embedded in Cisco Catalyst 3550 and 2950 Series switches, and provides wizards, configuration templates, and other tools that streamline tedious, time-consuming tasks and simplify the deployment of intelligent services
- Cisco network platforms and the Cisco IOS® Software on which they run are a unified system, providing a firm foundation for building Internet applications, and reducing training, management, and troubleshooting costs
- Cisco makes migrating to new technologies easy with end-to-end networking solutions, including the Cisco Aironet® family of wireless products and an edge-to-core IP telephony system with Cisco CallManager, IP phones, and voice VLAN technology
- Cisco solutions simplify the deployment, management, and use of advanced technologies, making both administrators and users more productive

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 957
Doc: 3702

16.83
2

Q: What sort of features and benefits do Cisco Catalyst 3550 Series Intelligent Ethernet switches offer?

A: Here are some highlights:

- **IP Routing** Increases network availability by extending Layer 3 functionality out of the wiring closet; features include Routing Information Protocol (RIP), Open Shortest Path First (OSPF), Interior Gateway Routing Protocol (IGRP), Enhanced IGRP (EIGRP), inter-VLAN routing, Protocol Independent Multicast (PIM), and Hot Standby Router Protocol (HSRP)
- **Advanced Quality of Service (QoS)** Prioritizes traffic to improve network performance, ensures critical needs are met first without starving low-priority traffic, and optimizes IP telephony, voice, and video applications; includes differentiated services code point (DSCP), strict priority queuing, Weighted Round Robin (WRR), and Weighted Random Early Detection (WRED)
- **Granular Rate Limiting** Controls the amount of bandwidth across any configured interface to ensure appropriate distribution of network resources at increments as low as 8 Kbps, giving administrators exceptionally granular control over bandwidth and ensuring users get the most out of the network
- **Security Access Control Lists (ACLs)** Governs access to all packets, either within or between VLANs, for additional security against internal and external threats; because filtering is performed in hardware, switching performance is not compromised
- **Cisco Cluster Management Suite (CMS) Software** Saves tremendous time and resources by simplifying network management tasks, with Web-based interfaces, wizards, and other tools that enable simultaneous configuration of up to 16 clustered switches
- **Multicast Management** Eases and improves delivery of multicast applications such as videoconferencing, corporate communications, distance learning, and software distribution through Cisco Group Management Protocol (CGMP)/ Internet Group Management Protocol (IGMP) snooping, CGMP server, and PIM
- **GBIC-based Connectivity** Offers tremendous deployment flexibility via built-in GBIC-based Gigabit Ethernet ports, accommodating a range of transceivers that includes the Cisco GigaStack® GBIC and 1000BASE-T, 1000BASE-SX, 1000BASE-LX/LH, 1000BASE-ZX, and Cisco CWDM GBICs; customers can implement one type of stacking and uplink configuration today, while keeping future options open

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 958
3702

16.832
D

Q: What sort of features and benefits do Cisco Catalyst 2950 Series switches offer?

A: It depends on the level of services you choose.

The Cisco Catalyst 2950 Series encompasses a range of switches to meet various needs. They generally fall into two subsets: Basic switches and Intelligent Ethernet switches. Intelligent Ethernet models support all the features and services of the basic models, plus much more, for the highest levels of availability, QoS, and security.

Cisco Catalyst 2950 Series Intelligent Ethernet Switches

- **Advanced QoS** Prioritizes traffic to improve network performance, ensures critical needs are met first, and enables IP telephony, voice, and video; includes DSCP, strict priority scheduling, and WRR
- **Rate Limiting** Controls the amount of bandwidth across any configured interface to ensure appropriate distribution of network resources—making the most of available bandwidth
- **Security Filters** Polices incoming traffic flows based on Layer 2, Layer 3, or Layer 4 access control parameters (ACPs) to prevent unauthorized data flows and protect against internal and external threats; because filtering is performed in hardware, switch performance is not compromised
- **Cisco CMS Software** Saves tremendous time and resources by simplifying network management tasks, with Web-based interfaces, wizards, and other tools that enable simultaneous configuration of up to 16 clustered switches
- **Multicast Management** Monitors and manages bandwidth for multicast applications such as videoconferencing, distance learning, and software distribution with IGMP snooping and broadcast and unicast storm control
- **GBIC-based Connectivity** Offers extreme flexibility via two built-in GBIC-based Gigabit Ethernet ports on Catalyst 2950G-12/24/48 switches, accommodating a range of transceivers, such as the Cisco GigaStack® GBIC and 1000BASE-T, 1000BASE-SX, 1000BASE-LX/LH, 1000BASE-ZX, and Cisco CWDM GBICs

Cisco Catalyst 2950 Series Switches

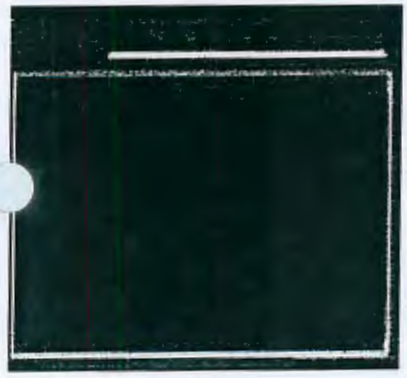
- **Availability** Increases network uptime and employee productivity with rapid failover recovery, Layer 2 load balancing, bandwidth aggregation, redundancy, and simplified administration

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 959
Nº 3702
Doc:

16.831
2

- **Security** Improves LAN security with capabilities that secure network management traffic through the protection of passwords and configuration information; that offer options for network security based on users, ports, and MAC addresses; and that enable more immediate responses to intruder and hacker detection
- **QoS** Increases network efficiency and ensures urgent needs are met by expediting time-sensitive applications such as IP voice and video—without starving low-priority packets—and providing control over the amount of bandwidth across any configured interface
- **Cisco CMS Software** Saves tremendous time and resources by simplifying network management tasks, with Web-based interfaces, wizards, and other tools that enable simultaneous configuration of up to 16 clustered switches

Q: Why is Cisco CMS Software so important?



Cisco CMS Software enables network managers to manage the entire LAN through a single Web interface.

A: Because it makes network management so easy.

From deploying and configuring hardware, to rolling out sophisticated new applications, and all the monitoring and troubleshooting tasks in between, Cisco CMS Software reduces complex tasks to a few simple clicks on a Web browser, anytime, anywhere. That means network administrators can save a lot of time, regardless of whether they choose to learn the command-line interface.

Cisco CMS software also ensures organizations can make the most of the latest technologies for high availability, advanced quality of service, and enhanced security. It comes embedded in Cisco Catalyst 3550 and 2950 Series switches, enabling network administrators to:

- Simultaneously manage up to 16 Catalyst 3550, 2950, 3500XL, and 2900XL switches using a standard Web browser, regardless of geographic proximity
- Use voice, video, data, and security wizards to optimize and configure sophisticated services
- Utilize the interactive Guide Mode for step-by-step configuration and context-sensitive online help
- Add features and update interconnected switches all at once with a simple, point-and-click interface

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 960
Nº 3702

16 850
L

Q: What's the difference between Cisco Catalyst 3550 Series SMI and EMI versions?

A: The difference is in the services.

The Cisco Catalyst 3550-24 and 3550-48 are available with either the Standard Multilayer Software Image (SMI) or the Enhanced Multilayer Software Image (EMI). The EMI provides a richer set of enterprise-class features, including hardware-based IP unicast and multicast routing, inter-VLAN routing, routed access control lists (RACLs), and Hot Standby Router Protocol (HSRP).

Basic routing (static and RIP routing) is provided in the SMI version (available Q3CY02).

An EMI upgrade kit gives users of the SMI version the flexibility to upgrade to the expanded set of routing features down the road.

The Cisco Catalyst 3550-12G and 3550-12T switches are available only with the EMI.

Q: What's the difference between the Cisco Catalyst 2950 Series SI and EI versions?

A: They support different services, and are embedded in different switch models.

Like the Cisco Catalyst 3550 Series, the Cisco Catalyst 2950 Series includes two software image versions that support different degrees of functionality—the Standard Image (SI) and the Enhanced Image (EI). But in this case, the version available depends solely on the model of switch selected, with no crossover or upgrade capabilities.

The SI version is embedded in Cisco Catalyst 2950-12/24 switches, and supports basic Cisco IOS functionality, Fast Ethernet connectivity, and cluster management.

The EI version supports all that and more. Embedded in Cisco Catalyst 2950T-24, 2950C-24, and 2950G-12/24/48 switches, it supports advanced intelligent services, gigabit connectivity, and a richer set of features. These include Cisco Spanning-Tree Protocol enhancements for high availability, access control parameters (ACPs) and Secure Shell (SSH) Protocol (available Q3CY02) for enhanced security, and Differentiated Services Code Point (DCSP) and rate limiting for advanced quality of service.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 961
Nº 3702 Doc:

16.829
L

Cisco Catalyst 3550 vs. 2950 Differentiation Matrix

	3550 Enhanced Multilayer Image	3550 Standard Multilayer Image	2950 Enhanced Image	2950 Standard Image
	Distribution/Aggregation: 3550-12T/G	Stackable: Catalyst 3550-24/48; 3550-24-FX; 3550-24-DC (Upgradeable to Enhanced Image)	Stackable: Catalyst 2950G-12, 2950G-24, 2950G-48; 2950G-24-DC Standalone: 2950C-24, 2950T-24	Basic Standalone: Catalyst 2950-12/24 (Not upgradeable to Enhanced Image)
	Aggregation: Medium-sized network/enterprise branch office distribution or small network core/backbone switch with fixed and GBIC-based gigabit/fiber connectivity.	Stackable: In medium-sized networks, serves as enterprise-class multilayer access switch and provides increased availability and control. Able to provide routed uplinks to the core to maximize network availability. Supports GBIC-based gigabit/fiber connectivity.	Stackable: Medium-sized network/enterprise branch office multilayer access switch with flexible GBIC-based gigabit/fiber connectivity. Standalone: Medium-sized/ enterprise branch office access switches with options for fixed 100FX and 1000BASE-T connectivity.	Basic Standalone: Small- to medium-sized network access switch providing basic connectivity.
	Yes	Yes	No	No
	Standard	Yes	No	No
	Standard	Yes	No	No
	Yes	Yes	No	No
	Yes	Yes	No	No
	IGMP Snooping/PIM	IGMP Snooping/PIM	IGMP Snooping	IGMP Snooping
	Yes	Yes	Yes	No
	Yes	Yes	Yes	No
	Yes	Yes	Yes	No
	Yes	Yes	Yes	No

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 962
Nº Doc: 3702

16.828
L

Cisco Catalyst 3550 vs. 2950 Differentiation Matrix (continued)

	3550 Enhanced Multilayer Image	3550 Standard Multilayer Image	2950 Enhanced Image	2950 Standard Image
	Yes	Yes	No	No
	Port, router, and VLAN-based	Port, router, and VLAN-based	Port-based	None
	Q3CY02	Q3CY02	Q3CY02	No
	Yes	Yes	Yes	Yes
	Yes	Yes	No	No
	Yes, all 64 values	Yes, all 64 values	Yes, only 13 values	No
	Yes	Yes	No	No
	8 on 10/100; 128 on GE	8 on 10/100; 128 on GE	6 on 10/100; 60 on GE	None
	8 on 10/100; 8 on GE	8 on 10/100; 8 on GE	None	None
	Yes	Yes	No	No
	Yes	Yes	No	No
	8000	2000	255	255
	12000	8000	8000	8000
	1000 (128 spanning-tree instances)	1000 (128 spanning-tree instances)	250 (64 spanning-tree instances)	64 (one spanning-tree instance per VLAN)

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 963
3702
Doc:

16.827

Q: Which switch is the right switch?

A: It all depends on how the switch will be used and what kind of configuration is needed (remember to keep future growth in mind).

Location, application, configuration, and price are key considerations when selecting a switch. The diagram to the right, along with the deployment scenarios below, should help you decide.

For stack server aggregation or small network backbones:

- **Cisco Catalyst 3550-12G or 3550-12T** Stackable 10/100 and Gigabit Ethernet configurations, high-performance switching and routing, enterprise-class intelligent services, and clustering capabilities

For intelligent access layer connectivity:

- **Cisco Catalyst 3550-24/48** Stackable 10/100 switching, Gigabit Interface Converter (GBIC)-based gigabit connectivity, high-performance multilayer switching and IP routing, enterprise-class intelligent services, clustering capabilities, and upgradeable to full dynamic IP routing
- **Cisco Catalyst 2950G-12/24/48** Stackable 10/100 switching, GBIC-based gigabit connectivity, advanced intelligent services, and clustering capabilities

For basic access layer connectivity:

- **Cisco Catalyst 2950-12/24** Wire-speed standalone 10/100 switching, basic Cisco IOS functionality, and clustering capabilities

For IP telephony and wireless networking:

- **Cisco Catalyst 3524-PWR XL** Stackable 10/100 switching, GBIC-based gigabit connectivity, intelligent services, integrated inline power, clustering capabilities

For fixed fiber access layer connectivity:

- **Cisco Catalyst 3550-24-FX-SMI** Stackable 100BASE-FX switching with 1000BASE-X uplinks, high-performance switching and routing, enterprise-class intelligent services, and clustering capabilities; upgradeable to full dynamic IP routing

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 964
Nº 3702
Doc:

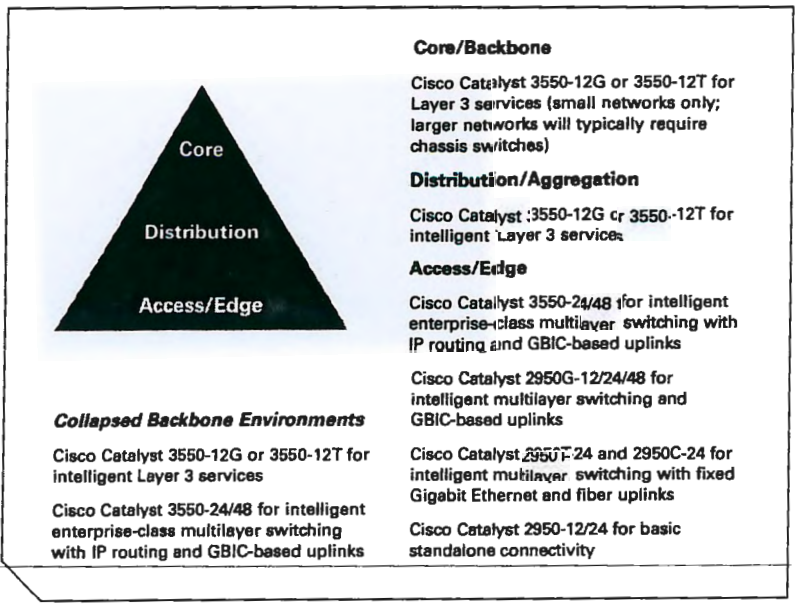
16 826

- **Cisco Catalyst 2950C-24** Wire-speed standalone 10/100 switching, 100BASE-FX uplinks, advanced intelligent services, and clustering capabilities

For fixed Gigabit Ethernet access layer connectivity:

- **Cisco Catalyst 2950T-24** Wire-speed standalone 10/100 switching, 10/100/1000BASE-T uplinks, advanced intelligent services, and clustering capabilities; ideal for deploying Gigabit Ethernet over a copper (Category 5) infrastructure

For deployments in telco/data communications network (DCN) environments, Cisco Catalyst 3550-24-DC and Cisco Catalyst 2950G-24-DC switches provide stackable 10/100 switching, GBIC-based gigabit connectivity, advanced intelligent services, clustering capabilities, and DC power.



RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 965
Doc: 3702

16.825
2

Cisco Catalyst 3550 Series Intelligent Ethernet Switches

Catalyst 3550-24*
24 10/100 ports
2 GBIC ports

Medium Port Density

Catalyst 3550-48
48 10/100 ports
2 GBIC ports

High Port Density

Catalyst 3550-12T
10 10/100/1000 ports
2 GBIC ports

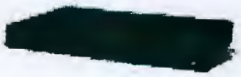
Catalyst 3550-12G
10 GBIC ports
2 10/100/1000 ports

Gigabit Ethernet Aggregation

Upgradeable to Enhanced Multilayer Software Image (EMI) feature set

*Two additional configurations provide integrated DC power and fixed fiber connectivity.

Cisco Catalyst 3524-PWR XL



Catalyst 3524-PWR XL
24 10/100 ports
2 GBIC ports
Inline power

Medium Port Density

Intelligent Services

Redundant Power System 300

Cisco Redundant Power System 300

The Cisco Redundant Power System 300 (RPS 300) makes it easy and affordable to boost the availability of converged data, voice, and video networks.

The Cisco RPS 300 provides internal power supply redundancy with immediate failover for up to six Cisco networking devices, including Catalyst 2950, 3550, and 3524-PWR XL switches. As a result, the devices will continue to operate without interruption in the rare event of an internal power supply failure.

When combined with the Catalyst 3524-PWR XL switch, which features integrated inline power and an uninterruptible power supply (UPS) system, the Cisco RPS 300 provides backup for the primary internal power supply as well as battery backup. This ensures the switches—along with any IP telephones or wireless access points receiving inline power over the network—will remain available if the switch's internal power supply fails or during a power outage.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 966
Nº Doc 3702

16.324
2

Cisco Catalyst 2950 Series Intelligent Ethernet Switches

Catalyst 2950G-12-EI
12 10/100 ports
2 GBIC ports

Low Port Density

Catalyst 2950G-24-EI
24 10/100 ports
2 GBIC ports

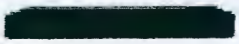
Catalyst 2950G-24-EI-DC
24 10/100 ports
2 GBIC ports
DC powered

Medium Port Density

Catalyst 2950G-48-EI
48 10/100 ports
2 GBIC ports

High Port Density

Cisco Catalyst 2950 Series Intelligent Ethernet Switches (continued)



Catalyst 2950T-24
24 10/100 ports
Two fixed 1000BASE-T ports

Catalyst 2950C-24
24 10/100 ports
Two fixed 100BASE-FX ports

Medium Port Density

Cisco Catalyst 2950 Series Switches

Catalyst 2950-12
12 10/100 ports

Low Port Density

Catalyst 2950-24
24 10/100 ports

Medium Port Density

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 967
Doc. 3702

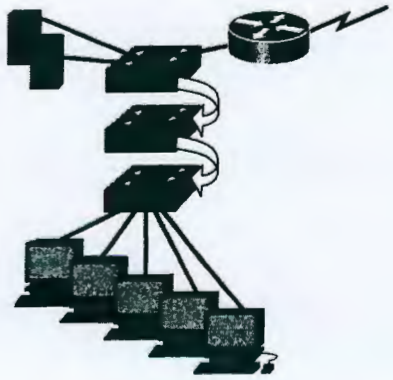
16.823
2

Sample designs of small, medium, and large networks

Network designs must take into account many factors, including the organization's overall requirements, as well as the needs of individual workgroups. These diagrams are intended to serve only as general examples of how switches might be deployed in networks of various sizes.

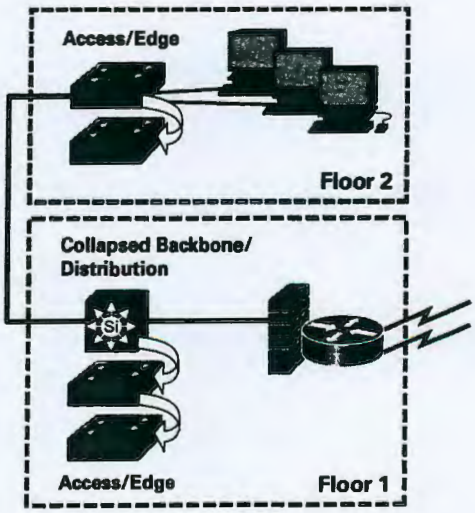
1) Growing Small Business or Small Branch Office

- Connectivity with basic or intelligent services
- No need for aggregation without a core switch, stack links directly to router



2) Medium-Sized Network/Branch Office

- Highly available collapsed backbone with IP routing and intelligent services
- QoS and security based on Layer 2–4 information at access/edge



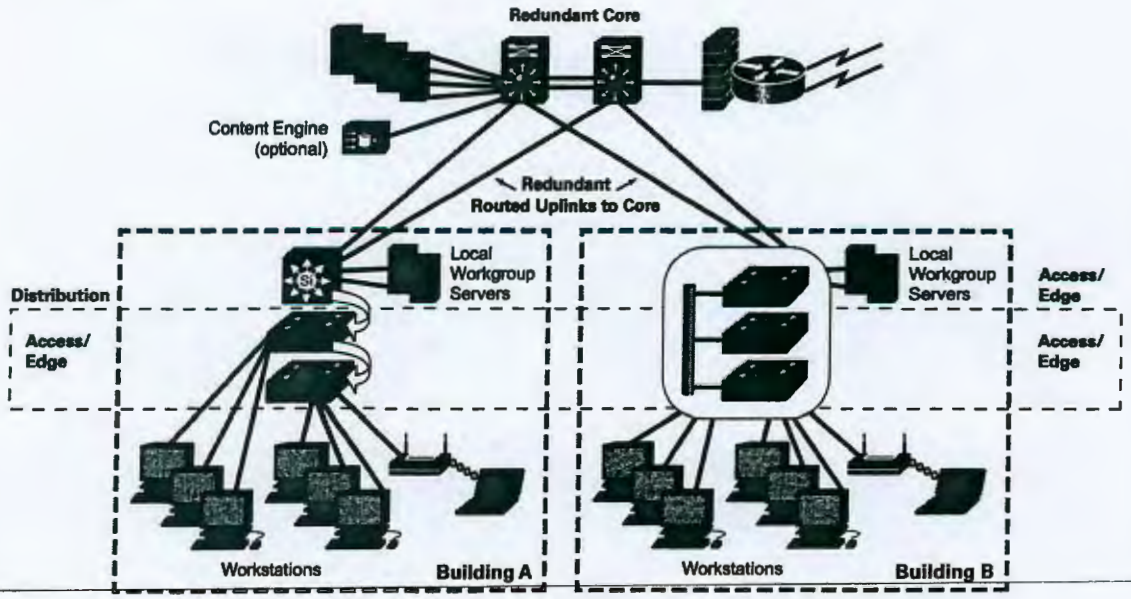
RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 968
Nº Doc: 3702

16.822
2

Sample designs of small, medium, and large networks (continued)

3) Larger Campus Network

- Highly available redundant core
- Building A: Distribution layer with intelligent services and routed uplinks to the core; highly granular rate limiting and security filtering at the access/edge
- Building B: Deliver same function as Building A via multilayer switches with IP routing and advanced intelligent services



RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 969
Doc 3702

16.821

Transition Matrix

Legacy Product	Legacy Product SKU	New Product	New Product SKU
Cisco Catalyst 3512 XL-EN			
12-port 10/100 switch with two fixed GBIC-based 1000BASE-X uplinks	(WS-C3512-XL-EN)	Cisco Catalyst 2950G-12-EI	WS-C2950G-12-EI
[illegible]	[illegible]	[illegible]	[illegible]
Cisco Catalyst 3548 XL-EN			
48-port 10/100 switch with two fixed GBIC-based 1000BASE-X uplinks	(WS-C3548-XL-EN)	Cisco Catalyst 3550-48-EMI Cisco Catalyst 3550-48-SMI Cisco Catalyst 2950G-48-EI	WS-C3550-48-EMI WS-C3550-48-SMI WS-C2950G-48-EI

The new Cisco Catalyst 3550 and 2950 Series Intelligent Ethernet switches are designed to replace the successful Cisco Catalyst 3512 XL, 3524 XL, and 3548 XL switches.

Cisco recommends migrating from the Catalyst 3512 XL switch to the Catalyst 2950G-12 switches, which provides equivalent port density at a lower price. Catalyst 3524 XL and Catalyst 3548 XL customers are advised to migrate to Catalyst 3550-24 and 3550-48 switches, which offer premium functionality at the same price (when selecting the Standard Multilayer Software Image [SMI] versions).

The Cisco Catalyst 3524-PWR XL remains the leading choice for inline power for converged networks, and the Cisco Catalyst 3508G XL remains the ideal solution for providing Layer 2 aggregation at a cost-effective price. Cisco will continue to sell and support these products.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 970
3702
Doc:

16 820
L

Transition Matrix

Legacy Product	Legacy Product SKU	New Product	New Product SKU
Catalyst 1912-A/Standard Edition	WS-C1912-A	Catalyst 2950-12	WS-C2950-12
Catalyst 1924-A/Standard Edition	WS-C1924-A	Catalyst 2950T-24 Catalyst 2950-24	WS-C2950T-24 WS-C2950-24
Catalyst 1924F-A/Standard Edition	WS-C1924F-A	Catalyst 2950C-24	WS-C2950C-24
Catalyst 1912C-EN/Enterprise Edition	WS-C1912C-EN	Catalyst 2950C-24	WS-C2950C-24
Catalyst 1924C-EN/Enterprise Edition	WS-C1924C-EN	Catalyst 2950C-24	WS-C2950C-24
Catalyst 1924-EN-DC/Enterprise Edition	WS-C1924-EN-DC	Catalyst 2950G-24-EI-DC	WS-C2950G-24-EI-DC
Catalyst 2828-EN/Enterprise Edition	WS-C2828-EN	Catalyst 2950-24 Catalyst 2950T-24 Catalyst 2950C-24	WS-C2950-24 WS-C2950T-24 WS-C2950C-24

The discontinuation of Cisco Catalyst 1900 and 2820 Series switches provides the opportunity to increase network performance and functionality by transitioning to the Catalyst 2950 Series switches. These new switches enable basic or intelligent connectivity with options for Gigabit Ethernet uplinks. In addition, customers can deploy Layer 2–4 services for higher availability, enhanced security, and advanced QoS.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 971
Nº 3702
Doc:

16.819
L

For more information on products in this guide

www.cisco.com/go/catalyst2950
www.cisco.com/go/catalyst3550

Want to learn more?

You'll find a wealth of information about Cisco Catalyst switches online, including:

- A solutions guide that explains how Cisco Catalyst 2950, 3550, 4000, and 6500 Series switches ease network migration and expansion
- Two additional solutions guides addressing the unique needs of customers in government and education
- A new multimedia preview of Cisco Cluster Management Suite Software, demonstrating how this free tool saves network administrators time and money while easing the deployment of intelligent services
- Sales tools highlighting each member of the Cisco Catalyst family
- A quick reference guide with ordering information for Cisco Catalyst products and accessories

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 972
3702
Doc:

16.818
L

An agent that precipitates
or accelerates a reaction,
development, or change.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 973
3702
Doc:

16.817
2

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www.cisco.com
Tel: +31 (0)20 357 1000
Fax: +31 (0)20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 305 718-2600
Fax: 305 718-2699

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 317 7777
Fax: +65 317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the Cisco.com Web site at www.cisco.com/go/offices.

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Czech Republic
Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel • Italy
Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal
Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Copyright © 2002, Cisco Systems, Inc. All rights reserved. Aironet, Catalyst, Cisco, Cisco IOS, Cisco Systems, the Cisco Systems Verified logo, EtherChannel, and GigaStack are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0206R)

Printed in the USA

job lyon 3625/07.02
Lit # 956460

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 974
Nº 3702
Doc:

16.816
L

Data Sheet

Cisco Systems **Redundant Power System** 675

The Cisco Redundant Power System 675 (RPS 675) is designed to increase availability in a converged data, voice, and video network. The system delivers superior internal power supply redundancy and resiliency at an affordable price.

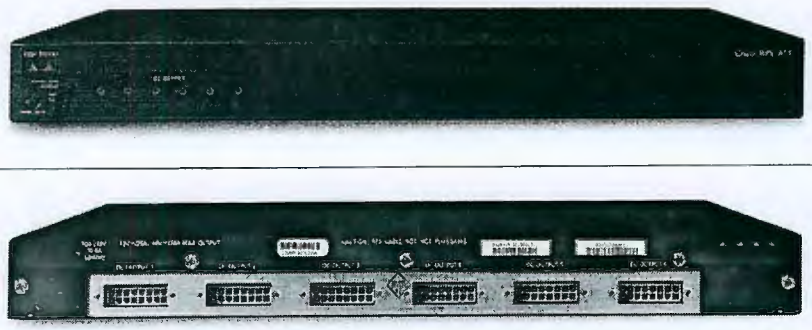
The Cisco RPS 675 supports internal power supply redundancy for up to six Cisco networking devices and features an innovative power architecture that provides customers with an immediate failover capability. The Cisco RPS 675 incorporates a quick failover feature, ensuring customers that the connected device will not reboot in the event of an internal power supply failure. For example, if an internal power supply fails on one of the six connected devices, the Cisco RPS 675 automatically senses the failure and delivers uninterrupted power to that device.

When a failure is detected, the Cisco RPS 675 sends status information showing that the other connected devices will not be supported until the failed device is restored or replaced. This status information can be monitored through CiscoWorks 2000 and the Cisco Cluster Management Suite (CMS) Software that provides Web-based network management. To achieve one-to-one redundancy, each device must be connected to a separate Cisco RPS 675.

The Cisco RPS 675 can be combined with the Cisco Catalyst® 3550-24 PWR desktop switch, featuring inline power and an uninterruptible power supply (UPS) system, to establish all of the elements of the Cisco Centralized Power Provisioning System. This combination provides a resilient, highly available converged network, offering 1) internal redundant power to the switch; 2) power to the IP phone via the switch's inline power feature (rather than wall power); and 3) back-up in the event of a power outage.

The Cisco RPS 675 will support future Cisco switches. Please refer to the 600-Watt Redundant AC Power System data sheet and the Cisco Systems Redundant Power Supply 300 (RPS 300) Data Sheet for non-RPS 675 supported devices.

ıre 1 The Cisco RPS 675 supports redundant power for up to six Cisco networking devices in a convenient single rack-unit (1RU) form factor



Cisco Systems, Inc.
All contents are Copyright © 2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

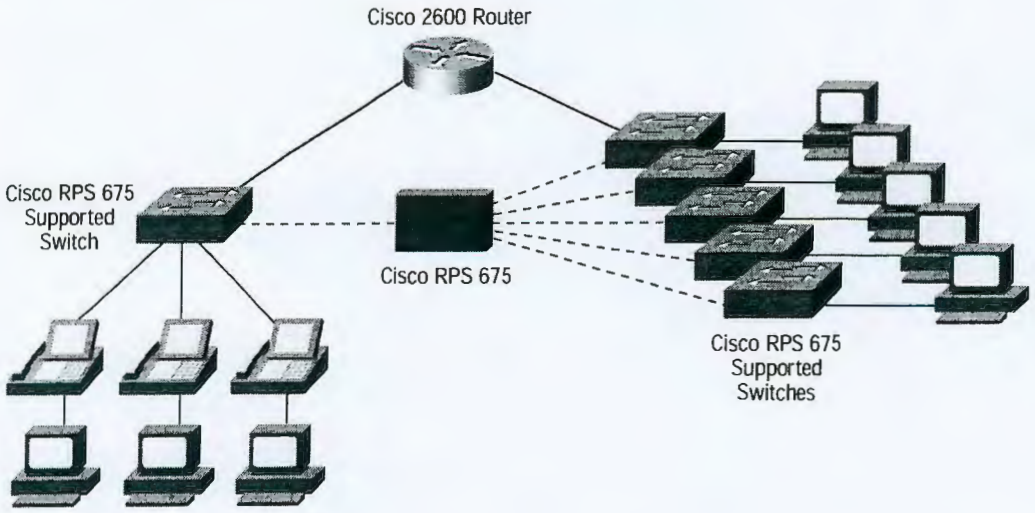
RQS nº 03/2005 - CN -
CPMI - CORREIOS
975
Fls Nº
3702
Doc:

16.815
L

Product Applications

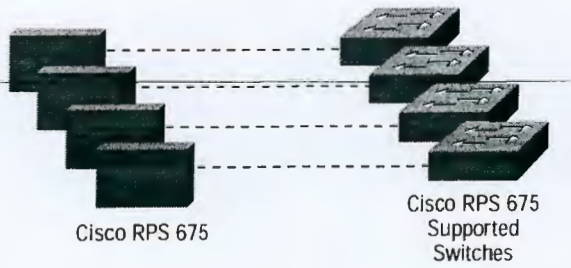
The Cisco RPS 675 can be deployed in a variety of situations to ensure network resiliency for mission-critical customer applications. Figure 2 illustrates the need for a more resilient network that provides maximum availability: a converged voice and data network includes switches connected to IP phones and PCs. In the rare event of a switch internal power supply failure, the Cisco RPS 675 ensures seamless voice/data network operation without interruption. In this scenario, multiple switches with inline power are supported by the Cisco RPS 675. The switches are connected to PCs and are used to power IP phones.

Figure 2 10/100 IP Phone and Desktop Computer Connections



The Cisco RPS 675 also provides maximum resiliency when implemented with one-to-one redundancy. With a one-to-one configuration, backup for an internal power supply failure of the associated switch is guaranteed. This application, displayed in Figure 3, a single Cisco RPS 675 is used to support a single desktop switch.

Figure 3 One-to-One Redundancy



Cisco Systems, Inc.
All contents are Copyright © 2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 976
3702
Doc:

16-814
2

Key Benefits and Features

High Availability/Increased Network Uptime

- Less than 60 s failover capability prevents switch reboot after an internal switch power failure
- Supports traditional Ethernet switches (12V output) and new inline powered Ethernet switches (-48V output) for voice-over-IP (VoIP) telephones
- The Cisco RPS 675, in combination with an uninterruptible power system (UPS), delivers maximum network uptime by providing backup for the primary internal power supply as well as battery backup to maintain availability during power outages
- Mean Time Between Failures (MTBF) in excess of 255,000 hours

Ease-of-Use and Ease-of-Deployment

- Single rack-unit (1RU) high form factor provides the most efficient wiring closet space utilization available
- Users can identify and monitor the following activity on the Cisco RPS 675, using the CiscoWorks2000 or Cisco CMS Software network management applications:
  - Switch connectivity
  - Power delivery status
- Hot insertion of external devices
- LEDs on front panel indicate:
  - System status (Active, Standby, Off)
  - Internal DC power status
  - DC output power status for each channel
  - Thermal status
  - Fan status

Cost-Effective Solution

- Innovative power architecture delivers a cost-effective unit price and allows the Cisco RPS 675 to support up to six switches, reducing the redundant power cost per switch
- One DC power cable included (CAB-RPS-1614=)

Technical Specifications

Supported Products

- Catalyst 3550 Series Switches
- Catalyst 2980G-A Switch
- Catalyst 2950 Series Switches
- Catalyst 2950 Series LRE Switches
- Catalyst 2900 LRE XL Switches

All contents are Copyright © 2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 977
3702
Doc:

16.813
2

Connectors and Cabling

RPS to external device connection: 1.2-meter cable with a 16-pin connector on the RPS end, and 14-pin connector on the switch end. The Cisco RPS 675 comes with one cable; others must be ordered separately. See ordering information below.

Indicators

- Status LEDs–standby/active, output power, temperature, fan
- DC Output LEDs–DC output status for each of the six channels

Dimensions and Weight

- 1.75 x 17.5 x 14.88 in. (4.5 x 44.5 x 37.8 cm)
- Single rack-unit (1RU) high
- 13 lb (5.9 kg)

Environmental Conditions and Power Requirements

- Operating temperature: 32 to 113 F (0 to 45 C)
- Storage temperature: -4 to 149 F (-20 to 65 C)
- Operating relative humidity: 10 to 85 percent non-condensing
- Operating altitude: up to 10,000 ft (3000 m)
- Storage altitude: up to 15,000 ft (4570 m)
- Power consumption: 675W maximum for both outputs; 375W maximum for -48VDC and 300W maximum for 12VDC
- AC input voltage/frequency: 85 to 264 VAC/50 to 60 Hz
- MTBF in excess of 255,000 hours

Electromagnetic Emissions Certifications

- FCC Part 15 Class A
- EN 55022 Class A
- VCCI Class A
- AS/NZS 3548 Class A
- CE Marking
- BSMI
- CCIB approval pending
- NOM approval pending

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 978
Doc: 3702

All contents are Copyright © 2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

IC 812
L

Safety Certifications

- UL 60950 3RD edition
- CAN/CSA C22.2 No. 60950-00
- EN 60950
- IEC 60950
- AS/NZS 3260, TS001
- CE Marking
- CCC

Warranty

Limited lifetime warranty

Ordering Information

- Model Number: PWR675-AC-RPS-N1=
- Cisco Redundant Power System 675 (RPS 675) with 1 connector cable
- The Cisco RPS 675 is sold with one cable. Other cables must be ordered separately.
- Cable: CAB-RPS-1614=
- 1.2 meter cable for Cisco RPS 675 to external device connection
- For More Information on Cisco Products, Contact:
- U.S. and Canada: 800 553-NETS (6387)
- Europe: 32 2 778 4242
- Australia: 612 9935 4107
- Other: 408 526-7209
- World Wide Web URL: http://www.cisco.com

CISCO SYSTEMS

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the

Cisco Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland
Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland
Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Catalyst, Cisco, Cisco IOS, Cisco Systems, and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0301R)

RQS nº 03/2005 - CN - CPMI - CORREIOS
03/03 BW8958
Fls Nº 979
Doc: 3702

ANEXO (14)

16 811

Data Sheet

Cisco Catalyst **2950** Series Intelligent Ethernet Switches for Metro Access (Enhanced Image)

Product Overview

The Cisco Catalyst® 2950 Series Intelligent Ethernet switches is an affordable line of fixed-configuration Fast Ethernet and Gigabit Ethernet switches that extend intelligence to the metro access edge, enabling service breadth, availability, security, and manageability. Key components of the Cisco Metro Ethernet Switching portfolio, these switches are ideal for service providers looking to deliver profitable Ethernet services to the residential and small-office, home-office (SOHO) market. Featuring advanced rate limiting, voice virtual LAN (VLAN) support, and multicast management, these switches enable a variety of residential metro services such as Internet access, voice over IP (VoIP), and broadcast video.

The Cisco Catalyst 2950 Series Intelligent Ethernet switches consists of the following devices—which are only available with the Enhanced Image (EI) software for the Cisco Catalyst 2950 Series:

- Cisco Catalyst 2950G-48 Switch—48 10/100 ports and 2 gigabit interface converter (GBIC)-based Gigabit Ethernet ports
- Cisco Catalyst 2950G-24 Switch—24 10/100 ports and 2 GBIC ports
- Cisco Catalyst 2950G-24-DC Switch—24 10/100 ports, 2 GBIC ports, and DC power
- Cisco Catalyst 2950G-12 Switch—12 10/100 ports and 2 GBIC ports
- Cisco Catalyst 2950T-24 Switch—24 10/100 ports and 2 fixed 10/100/1000BaseT uplink ports
- Cisco Catalyst 2950C-24 Switch—24 10/100 ports and 2 fixed 100BaseFX uplink ports
- Catalyst 2950ST-24-LRE—24 LRE and 2 Gigabit Ethernet ports (user can select either 10BaseT/100BaseTX/1000BaseT Ethernet Ports or Small Form Factor Pluggable (SFP) Transceivers)
- Catalyst 2950ST-8-LRE—8 LRE and 2 Gigabit Ethernet ports (user can select either 10BaseT/100BaseTX/1000BaseT Ethernet Ports or Small Form Factor Pluggable (SFP) Transceivers)

The two built-in Gigabit Ethernet ports on the Cisco Catalyst 2950G-12, 2950G-24, and 2950G-48 accommodate a range of GBIC transceivers, including the Cisco Course Wave Division Multiplexing (CWDM) GBIC Solution, Cisco GigaStack® GBIC, 1000BaseSX, 1000BaseLX/LH, 1000BaseZX and 1000BaseT GBICs. The dual GBIC-based Gigabit Ethernet implementation provides customers with tremendous deployment flexibility— allowing them increased availability with the redundant uplinks. High levels of resiliency can also be implemented by deploying dual redundant Gigabit Ethernet uplinks, UplinkFast and

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 980
Nº Doc: 3702

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

16.810

Per-VLAN Spanning Tree Plus (PVST+) for uplink load balancing. This Gigabit Ethernet flexibility makes the Cisco Catalyst 2950 Series switches an ideal metro access edge complement to the Cisco 7600 Series Internet Router and Cisco Catalyst 6500 Series of metro Ethernet switches.

Intelligence at the Metro Access Edge: Enabling Profitable Ethernet Services

Service providers that address the residential and SOHO market face the continual challenge of offering compelling value-added services.

Although alternative broadband technologies such as DSL can offer bandwidth at speeds ranging up to 1.5 Mbps, the monthly subscriber fees for such speeds can be out of reach for most users. As a result, compelling high-quality services such as high-speed Internet access, VoIP, or broadcast video are often not viable propositions over these technologies. However, in the metro, service providers are discovering that high-performance, Ethernet access over fiber-optic networks can easily provide cost-effective bandwidth of 10 to 100 Mbps. By taking advantage of the simplicity and cost benefits of Ethernet, revenue growth via voice, video, and data services becomes a reality. When considering the deployment of Ethernet services, service providers must consider the following issues:

- Building cost-effective, highly available, scalable metro Ethernet networks
- Providing profitable new services while reducing operational and capital costs
- Having the network flexibility to move up market to enterprise and small and medium- sized business services

These issues are especially relevant at the metro access edge. As service providers look to provide profitable Ethernet services such as high-speed Internet access, voice, and video, Cisco intelligent functionality such as advanced quality of service (QoS), granular rate limiting, and multicast management are essential in the provider's customer-located equipment. In addition, availability and security concerns at the access edge are addressed with intelligent features such as subsecond Spanning Tree Protocol (STP) convergence and 802.1x support. With Cisco Catalyst 2950 Series Intelligent Ethernet switches, Cisco delivers the ideal balance of affordability and intelligence, enabling profitable Ethernet service breadth, availability, security and manageability.

Most important, the Cisco Catalyst 2950 Series is a key component of the Cisco Metro Ethernet Switching portfolio. As such, service providers are assured that they can offer a range of residential and commercial services over the same network. For regional metro, metro aggregation, and metro access, Cisco Metro Ethernet Switching enables service providers to deliver profitable, comprehensive Ethernet services. With the effective integration of existing WAN services such as Frame Relay and ATM, Cisco Metro Ethernet Switching offers an unmatched breadth of service delivery mechanisms. Cisco also helps service providers minimize total cost of ownership for new services with its extensive automated operations support. Through technology leadership, financial stability, and a commitment to customer support, Cisco ensures service success from "start to scale."

Service Breadth Through Advanced Quality of Service, Rate Limiting, and Voice/ Multicast Features

To achieve profitability, service providers that serve the residential and SOHO markets must offer value-added services such as voice and video in addition to basic high-speed Internet connectivity to increase revenue per subscriber. But these services are compelling only when service quality matches that of competing voice and video offerings.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 981
Doc: 3702

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

16-809
2

The Cisco Catalyst 2950 Series offers superior and highly granular QoS to ensure that network traffic is classified and prioritized, and that congestion is avoided in the best possible manner. The Cisco Catalyst 2950 Series can classify, reclassify, police (determine if the packet is in or out of predetermined profiles and affect actions on the packet), and mark or drop the incoming packets before the packet is placed in the shared buffer. Packet classification allows the network elements to discriminate between various traffic flows and enforce policies based on Layer 2 and Layer 3 QoS fields.

To implement QoS, first, the Cisco Catalyst 2950 Series switches identify traffic flows, or packet groups, and classify or reclassify these groups using either the Differentiated Services Code Point (DSCP) field or the 802.1p class-of-service (CoS) field, or both. Classification and reclassification can be based on criteria as specific as the source/destination IP address, source/destination Media Access Control (MAC) address, or the Layer 4 Transmission Control Protocol/User Datagram Protocol (TCP/UDP) port. At the ingress, the Cisco Catalyst 2950 Series can also perform policing and marking of the packet.

After the packet goes through classification, policing, and marking, it is then assigned to the appropriate queue before exiting the switch. The Cisco Catalyst 2950 Series supports four egress (outgoing port) queues per port, which allows the service provider to be more discriminating and specific in assigning priorities for the various applications. At the egress, the switch performs Weighted Round Robin (WRR) or strict priority scheduling to determine the order in which the queues are processed. The WRR queuing algorithm ensures that the lower-priority packets are not entirely starved for bandwidth and are serviced without compromising the priority settings administered by the network manager. Strict priority scheduling ensures that the highest-priority packets are always serviced first, ahead of all other traffic.

In terms of rate limiting, the Cisco Catalyst 2950 Series is capable of allocating bandwidth based on several criteria, including MAC source address, MAC destination address, IP source address, IP destination address, and TCP/UDP port number. Bandwidth allocation is essential in network environments requiring service-level agreements (SLAs), or when it is necessary for the network manager to control the bandwidth given to certain subscribers. The Cisco Catalyst 2950 Series supports up to 6 policers per Fast Ethernet port and up to 60 policers on a Gigabit Ethernet port. Traffic policing can be done in 1-Mbps increments on Fast Ethernet ports and 8-Mbps increments on Gigabit Ethernet ports, giving the network manager very granular control of network bandwidth.

In addition, the Cisco Catalyst 2950 Series provides key voice and video service features with voice VLAN (auxiliary VLAN) for VoIP services and hardware-based Internet Group Management Protocol (IGMP) snooping, allowing the switch to "listen in" on the IGMP conversation between hosts and routers. When a switch hears an IGMP join request from a host for a given multicast group, the switch adds the host port number to the Group Destination Address (GDA) list for that group. And, when the switch hears an IGMP leave request, it removes the host port from the list. Together with the superior QoS and rate-limiting features mentioned previously, service providers can build a flexible network with the Cisco Catalyst 2950 Series to provide voice, video, and data services all in one network architecture.

Service Availability through Resiliency Enhancements and Network Redundancy

The Cisco Catalyst 2950 Series provides a rich set of resiliency enhancement features to ensure quick failover recovery and create a high-availability network. The IEEE 802.1w Rapid Spanning Tree standard allows the service provider to achieve subsecond spanning tree convergence times to maximize network stability and reliability. The

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
982
Fls Nº
3102
Doc:

16.808
L

IEEE 802.1s Multiple Spanning Tree standard can be deployed in conjunction with 802.1w to improve the scalability of the STP by grouping VLANs into spanning tree instances, as well as to provide backward compatibility to devices running the 802.1D STP.

In addition, service providers can enable Bridge Protocol Data Unit (BPDU) guard and Spanning Tree Root Guard (STRG) to enhance the reliability of their networks. BPDU guard allows the service provider to shut down STP PortFast-enabled interfaces to avoid receiving BPDUs from their customers' networks. STRG prevents customer devices outside of the service provider's network from becoming STP root nodes.

The Cisco Catalyst 2950 Series enables the service provider to construct a highly redundant network. PVST+ allows the service provider to implement Layer 2 load-sharing on redundant links, efficiently utilizing the extra capacity inherent in a redundant design. Service providers can also utilize Cisco EtherChannel® technology to aggregate up to 4 Gbps through Gigabit EtherChannel technology and up to 1.6 Gbps through Fast EtherChannel technology. The Cisco EtherChannel technology enhances fault tolerance and offers higher-speed aggregated bandwidth between switches and to routers.

In addition to resiliency and network redundancy advantages, the Cisco Catalyst 2950 Series enables metro network scalability at the access edge through its support of Cisco CWDM GBIC Solution. This solution allows service providers to scale their bandwidth without deploying additional fiber. The service provider can scale up to eight gigabits of bandwidth on a pair of single-mode fibers at distances up to 120 km. With the support for Cisco CWDM GBICs on the Cisco Catalyst 2950 Series, service providers can aggregate multiple Cisco Catalyst 2950 Series switches to easily upgrade network bandwidth with existing fiber infrastructure.

Metro network scalability is also enhanced by the Cisco Catalyst 2950 Series support of 4096 VLAN IDs and 256 active VLANs per switch.

Service Security Through Cisco Access Control Parameters and Enhanced Security Features

The Cisco Catalyst 2950 Series offers enhanced data security through the use of access control parameters (ACPs). By denying packets based on source and destination MAC addresses, IP addresses, or TCP/UDP ports, users can be restricted from sensitive portions of the network. Also, because all ACP lookups are done in hardware, forwarding performance is not compromised when implementing ACP-based security in the network.

Service providers can also implement higher levels of data security by supporting private VLAN edge. This feature provides security and isolation between ports on a switch, ensuring that traffic travels directly from its entry point to the aggregation device through a virtual path and cannot be directed to a different port. Local Proxy Address Resolution Protocol (ARP) works in conjunction with private VLAN edge to minimize broadcasts and maximize available bandwidth.

With the Cisco Catalyst 2950 Series, service providers can implement high levels of console security. Multilevel access security on the switch console and the Web-based management interface prevents unauthorized users from accessing or altering switch configuration. Terminal Access Controller Access Control System (TACACS+) authentication enables centralized access control of the switch and restricts unauthorized users from altering the configuration.

Service providers are also able to enhance their network security by adding 802.1x port-based authentication for authenticating individual customers, and port security with MAC address aging for limiting the concurrent MAC addresses allowed per port.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 983
3702
Doc:

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

16·807
L

Service Management Through Cisco IE 2100 Series and SNMP

The Cisco Catalyst 2950 Series provides outstanding service management capabilities via Cisco IE 2100 Series Intelligence Engine support and Simple Network Management Protocol (SNMP). Service providers will be able to integrate the Cisco Catalyst 2950 Series seamlessly into their operations support systems (OSSs) and enable improved flow-through provisioning.

The Cisco IE 2100 Series network device allows service providers to effectively manage a network of Cisco IOS® devices, including the Cisco Catalyst 2950 Series. It is a completely self-contained unit that includes a task-oriented Web graphical user interface (GUI), a programmable extensible markup language (XML) interface, configuration template management, and an embedded repository. Network operators can use the Web GUI to quickly turn existing Cisco IOS command-line interface (CLI) configuration files into reusable templates. The Cisco IE 2100 Series supports easy integration into existing customer OSS/business support system (BSS) and provisioning systems via its external repository support and the event-based Cisco IOS XML interface that effectively "workflow-enables" Cisco device deployment.

Service providers also can manage the Cisco Catalyst 2950 Series using SNMP version 2 and version 3, and the Telnet interface for comprehensive in-band management. A CLI-based management console provides detailed out-of-band management.

A comprehensive set of Management Information Bases (MIBs) is provided for the service provider to collect traffic information on the Cisco Catalyst 2950 Series for various billing methods.

Figure 1
Cisco Catalyst 2950 Series Intelligent Ethernet Switches

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
984
Fls Nº
3702
Doc:

16 806

Product Features and Benefits

Feature	Benefit
Service Breadth	
Advanced QoS	• This feature enables end-to-end QoS in the network by extending the QoS trust boundary to the edge of the network. • The switches support configuring QoS ACPs on all ports to ensure proper policing and marking on a per-packet basis using ACPs. Up to four ACPs per switch are supported in configuring either QoS ACPs or security filters.
	QoS Classification Support at Ingress • The switches support QoS classification of incoming packets for QoS flows based on Layer 2, Layer 3, and Layer 4 fields. • The following Layer 2 fields or a combination can be used for classifying incoming packets to define QoS flows: source MAC address, destination MAC address, 16-bit Ethertype. • The following Layer 3 and 4 fields or a combination can be used to classify incoming packets to define QoS flows: source IP address, destination IP address, TCP source or destination port number, UDP source or destination port number.
	QoS Metering/Policing at Ingress • Support for metering/policing of incoming packets restricts incoming traffic flows to a certain rate. • The switches support up to 6 policers per Fast Ethernet port, and 60 policers on a Gigabit Ethernet port. • The switches offer granularity of traffic flows at 1 Mbps on Fast Ethernet ports, and 8 Mbps on Gigabit Ethernet ports. QoS Marking at Ingress • The switches support marking/remarking packets based on state of policers/meters. • The switches support marking/remarking based on the following mappings: from DSCP to 802.1p, and 802.1p to DSCP. • The switches support 14 well-known and widely used DSCP values. • The switches support classifying or reclassifying packets based on default DSCP per port. • The switches support classifying or reclassifying frames based on default 802.1p value per port. • The switches support 802.1p override at ingress.

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 985
3702
Doc:

16805

Feature	Benefit
Service Breadth	
Advanced QoS (continued)	QoS Scheduling Support at Egress • Four queues per egress port are supported in hardware. • The WRR queuing algorithm ensures that low-priority queues are not starved. • Strict-priority queue configuration ensures that time-sensitive applications such as voice always follow an expedited path through the switch fabric.
Granular rate limiting	• The switch supports up to 6 policers per Fast Ethernet port and up to 60 policers on a Gigabit Ethernet port. • The switch offers granularity of traffic flows at 1 Mbps on Fast Ethernet ports and 8 Mbps on Gigabit Ethernet ports. • The switch offers the ability to limit data flows based on MAC source/destination address, IP source/destination address, TCP/UDP port numbers, or any combination of these fields. • The switch offers the ability to manage data flows asynchronously upstream and downstream from the end station or on the uplink.
Voice and video services	• The IGMP snooping feature allows the switch to "listen in" on the IGMP conversation between hosts and routers. When a switch hears an IGMP join request from a host for a given multicast group, the switch adds the host port number to the GDA list for that group. And, when the switch hears an IGMP leave request, it removes the host port from the list. • Multicast VLAN registration (MVR) continuously sends multicast streams in a multicast VLAN while isolating the streams from subscriber VLANs for bandwidth and security reasons. • IGMP filtering provides the control of the set of multicast groups to which a user on a switch port can belong. • Voice VLAN (auxiliary VLAN) support for VoIP application allows the creation
Resiliency and reliability	• IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) takes advantage of point-to-point wiring and provides rapid convergence of the spanning tree independent of spanning-tree timers. Reconfiguration of the spanning tree can occur in less than one second, a feature that is critical for networks carrying delay-sensitive traffic such as voice and video. • IEEE 802.1s Multiple Spanning Tree (MSTP), which uses RSTP for rapid convergence, enables VLANs to be grouped into a spanning-tree instance, with each instance having a spanning-tree topology independent of other spanning-tree instances. This architecture provides for multiple forwarding paths for data traffic, enables load balancing, and reduces the number of spanning-tree instances required to support a large number of VLANs. • Cisco UplinkFast/BackboneFast technologies ensure quick failover recovery, enhancing overall network stability and reliability.

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 986
Doc: 3702

16.804
2

Feature	Benefit
Service Breadth	
Resiliency and reliability (continued)	• Cisco CrossStack UplinkFast (CSUF) technology provides increased redundancy and network resiliency through fast spanning-tree convergence (less than two seconds) across a stack of switches using Cisco GigaStack GBICs in an independent stack backplane cascaded configuration. • Redundant stacking connections provide support for a redundant loopback connection for top and bottom switches in an independent stack backplane cascaded configuration. • BPDU guard shuts down STP PortFast-enabled interfaces when BPDUs are received to avoid accidental spanning tree topology changes. • STRG prevents edge devices not in the network administrator's control from becoming STP root nodes. • Command switch redundancy enabled in the Cisco Cluster Management Suite (CMS) Software allows customers to designate a backup command switch that takes over cluster management functions if the primary command switch fails. • Unidirectional link detection (UDLD) detects and disables unidirectional links on fiber-optic interfaces caused by incorrect fiber-optic wiring or port faults. Aggressive UDLD allows precautionary disabling of port on bidirectional links. • Per-port broadcast, multicast, and unicast storm control prevents faulty end stations from degrading overall systems performance. • Support for Cisco's optional RPS 300 Redundant Power System provides superior internal power source redundancy for up to six Cisco networking devices, resulting in improved fault tolerance and network uptime.
Redundancy	• Bandwidth aggregation up to 4 Gbps through Cisco Gigabit EtherChannel technology and up to 1.6 Gbps through Cisco Fast EtherChannel technology enhances fault tolerance and offers higher-speed aggregated bandwidth between switches, to routers and individual servers. • IEEE 802.1D STP support for redundant backbone connections and loop-free networks simplifies network configuration and improves fault tolerance. • PVST+ allows for Layer 2 load sharing on redundant links to efficiently utilize the extra capacity inherent in a redundant design. • VLAN Trunking Protocol (VTP) pruning limits bandwidth consumption on VTP trunks by flooding broadcast traffic only on trunk links required to reach the destination devices.
Scalability	• CWDM GBIC solution support allows for the scaling of bandwidth without deploying additional fiber. It provides scalability of up to eight Gigabits of bandwidth on a pair of single-mode fibers to reach distances up to 100–120 km. • Support for up to 4096 VLAN Ids with 250 active VLANs per switch, and up to 64 spanning tree instances per switch.

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 987
3702
Doc:

16.803
2

Feature	Benefit
Service Security	
Network-wide security features	• Filtering of incoming traffic flows based on Layer 2, Layer 3, or Layer 4 ACPs prevents unauthorized data flows. Up to four ACPs are supported in configuring either QoS or security filters. – The following Layer 2 ACPs or a combination can be used for security classification of incoming packets: source MAC address, destination MAC address, and 16-bit Ethertype. – The following Layer 3 and Layer 4 fields or a combination can be used for security classification of incoming packets: source IP address, destination IP address, TCP source or destination port number, UDP source, or destination port number. • Private VLAN edge provides security and isolation between ports on a switch, ensuring that voice traffic travels directly from its entry point to the aggregation device through a virtual path and cannot be directed to a different port. • IEEE 802.1x for dynamic port-based security. • Support for "secure ports" prevents unauthorized stations from accessing the switch by restricting the number of concurrent MAC addresses allowed to access the port. Up to 132 addresses can be configured per port. • STRG prevents edge devices not in the network administrator's control from becoming STP root nodes. • The STP PortFast/ BPDU guard feature disables access ports with STP PortFast enabled upon reception of a BPDU, and increases network reliability, manageability, and security. • Multilevel security on console access prevents unauthorized users from altering the switch configuration. • TACACS+ and Remote Access Dial-In User Service (RADIUS) authentication enables centralized control of the switch and restricts unauthorized users from altering the configuration.
Service Management	
Superior manageability	• Cisco IE 2100 support for flow- through provisioning and integration with OSS applications via programmatical interfaces. • SNMP v1, v2c, v3, and Telnet interface support delivers comprehensive in-band management, and a CLI-based management console provides detailed out-of-band management. • Manageable through CiscoWorks network management software on a per-port and per-switch basis providing a common management interface for Cisco routers, switches, and hubs. • Comprehensive MIBs enable the service provider to collect traffic information on the Cisco Catalyst 2950 Series for various billing methods.

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
988
Fls Nº
3702
Doc:

Feature	Benefit
Service Management	
Superior manageability (continued)	• An embedded Remote Monitoring (RMON) software agent supports four RMON groups (history, statistics, alarms, and events) for enhanced traffic management, monitoring, and analysis. • The switch supports all nine RMON groups through the use of a Cisco SwitchProbe® Analyzer (Switched Port Analyzer [SPAN]) port, permitting traffic monitoring of a single port, a group of ports, or the entire switch from a single network analyzer or RMON probe. • RSPAN (Remote SPAN) allows network administrators to remotely monitor ports in a Layer 2 switch network from any other switch in the same network. • The Domain Name System (DNS) provides IP address resolution with user-defined device names. • Trivial File Transfer Protocol (TFTP) reduces the cost of administering software upgrades by downloading from a centralized location. • Network Timing Protocol (NTP) provides an accurate and consistent timestamp to all switches within the intranet. • Multifunction LEDs per port for port status, half-duplex/full-duplex, 10BaseT/100BaseTX/1000BaseT indication, as well as switch-level status LEDs for system, redundant power supply, and bandwidth utilization provide a comprehensive and convenient visual management system.
Ease of use and ease of deployment	• Autoconfiguration eases deployment of switches in the network by automatically configuring multiple switches across a network via a boot server. • Autosensing on each non-GBIC port detects the speed of the attached device and automatically configures the port for 10-, 100-, or 1000-Mbps operation, easing the deployment of the switch in mixed 10, 100, and 1000BaseT environments. • Autonegotiating on all ports automatically selects half- or full-duplex transmission mode to optimize bandwidth. • Cisco Discovery Protocol Versions 1 and 2 enable a CiscoWorks network management station to automatically discover the switch in a network topology. • Cisco VTP supports dynamic VLANs and dynamic trunk configuration across all switches. • Support for dynamic VLAN assignment through implementation of VLAN Membership Policy Server (VMPS) client functionality provides flexibility in assigning ports to VLANs. • Dynamic Trunking Protocol (DTP) enables dynamic trunk configuration across all ports in the switch. • Port Aggregation Protocol (PAgP) automates the creation of Cisco Fast EtherChannel or Gigabit EtherChannel groups, enabling linking to another switch, router, or server. • IEEE 802.3z-compliant 1000BaseSX, 1000BaseLX/LH, 1000BaseZX, and 1000BaseT physical interface support through a field-replaceable GBIC module provides customers unprecedented flexibility in switch deployment.

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 989
3702
Doc:

16.801

Feature	Benefit
Service Management	
Ease of use and ease of deployment (continued)	• The default configuration stored in Flash memory ensures that the switch can be quickly connected to the network and can pass traffic with minimal user intervention. • The switches support nonstandard Ethernet frame sizes (mini-giants) up to 1542 bytes (configurations with GBIC ports only).

Product Specifications

(See separate Cisco Catalyst 2950 LRE data sheet for Catalyst 2950ST-24-LRE and Catalyst 2950ST-8-LRE product specifications)

Feature	Description
Performance	• 13.6-Gbps switching fabric • 6.8-Gbps maximum forwarding bandwidth • Forwarding rates based on 64-byte packets • Cisco Catalyst 2950G-48: 10.1-Mpps wire-speed forwarding rate • Cisco Catalyst 2950G-24 and 2950G-24-DC: 6.6-Mpps wire-speed forwarding rate • Cisco Catalyst 2950G-12: 4.8-Mpps wire-speed forwarding rate • Cisco Catalyst 2950T-24: 6.6-Mpps wire-speed forwarding rate • Cisco Catalyst 2950C-24: 3.9-Mpps wire-speed forwarding rate • 32-MB maximum packet buffer shared by all ports • 16-MB DRAM and 8-MB Flash memory • Configurable up to 8000 MAC addresses • Configurable maximum transmission unit (MTU) of up to 1530 bytes (Cisco Catalyst 2950G
Management	• BRIDGE-MIB • CISCO-CDP-MIB • CISCO-CLUSTER-MIB • CISCO-CONFIG-MAN-MIB • CISCO-FLASH-MIB • CISCO-IMAGE-MIB • CISCO-MAC-NOTIFICATION-MIB • CISCO-MEMORY-POOL-MIB • CISCO-PAGP-MIB • CISCO-PING-MIB • CISCO-PROCESS-MIB • CISCO-PRODUCTS-MIB • CISCO-RTTMON-MIB • CISCO-STACKMAKER-MIB • CISCO-STP-EXTENSIONS-MIB

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 990
3702
Doc:

16.800
L

Feature	Description
Management (continued)	• CISCO-SYSLOG-MIB • CISCO-TCP-MIB • CISCO-VLAN-MEMBERSHIP-MIB • CISCO-VTP-MIB • ENTITY-MIB • IANAifType-MIB • IF-MIB (RFC 1573) • OLD-CISCO-CHASSIS-MIB • OLD-CISCO-CPU-MIB • OLD-CISCO-INTERFACES-MIB • OLD-CISCO-IP-MIB • OLD-CISCO-MEMORY-MIB • OLD-CISCO-SYSTEM-MIB • OLD-CISCO-TCP-MIB • OLD-CISCO-TS-MIB • CISCO-PAGP-MIB • CISCO-UDLD-MIB • RFC1213-MIB (MIB-II) • RFC1398-MIB (ETHERNET-MIB) • RMON-MIB (RFC 1757) • RS-232-MIB • SNMPv2-MIB • SNMPv2-SMI • SNMPv2-TC • TCP-MIB • UDP-MIB
Standards	• IEEE 802.1x support • IEEE 802.1w • IEEE 802.1s • IEEE 802.3x full duplex on 10BaseT, 100BaseTX, and 1000BaseT ports • IEEE 802.1D STP • IEEE 802.1p class-of-service (CoS) prioritization • IEEE 802.1Q VLAN • IEEE 802.3 10BaseT specification • IEEE 802.3u 100BaseTX specification • IEEE 802.3ab 1000BaseT specification • IEEE 802.3z 1000BaseX specification

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN - CPMI - CORREIOS
991
Fls Nº
3702
Doc:

16.799

Feature	Description	
Standards (continued)	• 1000BaseX (GBIC) • 1000BaseSX • 1000BaseLX/LH • 1000BaseZX • 1000Base-CWDM GBIC 1470 nm • 1000Base-CWDM GBIC 1490 nm • 1000Base-CWDM GBIC 1510 nm • 1000Base-CWDM GBIC 1530 nm • 1000Base-CWDM GBIC 1550 nm • 1000Base-CWDM GBIC 1570 nm • 1000BaseE-CWDM GBIC 1590 nm • 1000Base-CWDM GBIC 1610 nm • RMON I and II standards • SNMPv1, SNMPv2c, and SNMPv3	
Year 2000 (Y2K) compliance	• Y2K compliant	
Connectors and cabling	• 10BaseT ports: RJ-45 connectors; two-pair Category 3, 4, or 5 unshielded twisted-pair (UTP) cabling • 100BaseTX ports: RJ-45 connectors; two-pair Category 5 UTP cabling • 1000BaseT ports: RJ-45 connectors; two-pair Category 5 UTP cabling • 100BaseFX ports: MT-RJ connectors, 50/125 or 62.5/125 micron multimode fiber-optic cabling • 1000BaseSX, -LX/LH, -ZX GBIC-based ports: SC fiber connectors, single-mode or multimode fiber • Cisco GigaStack GBIC ports: copper-based Cisco GigaStack cabling • Management console port: 8-pin RJ-45 connector, RJ-45-to-RJ-45 rollover cable with RJ-45-to-DB9 adapter for PC connections; for terminal connections, use RJ-45-to-DB25 female data-terminal-equipment (DTE) adapter (can be ordered separately from Cisco, part number ACS-DSBUASYN=)	
MT-RJ patch cables for Cisco Catalyst 2950C-24 Switch	**Type of Cable**	**Cisco Part Number**
	1-meter, MT-RJ-to-SC multimode cable	CAB-MTRJ-SC-MM-1M
	3-meter, MT-RJ-to-SC multimode cable	CAB-MTRJ-SC-MM-3M
	5-meter, MT-RJ-to-SC multimode cable	CAB-MTRJ-SC-MM-5M
	1-meter, MT-RJ-to-ST multimode cable	CAB-MTRJ-ST-MM-1M
	3-meter, MT-RJ-to-ST multimode cable	CAB-MTRJ-ST-MM-3M
	5-meter, MT-RJ-to-ST multimode cable	CAB-MTRJ-ST-MM-5M

Cisco Systems, Inc.
All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 992
3702
Doc:

16.798

Feature	Description
Power connectors	Customers can provide power to a switch by using either the internal power supply or the Cisco RPS 300. The connectors are located at the back of the switch. **Internal Power Supply Connector** • The internal power supply is an auto-ranging unit. • The internal power supply supports input voltages between 100 and 240 VAC. • Use the supplied AC power cord to connect the AC power connector to an AC power outlet. **Cisco RPS Connector** • The connector offers connection for an optional Cisco RPS 300 that uses AC input and supplies DC output to the switch. • The connector offers a 300-watt redundant power system that can support six external network devices and provides power to one failed device at a time. • The connector automatically senses when the internal power supply of a connected device fails and provides power to the failed device, preventing loss of network traffic. • When the internal power supply has been brought up or replaced, the Cisco RPS 300 automatically stops powering the device. • Attach only the Cisco RPS 300 (model PWR300-AC-RPS-N1) to the redundant power supply receptacle.
Indicators	• Per-port status LEDs: link integrity, disabled, activity, speed, and full-duplex indications • System status LEDs: system, RPS, and bandwidth utilization indications
Dimensions and weight (H x W x D)	• 1.72 x 17.5 x 9.52 in. (4.36 x 44.5 x 24.18 cm) (Cisco Catalyst 2950T-24, 2950C-24, 2950G-12, 2950G-24, and 2950G-24-DC) • 1.72 x 17.5 x 13 in. (4.36 x 44.5 x 33.02 cm) (Cisco Catalyst 2950G-48) • 1.0 rack-unit high • 6.5 lb. (3.0 kg) (Cisco Catalyst 2950T-24, 2950C-24, 2950G-12, 2950G-24, and 2950G-24-DC) • 10 lb. (4.5 kg) (Cisco Catalyst 2950G-48)
Environmental ranges	• Operating temperature: 32 to 113 F (0 to 45 C) • Storage temperature: –13 to 158 F (–25 to 70 C) • Operating relative humidity: 10 to 85% (noncondensing) • Operating altitude: Up to 10,000 ft. (3000m) • Storage altitude: Up to 15,000 ft. (4500m) • Not intended for use on top of desktops or in open office environments
Power requirements	• Power consumption: 30W maximum, 102 BTUs per hour (Cisco Catalyst 2950T-24, 2950C-24, 2950G-12, 2950G-24, and 2950G-24-DC) • Power consumption: 45W maximum, 154 BTUs per hour (Cisco Catalyst 2950G-48) • AC input voltage/frequency: 100 to 127/200 to 240 VAC (autoranging), 50 to 60 Hz • DC input voltages – RPS input: +12V @ 4.5 A – DC input for 2950G-24-DC: –36 to –72 VDC @ 1A

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 993
Nº Doc. 3702

16.797
2

Feature	Description
Mean time between failure (MTBF) – Predicted	• 482,776 hours (Cisco Catalyst 2950G-12) • 468,884 hours (Cisco Catalyst 2950G-24) • 479,086 hours (Cisco Catalyst 2950G-24-DC) • 159,026 hours (Cisco Catalyst 2950G-48) • 297,144 hours (Cisco Catalyst 2950T-24) • 268,292 hours (Cisco Catalyst 2950C-24)
Fiber-port specifications for Cisco Catalyst 2950C-24 Switch	Fiber-port power levels: • Optical transmitter wavelength: 1300 nanometers • Optical receiver sensibility: –14 dBm2 • Optical transmitter power: –19 to –14 dBm • Transmit: –19 to –14 dBm
Regulatory Agency Approvals	
Safety certifications	• UL 1950/CSA 22.2 No. 950 • IEC 950-EN 60950 • AS/NZS 3260, TS001 • CE Marking
Electromagnetic emissions certifications	• FCC Part 15 Class A • EN 55022: 1998 Class A (CISPR22 Class A) • EN 55024: 1998 (CISPR24) • VCCI Class A • AS/NZS 3548 Class A • CE Marking • CNS 13438 • BSMI Class A • MIC
NEBS	• Bellcore • GR-1089-CORE • GR-63-CORE • SR-3580 Level 3
Warranty	• Limited lifetime warranty

Cisco Systems, Inc.
All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 994
Doc: 3702

16.796
L

Service and Support

The services and support programs described in the table below are available as part of the Cisco Desktop Switching Service and Support solution, and are available directly from Cisco and through resellers

Service and Support	Features	Benefits
Cisco Advanced Services		
Cisco Total Implementation Solutions (TIS)—available direct from Cisco **Packaged Total Implementation Solutions (Packaged TIS)—available through resellers**	• Project management • Site survey, configuration deployment • Installation, text, and cutover • Training • Major moves, adds, changes • Design review and product staging	• Supplements existing staff • Ensures functionality meets needs • Mitigates risk
Technical Support Services		
Cisco SMARTnet™ and SMARTnet Onsite Support (OS)—available direct from Cisco	• 24x7 access to software updates • Web access to technical repositories • Telephone support through the Cisco Technical Assistance Center (TAC)	• Enables proactive or expedited issue resolution • Lowers cost of ownership by utilizing Cisco expertise and knowledge
Packaged SMARTnet—available through resellers	• Advance replacement of hardware parts	• Minimizes network downtime

Ordering Information

Model numbers	Configuration
WS-C2950G-48-EI	• 48 10/100 ports + 2 1000BaseX ports • Enhanced Software Image (EI) installed
WS-C2950G-24-EI	• 24 10/100 ports + 2 1000BaseX ports • EI installed
WS-C2950G-24-EI-DC	• 24 10/100 ports + 2 1000BaseX ports, DC power • EI installed
WS-C2950G-12-EI	• 12 10/100 ports + 2 1000BaseX ports • EI installed
WS-C2950T-24	• 24 10/100 ports + 2 1000BaseT ports • EI installed
WS-C2950C-24	• 24 10/100 ports + 2 100BaseFX ports • EI installed
WS-C2950ST-24-LRE	• 24 LRE ports + 2 10BaseT/100BaseTX/1000BasetT Ethernet ports + 2 Small Form Factor Pluggable (SFP) Transceivers (two of four uplink ports active at one time • EI Installed
WS-C2950ST-8-LRE	• 8 LRE ports + 2 10BaseT/100BaseTX/1000BasetT Ethernet ports + 2 Small Form Factor Pluggable (SFP) Transceivers (two of four uplink ports active at one time • EI Installed

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 995
Doc 3702

16.795
2

For More Information on Cisco Products, Contact:

- United States and Canada: 800 553-NETS (6387)
- Europe: 32 2 778 4242
- Australia: 612 9935 4107
- Other: 408 526-7209
- World Wide Web URL: http://www.cisco.com

CISCO SYSTEMS

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 317 7777
Fax: +65 317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the **Cisco Web site at www.cisco.com/go/offices**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

All contents are Copyright © 1992–2002, Cisco Systems, Inc. All rights reserved. Catalyst, Cisco, Cisco IOS, Cisco Systems, and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0208R)

LW3663 0902

ECT nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 996
Doc: 3702

Cisco Products
Quick Reference Guide

February 2002

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

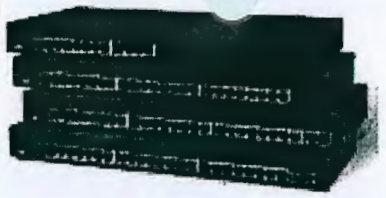
Page 3702
Ne 99 1 6
Rqsn° 03/2002 CN - CORRIOS

You can purchase additional copies of this guide on an as-needed basis or as an annual subscription. To purchase, go to the Cisco Subscription Program Web site http://www.cisco.com/go/subscription or call 800 768-7162 (US) or 925 327-4072 (International).

Customer Order Number DOC-785983

16 794

Cisco Catalyst 2950 Series Intelligent Ethernet Switches



Cisco extends its Catalyst 2950 Series with Intelligent Ethernet Switches with new fixed-configuration, stackable models that provide wire-speed Fast Ethernet and Gigabit Ethernet connectivity for mid-sized networks. The Catalyst 2950 Series is an affordable product line that brings intelligent services, such as advanced quality of service, rate-limiting, security filters, and multicast management, to the network edge-while maintaining the simplicity of traditional LAN switching. When a Catalyst 2950 Switch is combined with a Catalyst 3550 Series Switch, the solution enables IP routing from the edge to the core of the network.

When to Sell

Sell This Product	When a Customer Needs These Features
Catalyst 2950G-48-EI	• Ideal for desktop connectivity • High Port Density
Catalyst 2950G-24-EI	• Ideal for desktop connectivity • Medium Port Density
Catalyst 2950G-24-EI-DC	• Ideal for Telco/DCN environments • NEBS compliant • Medium Port Density
Catalyst 2950G-12-EI	• Ideal for desktop connectivity· • Low Port density
Catalyst 2950G Series	• Wire-speed performance • Advanced QoS, Security, High availability and STP enhancements • Cisco Cluster Management
Catalyst 2950T-24	• Wire speed, high performance switch for delivering 10Mbps or 100Mbps speed connectivity to desktop PCs, servers and other systems • Enhanced Quality of Service and multicast management capabilities • High speed uplink flexibility with 10/100/1000BaseT ports • Low price per port
Catalyst 2950C-24	• Wire speed, high performance switch for delivering 10Mbps or 100Mbps speed connectivity to desktop PCs, servers and other systems • Enhanced Quality of Service and multicast management capabilities • High speed uplink flexibility over extended distances with 100BASE-FX connections using MT-RJ connectors • Low price per port

Key Features

- Wire-speed performance in connecting end-stations to the LAN
- Ideal for mid-sized networks
- Catalyst 2950T-24 switch is a component of the Cisco Gigabit Ethernet over copper solution, offering 10/100/1000BaseT uplinks
- Powerful Gigabit uplink options—GBIC-based or 1000BaseT
- Superior control through advanced intelligent services—advanced quality of service based on Layer 2 through Layer 4 parameters
- Superior Security features: based on Layer 2 through Layer 4 Access Control Parameters
- Sophisticated Multicast Management via IGMP Snooping

Doc: QOS R 0200 CN PMU 0398 ORREIGS 3/10/98

(1)

- Scalability and high availability features
- Cisco Cluster Management (CMS) software offers superior manageability, ease-of-use and ease-of-deployment and enhanced configuration wizards
- Enhanced Cisco IOS Services
- Support for Cisco Redundant Power System 300 (RPS 300)

Competitive Products

- Hewlett Packard: Procurve 2500 / 4108GL
- Nortel: BPS 2000
- 3 Com: Superstack 3300/4300/4400
- Extreme: Summit 24 e2e3

Specifications

Feature	Catalyst 2950G-48-EI	Catalyst 2950G-24-EI	Catalyst 2950G-24-EI-DC	Catalyst 2950G-12-EI
Fixed Ports	48 port 10/100 autosensing & 2 GBIC-based Gigabit Ethernet ports	24 port 10/100 autosensing & 2 GBIC ports	24 port 10/100 autosensing & 2 GBIC ports and DC Power	12 port 10/100 autosensing & 2 GBIC ports
Modular Slots	None	None	None	None
Backplane	13.6 Gbps	13.6 Gbps	13.6 Gbps	13.6 Gbps
Forwarding Rate	10.1 Mpps	6.6 Mpps	6.6 Mpps	4.8 Mpps
Stackable	Yes	Yes	Yes	Yes
Full-Duplex Capabilities	All Ports	All Ports	All Ports	All Ports
VLAN Maximum	64-port-based VLANS	64-port-based VLANS	64-port-based VLANS	64-port-based VLANS
FEC	Yes	Yes	Yes	Yes
802.1Q	Yes	Yes	Yes	Yes
Multicast	IGMP Snooping	IGMP Snooping	IGMP Snooping	IGMP Snooping
QoS	802.1P, 4 egress queues, WRR	802.1P, 4 egress queues, WRR	802.1P, 4 egress queues, WRR	802.1P, 4 egress queues, WRR
Management Capabilities	SNMP, Telnet, RMON, CWSI, (CLI)-based out-of-band, embedded CMS	SNMP, Telnet, RMON, CWSI, (CLI)-based out-of-band, embedded CMS	SNMP, Telnet, RMON, CWSI, (CLI)-based out-of-band, embedded CMS	SNMP, Telnet, RMON, CWSI, (CLI)-based out-of-band, embedded CMS
Flash Memory	8 MB	8 MB	8 MB	8 MB
CPU DRAM	64 MB	64 MB	64 MB	64 MB
Embedded RMON	History, Events, Alarms, Statistics	History, Events, Alarms, Statistics	History, Events, Alarms, Statistics	History, Events, Alarms, Statistics
Dimensions (H x W x D)	1.72 x 17.5 x 13 in.	1.72 x 17.5 x 9.52 in.	1.72 x 17.5 x 9.52 in.	1.72 x 17.5 x 9.52 in.

Feature	Catalyst 2950T-24	Catalyst 2950C-24	Catalyst 2950-24	Catalyst 2950-12
Fixed Ports	26-port (24 10/100 autosensing & 2 ports 1000BaseT	26-port (24 10/100 autosensing & 2 ports100BaseFX)	24-port 10/100 autosensing	12-port 10/100 autosensing
Modular Slots	None	None	None	None
Backplane	8.8 Gbps	8.8 Gbps	8.8 Gbps	8.8 Gbps
Forwarding Rate	6.6 Mpps	3.9 Mpps	3.6 Mpps	1.8 Mpps
Stackable	No	No	No	No
Full-Duplex Capabilities	All Ports	All Ports	All Ports	All Ports
VLAN Maximum	64-port-based VLANS	64-port-based VLANS	64-port-based VLANS	64-port-based VLANS
FEC	Yes	Yes	Yes	Yes

ANEXO (14 B)

16.792
2

CISCO SYSTEMS

Data Sheet

Cisco Systems **GigaStack Gigabit Interface Converter**

The Cisco Systems GigaStack® Gigabit Interface Converter (GBIC) is a versatile, low-cost, Gigabit Ethernet stacking GBIC that offers high-speed interconnectivity between Catalyst® 3550, 2950G, 3500 XL and modular Catalyst 2900 XL Switches.

The GigaStack GBIC is implemented in a standard GBIC form, which offers customers the highest level of deployment flexibility and scalability—using available Gigabit Ethernet GBIC ports for high-performance stacking today while preserving the option to migrate to standard Gigabit Ethernet uplinks tomorrow.

Figure 1 The two-port GigaStack GBIC delivers high-speed interconnectivity for stacking connections

The GigaStack GBIC offers wiring closet deployment flexibility through its dual operating modes. It delivers a 1-Gbps forwarding rate in a half-duplex cascade configuration or up to 2-Gbps full-duplex connectivity in a dedicated, switch-to-switch configuration. The two-port GigaStack GBIC allows customers to deploy the GigaStack GBIC with various performance and cabling options. Customers can initially deploy the low-cost GigaStack GBIC to create a 1-Gbps independent stack backplane in a cascade configuration. At any point, customers may increase stack performance to 12 Gbps using the same GigaStack GBICs in combination with the high-performance Catalyst 3550-12G Gigabit Ethernet aggregation switch.

Half-Duplex Configuration Options

Using both ports of each GigaStack GBIC, users can implement a half-duplex cascade of up to nine switches. In this configuration, the GigaStack GBIC will create a half-duplex repeater bus external to the switch fabric of connected switches. This means that traffic bound from one switch to another will not traverse the switch fabric of intermediate switches. Support for nine switches in a single GigaStack stack offers significant wiring-closet port growth opportunities up to a maximum of 432 10/100 ports per stack.

Customers can choose to implement various stackwide physical redundancy options to provide the highest levels of resiliency. For example, users can choose to deploy a 1-meter redundant loopback cable and a second GigaStack GBIC in the top and bottom stack members. This will create a secondary failover connection in the rare case that a stack member or stack cable fails. Alternatively, users can choose to deploy a 1-meter redundant loopback cable attached to the unused GigaStack ports in the top and

RQS nº 03/2005 - CN -
CPMI - CORREIOS
999
Fls Nº
3702
Doc:

All contents are Copyright © 2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

16-791
L

bottom stack members. New switch cluster command management redundancy features enable the switches to achieve the highest levels of system resiliency.

Figure 2 illustrates a switch stack combined with the GigaStack GBIC half-duplex cascade feature. This configuration depicts a stack of Catalyst 3550 switches and is suitable for those who recognize the need for Gigabit Ethernet uplinks today. In this scenario, connection redundancy is ensured via the redundant loopback cable attached to the top and bottom switches in the stack.

Figure 2 Half-Duplex GigaStack Cascade Configuration

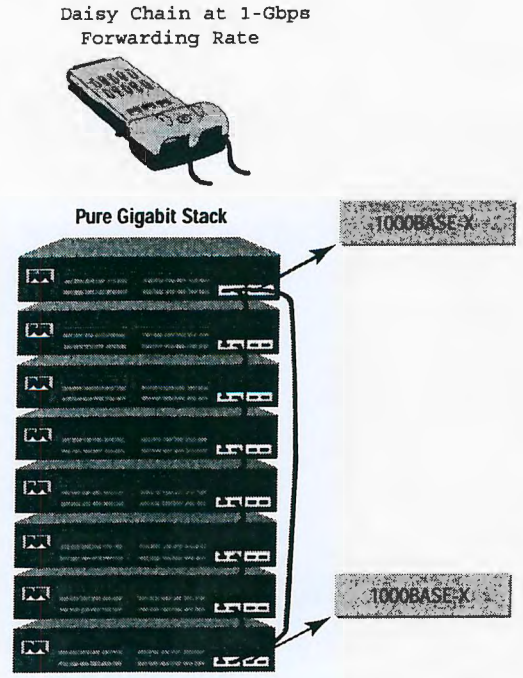
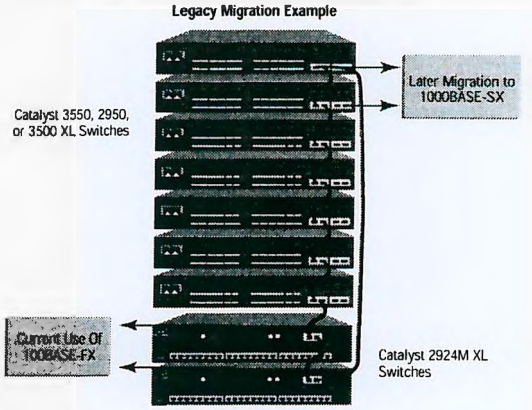


Figure 3 illustrates how the Catalyst 2912MF XL or Catalyst 2924M XL switch can be used in combination with Catalyst 3550, 2950G, or 3500 XL switches using the GigaStack GBIC half-duplex cascade feature. This configuration will provide the flexibility to implement a migration plan from legacy uplink connections to Gigabit Ethernet in the future. For example, each Catalyst 2924M XL switch may initially be used to support 100BASE-FX or ATM uplinks while still maintaining the full capabilities of Gigabit Ethernet stacking and compatibility with Cisco Switch Clustering Management. At any subsequent time, Catalyst 3550 or 2950G switches may be used to support a migration plan to Gigabit Ethernet fiber uplinks.

Figure 3 Half-Duplex GigaStack Cascade Configuration with Legacy Uplink Migration Flexibility



Full-Duplex Configuration Options

Customers can also use the GigaStack GBIC to create a low-cost dedicated Gigabit Ethernet connection between two stack members, providing a scalability option to increase overall stack bandwidth. When connecting two GigaStack GBICs with a single cable, the GBIC will autonegotiate to full-duplex and provide a 1-Gbps forwarding rate in each direction—or 2 Gbps. By simply changing the stack configuration from a cascade to a star configuration, customers can provide dedicated Gigabit Ethernet connectivity to each stack member. When combined with a Catalyst 3550-12G Gigabit Ethernet aggregation switch, this solution offers a very high-performance migration path. The Catalyst 3550-12G can provide stack aggregation with Gigabit Ethernet port connectivity.

All contents are Copyright © 2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN - CPMI - CORREIOS
1000
Fls Nº
3702
Doc:

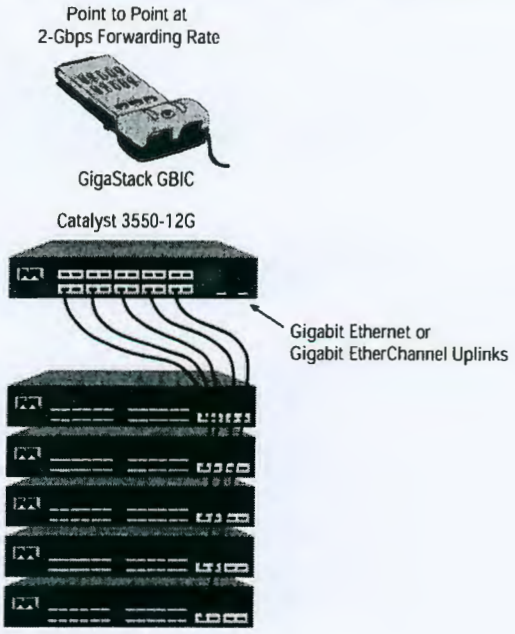
16.790
L

Users can also choose to implement higher levels of resiliency in their full-duplex GigaStack configurations. High levels of redundancy can be implemented within the wiring closet stack and on the network core uplinks. Within the wiring closet, a second Catalyst 3550-12T or 3550-12G aggregation switch can be deployed with redundant links to each stack member. And, redundant uplinks can be deployed from the distribution layer to the network core. When deploying redundant gigabit uplinks, users can benefit from link failover times that are significantly shorter than standard Spanning Tree Protocols. By implementing the Cisco UplinkFast feature, failover can be minimized to as little as 1 to 2 seconds. In addition, the Cisco Per-VLAN Spanning Tree Plus (PVST+) feature can be deployed to ensure that all redundant uplinks perform load balancing. In other words, all redundant uplinks are active and carry traffic.

Users can achieve even higher levels of performance in their full-duplex stacks by configuring dual links from an aggregation switch to each stack member. The two Gigabit Ethernet ports on each Catalyst 3550 Series switch can be grouped together using Gigabit EtherChannel® technology to create a stack connection with a full-duplex 4-Gbps forwarding rate.

Figure 4 illustrates a switch stack configured with GigaStack GBICs operating in full-duplex mode. In this configuration, the Catalyst 3550-12G Gigabit Ethernet switch creates a high-performance option for switch aggregation using point-to-point links. Fault tolerance is implemented via a redundant Catalyst 3550-12G switch. High-speed uplinks from the Catalyst 3550-12G switch to the network core are provided via Gigabit EtherChannel technology.

Figure 4 Full-Duplex GigaStack Star Configuration



Full Compatibility with Cisco Switch Clustering Management Technology

Users can choose to deploy GigaStack GBIC stacking while benefiting from the powerful multidevice management technology available in Cisco Switch Clustering technology. Switch Clustering technology allows customers to manage a stack of devices within a wiring closet or a broadly dispersed set of devices across a campus as a single IP entity. Switch Clustering technology uses standard TCP/IP packets to distribute and collect management information for all switches in the cluster. Switch Clustering supports a broad range of physical interconnections, including the GigaStack GBIC.

Cisco Systems, Inc.
All contents are Copyright © 2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1001
3702
Doc:

16.789
L.

Key Features and Benefits

- Delivers a hardware-based, independent stack bus with 1-Gbps forwarding bandwidth in a half-duplex, cascade configuration, or up to a 2-Gbps forwarding rate in a point-to-point, full-duplex configuration
- Allows up to nine switches to be interconnected in a half-duplex, cascade stack configuration, forming a highly scalable 1-Gbps independent stack bus
- When deployed in full-duplex in combination with a Catalyst 3550-12T or 3550-12G aggregation switch, provides a high-performance option for switch aggregation using point-to-point links
- Standard GBIC form factor provides customers unprecedented flexibility in installation and deployment
- Offers many redundancy and resiliency options to ensure network availability
- Delivers a hardware-based stacking solution to Catalyst 3550, 2950G, 3500 XL switches and gigabit-enabled Catalyst 2900 Series XL switches
- Full- and half-duplex autonegotiating automatically selects and optimizes bandwidth between interconnected switches

Technical Specifications

Performance

- 1 Gbps in half-duplex, cascade configuration; 2 Gbps in point-to-point, full-duplex configuration

Supported Products

- Catalyst 3550 Series
- Catalyst 2950G Switches
- Catalyst 3500 Series XL
- Catalyst 2912MF XL
- Catalyst 2924M XL

Standards

- IEEE 802.3z, IEEE 802.3x 1000BASE-X half/ full-duplex specification

Y2K

- Y2K compliant

Connectors and Cabling

- Switch connection: GBIC-compliant connector
- Stacking connection: copper-based Cisco GigaStack cabling

Indicators

- Link integrity, disabled, activity, speed, and full-duplex indications

Dimensions and Weight (H x W x D)

- 0.75 x 1.54 x 3.50 in. (1.90 x 3.91 x 8.89 cm)
- 1.8 oz (56 grams)

Environmental Conditions and Power Requirements

- Operating temperature: 32 to 113 F (0 to 45 C)
- Storage temperature: –13 to 158 F (–25 to 70 C)
- Operating relative humidity: 10 to 85% noncondensing
- Operating altitude: up to 10,000 ft (3000 m)
- Power consumption: 2W maximum; 6.8 BTU per hour
- MTBF 4.4 million hours

Safety Certifications

- UL 1950
- CSA 22.2 No. 950
- EN 60950
- IEC 950
- AS/NZS 3260, TS001
- CE

Cisco Systems, Inc.
All contents are Copyright © 2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1002
3702
Doc:

16-788
D

Electromagnetic Emissions Certifications

- FCC Part 15 Class A
- EN 55022B Class A (CISPR 22 Class A)
- VCCI Class A
- AS/NZS 3548 Class A
- BCIQ
- CE Marking

Warranty

- Lifetime limited warranty

Ordering Information

- Model Number: WS-X3500-XL (Cisco GigaStack GBIC and 50 centimeter cable for GigaStack GBIC)
- Cable: CAB-GS-1M (1 meter cable for GigaStack GBIC)

For More Information on Cisco Products, Contact:

- U.S. and Canada: 800 553-NETS (6387)
- Europe: 32 2 778 4242
- Australia: 612 9935 4107
- Other: 408 526-7209
- World Wide Web URL: http://www.cisco.com

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 317 7777
Fax: +65 317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the **Cisco Web site at www.cisco.com/go/offices**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

All contents are Copyright © 1992–2002, Cisco Systems, Inc. All rights reserved. Catalyst, Cisco, Cisco Systems, Cisco IOS, the Cisco Systems logo, and EtherChannel are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0206R)

0702/BW8402

ROS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1003
3702
Doc:

ANEXO (14C)

16.787
L

Installation

This chapter describes how to install your switch, interpret the power-on self-test (POST), and connect the switch to other devices. Read these topics, and perform the procedures in this order:

- Preparing for Installation, page 2-2
- Verifying Switch Operation, page 2-10
- Installing the Switch in a Rack, page 2-15
- Installing the Switch on a Table, Shelf, or Desk, page 2-26
- Installing the Switch on a Wall, page 2-27
- Installing the GBIC Modules, page 2-30
- Installing and Removing SFP Modules, page 2-32
- Connecting to 10/100 and 10/100/1000 Ports, page 2-36
- Connecting to 100BASE-FX and 1000BASE-SX Ports, page 2-40
- Connecting to an LRE Port, page 2-42
- Connecting to GBIC Module Ports, page 2-45
- Connecting to an SFP Module, page 2-50
- Where to Go Next, page 2-51

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1004
3702
Doc:

16-786
6

Preparing for Installation

This section provides information about these topics:

- Warnings, page 2-2
- EMC Regulatory Statements, page 2-4
- Installation Guidelines, page 2-7
- Verifying Package Contents, page 2-9

Warnings

These warnings are translated into several languages in Appendix C, "Translated Safety Warnings."

Warning **This equipment is to be installed and maintained by service personnel only as defined by AS/NZS 3260 Clause 1.2.14.3 Service Personnel.**

Warning **This unit is intended for installation in restricted access areas. A restricted access area can be accessed only through the use of a special tool, lock and key, or other means of security.**

Warning **Only trained and qualified personnel should be allowed to install or replace this equipment.**

Warning **Read the installation instructions before you connect the system to its power source.**

Warning **Unplug the power cord before you work on a system that does not have an on/off switch.**

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1005
Doc: 3702

16.785

Warning Do not stack the chassis on any other equipment. If the chassis falls, it can cause severe bodily injury and equipment damage.

Warning To comply with safety regulations, mount switches on a wall with the front panel facing up.

Warning If a redundant power system (RPS) is not connected to the switch, install an RPS connector cover on the back of the switch.

Warning The plug-socket combination must be accessible at all times because it serves as the main disconnecting device.

Warning To prevent the switch from overheating, do not operate it in an area that exceeds the maximum recommended ambient temperature of 113°F (45°C). To prevent airflow restriction, allow at least 3 inches (7.6 cm) of clearance around the ventilation openings.

Warning When installing the unit, always make the ground connection first and disconnect it last.

Warning This equipment is intended to be grounded. Ensure that the host is connected to earth ground during normal use.

Warning Before working on equipment that is connected to power lines, remove jewelry (including rings, necklaces, and watches). Metal objects will heat up when connected to power and ground and can cause serious burns or weld the metal object to the terminals.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1006
3702
Doc:

16.784
L

Warning **Do not work on the system or connect or disconnect cables during periods of lightning activity.**

Warning **Ultimate disposal of this product should be handled according to all national laws and regulations.**

Warning **Attach only the Cisco RPS (model PWR300-AC-RPS-N1) to the RPS receptacle.**

Warning **Invisible laser radiation may be emitted from disconnected fibers or connectors. Do not stare into beams or view directly with optical instruments.**

Warning **Class 1 laser product**

Warning **Avoid direct exposure to the laser beam**

EMC Regulatory Statements

This section includes specific regulatory statements about the Catalyst 2950 switches.

U.S.A.

U.S. regulatory information for this product is in the front matter of this manual.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1007
Nº 3702
Doc:

16.783

Taiwan

This is a Class A Information product. When used in a residential environment, it may cause radio frequency interference. Under such circumstances, the user may be requested to take appropriate countermeasures.

警告使用者：
這是甲類的資訊產品，在居住的環境中使用時，可能會造成射頻干擾，在這種情況下，使用者會被要求採取某些適當的對策。

Japan

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。

46464

RQS nº 03/2005 - CN -
CPMI - CORREIOS
1008
Fls Nº
3702
Doc:

16 782
2

Korea

Warning **This is a Class A Device and is registered for EMC requirements for industrial use. The seller or buyer should be aware of this. If this type was sold or purchased by mistake, it should be replaced with a residential-use type.**

주의 A급 기기 이 기기는 업무용으로 전자파 적합 등록을 한 기기이오니 판매자 또는 사용자는 이 점을 주의하시기 바라며 만약 잘못 판매 또는 구입하였을 때에는 가정용으로 교환하시기 바랍니다.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1009
3702
Doc:

16.781
2

Hungary

This equipment is a Class A product and should be used and installed properly according to the Hungarian EMC Class A requirements (MSZEN55022). Class A equipment is designed for typical commercial establishments for which special conditions of installation and protection distance are used.

Figyelmeztetés a felhasználói kézikönyv számára:
Ez a berendezés "A" osztályú termék, felhasználására és üzembe helyezésére a magyar EMC "A" osztályú követelményeknek (MSZ EN 55022) megfeleloen kerülhet sor, illetve ezen "A" osztályú berendezések csak megfelelo kereskedelmi forrásból származhatnak, amelyek biztosítják a megfelelo speciális üzembe helyezési körülményeket és biztonságos üzemelési távolságok alkalmazását.

Installation Guidelines

When determining where to place the switch, observe these guidelines.

- Before installing the switch, first verify that the switch is operational by powering it on and running POST. Follow the procedures in the "Powering On the Switch and Running POST" section on page 2-14.
- For 10/100 ports and 10/100/1000 ports, the cable length from a switch to an attached device cannot exceed 328 feet (100 meters).
- For 100BASE-FX ports, the cable length from a switch to an attached device cannot exceed 6562 feet (2 kilometers).
- For 1000BASE-SX ports and 1000BASE-SX GBIC module ports, the cable length from a switch to an attached device cannot exceed 1804 feet (550 meters).
- For 1000BASE-LX/LH GBIC module ports, the cable length from a switch to an attached device cannot exceed 32,810 feet (10 kilometers).
- For 1000BASE-ZX GBIC module ports, the cable length from a switch to an attached device cannot exceed 328,100 feet (100 kilometers).
- For 1000BASE-T GBIC module ports, the cable length from switch to an attached device cannot exceed 328 feet (100 meters).

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1010
Nº 370
Doc:

- For Coarse Wave Division Multiplexing (CWDM) GBIC module ports, the cable length from a switch to an attached device cannot exceed 393,719 feet (120 kilometers). For specific cable lengths, refer to the CWDM GBIC module documentation.
- For GigaStack GBIC module ports, the cable length from a switch to an attached device cannot exceed 3 feet (1 meter).
- For LRE ports, cable-length specifications vary. Refer to the "LRE Ports" section on page 1-11.
- Operating environment is within the ranges listed in Appendix A, "Technical Specifications."
- Clearance to front and rear panels meet these conditions:
  - Front-panel LEDs can be easily read.
  - Access to ports is sufficient for unrestricted cabling.
  - Rear-panel AC power connector is within reach of an AC power outlet.
  - Rear-panel direct current (DC) power connector is within reach of a circuit breaker.
- Airflow around the switch and through the vents is unrestricted.
- Temperature around the unit does not exceed 113°F (45°C).

Note If the switch is installed in a closed or multirack assembly, the temperature around it might be greater than normal room temperature.

- Cabling is away from sources of electrical noise, such as radios, power lines, and fluorescent lighting fixtures.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1011
Nº 3702
Doc:

16.779

Verifying Package Contents

Note Carefully remove the contents from the shipping container, and check each item for damage. If any item is missing or damaged, contact your Cisco representative or reseller for support. Return all packing materials to the shipping container and save them.

The switch is shipped with these items:

- AC power cord
- Mounting kit containing these items:
  - Four rubber feet for mounting the switch on a table, shelf, or desk
  - Two 19-inch or 24-inch rack-mounting brackets
  - Six number-8 Phillips flat-head screws for attaching the brackets to the switch
  - Four number-8 Phillips truss-head screws for attaching the brackets to the switch
  - Four number-12 Phillips machine screws for attaching the brackets to a rack
  - One cable guide and one black Phillips machine screw for attaching the cable guide to one of the mounting brackets
  - RPS connector cover
- DC-switch kit containing these items:
  - One DC terminal block plug (also called a terminal block header)
  - One ground lug
  - Two number-10-32 screws for attaching the ground lug to the switch
  - Two 23-inch rack-mounting brackets (with 1-inch spacing for telco racks)
  - Four number-8 Phillips truss-head screws for attaching the brackets to the switch

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1012
Doc 3702

16.728

- Two number-12 Phillips machine screws for attaching the brackets to a rack

Note The DC-switch kit ships only with the Catalyst 2950G-24-EI-DC switch.

- One RJ-45-to-DB-9 adapter cable
- Product ownership registration card

If you want to connect a terminal to the switch console port, you need to provide an RJ-45-to-DB-25 female DTE adapter. You can order a kit (part number ACS-DSBUASYN=) with that adapter from Cisco.

You can connect a 100BASE-FX or 1000BASE-SX port to an SC or ST port on a target device by using one of the MT-RJ fiber-optic patch cables listed in Table 2-1. Use the Cisco part numbers in Table 2-1 to order the patch cables that you need.

Table 2-1 MT-RJ Patch Cables for 100BASE-FX and 1000BASE-SX Connections

Type	Cisco Part Number
1-meter, MT-RJ-to-SC multimode cable	CAB-MTRJ-SC-MM-1M
3-meter, MT-RJ-to-SC multimode cable	CAB-MTRJ-SC-MM-3M
5-meter, MT-RJ-to-SC multimode cable	CAB-MTRJ-SC-MM-5M
1-meter, MT-RJ-to-ST multimode cable	CAB-MTRJ-ST-MM-1M
3-meter, MT-RJ-to-ST multimode cable	CAB-MTRJ-ST-MM-3M
5-meter, MT-RJ-to-ST multimode cable	CAB-MTRJ-ST-MM-5M

Verifying Switch Operation

Before installing the switch in a rack, on a wall, or on a table or shelf, you should power on the switch and verify that the switch passes POST. These sections describe the steps required to connect a PC to the switch console port and to power on the switch.

- Connecting a PC or a Terminal to the Console Port, page 2-11

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1013
Nº 3702
Doc:

16.777
2

• Powering On the Switch and Running POST, page 2-14

Connecting a PC or a Terminal to the Console Port

To connect a PC to the console port, use the supplied RJ-45-to-DB-9 adapter cable. To connect a terminal to the console port, you need to provide an RJ-45-to-DB-25 female DTE adapter. You can order a kit (part number ACS-DSBUASYN=) with that adapter from Cisco. For console-port and adapter-pinout information, see the"Cable and Adapter Specifications" section on page B-9.

The PC or terminal must support VT100 terminal emulation. The terminal-emulation software—frequently a PC application such as HyperTerminal or Procomm Plus—makes communication between the switch and your PC or terminal possible during the setup program.

Follow these steps to connect the PC or terminal to the switch:

Step 1 Make sure that your terminal-emulation software is configured to communicate with the switch through hardware flow control.

Step 2 Configure the baud rate and character format of the PC or terminal to match these console-port default characteristics:

- 9600 baud
- Eight data bits
- One stop bit
- No parity

After gaining access to the switch, you can change the port baud rate. Refer to the switch software configuration guide for instructions.

Step 3 Insert the adapter cable in the console port, as shown in Figure 2-1 through . (See the "Cable and Adapter Pinouts" section on page B-12 for pinout descriptions.)

Note The console port is on the front panel of the Catalyst 2950 LRE switches.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1014
Doc: 3702

16.776

Figure 2-1 Connecting to the Console Port

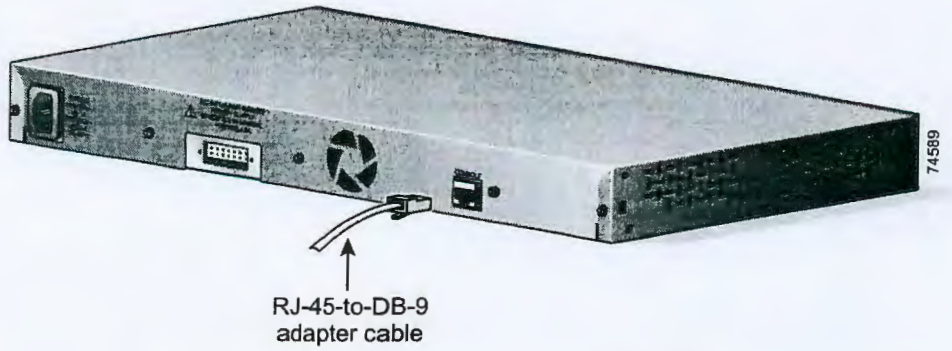
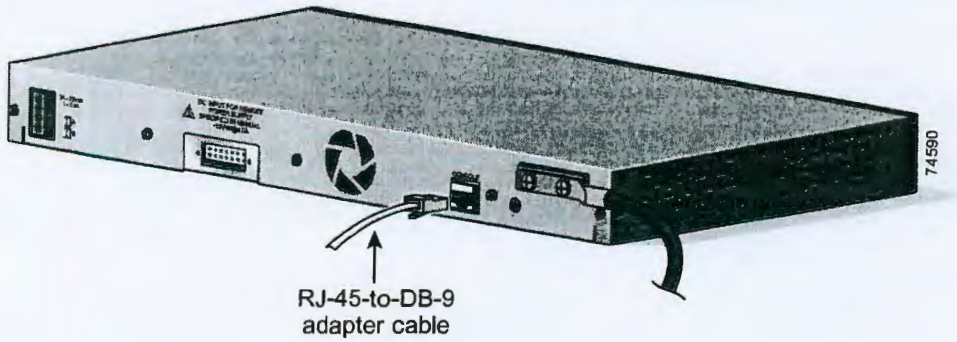


Figure 2-2 Connecting to a Console Port Only on Catalyst 2950G-24-EI-DC Switches



RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1015
3702
Doc

16.775
2

Figure 2-3 Connecting to a Console Port Only on Catalyst 2950G-48-EI Switches

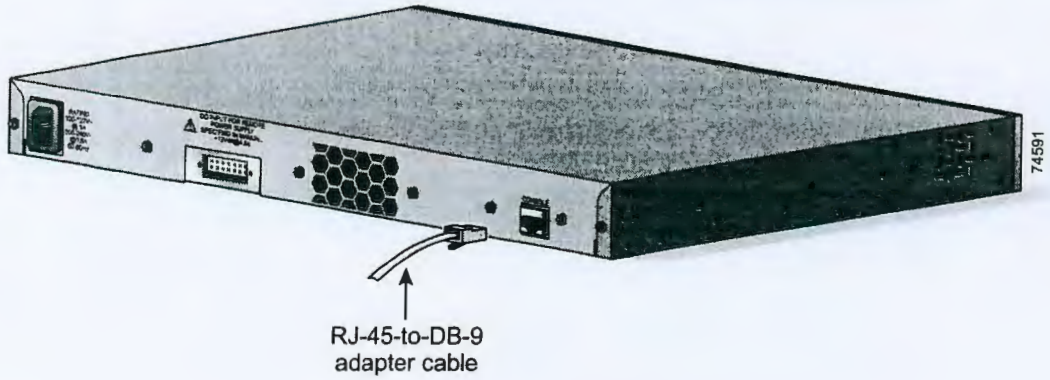
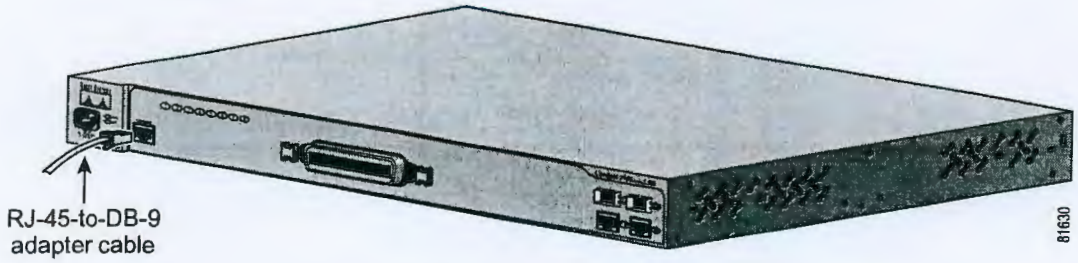


Figure 2-4 Connecting to a Console Port Only on Catalyst 2950ST-8 LRE and Catalyst 2950ST-24 LRE Switches



Step 4 Attach the appropriate adapter to the terminal, if needed.

Step 5 Insert the other adapter cable end in the PC or terminal adapter.

Step 6 Start the terminal-emulation software.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1016
3702
Data:

16.774

Powering On the Switch and Running POST

If your switch is connected to an RPS, connect the switch and the RPS to the same AC power source. Refer to the Cisco RPS documentation for more information. For information about connecting a Catalyst 2950G-24-EI-DC switch to a DC-input power source, see Appendix D, "Connecting to DC Power."

Note Always put the RPS in standby mode when you are connecting devices to it and in active mode during normal operation.

To power on the switch, follow these steps:

Step 1 Make sure that you have started the terminal emulation software program (such as ProComm, HyperTerminal, tip, or minicom) from your management station. See the "Connecting a PC or a Terminal to the Console Port" section on page 2-11 for information on connecting to the switch console port.

Step 2 Connect one end of the AC power cord to the AC power connector on the switch.

Step 3 Connect the other end of the power cord to an AC power outlet.

Warning **Attach only the Cisco RPS 300 (model PWR300-AC-RPS-N1) to the RPS receptacle.**

After the power is connected, the switch automatically begins POST, a series of tests that verifies that the switch functions properly. When the switch begins POST, the system LED is off. If POST completes successfully, the LED turns green. If POST fails, the LED turns amber. See Chapter 3, "Troubleshooting," to determine a corrective action.

Note POST failures are usually fatal. Call Cisco Systems immediately if your switch does not pass POST.

ECT nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1017
Doc: 3702

16.773
2

After successfully running POST, follow these steps.

Step 1 Turn off power to the switch.

Step 2 Disconnect the cables.

Step 3 Determine where the switch is to be installed.

Installing the Switch in a Rack

Warning **To prevent bodily injury when mounting or servicing this unit in a rack, you must take special precautions to ensure that the system remains stable. The following guidelines are provided to ensure your safety:**

- This unit should be mounted at the bottom of the rack if it is the only unit in the rack.
- When mounting this unit in a partially filled rack, load the rack from the bottom to the top with the heaviest component at the bottom of the rack.
- If the rack is provided with stabilizing devices, install the stabilizers before mounting or servicing the unit in the rack.

Note Figure 2-5 to show the Catalyst 2950-24, 2950G-24-EI-DC, and 2950G-48-EI switches as examples. You can install other Catalyst 2950 switches in a rack as shown in these illustrations.

To install the switch in a 19-, 23-, or 24-inch rack, follow these steps:

- Attaching the Brackets to the Switch, page 2-16
- Mounting the Switch in a Rack, page 2-25
- Attaching the Optional Cable Guide, page 2-26

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1018
Nº 3702
Doc:

16.772

Note Installing the Catalyst 2950G-48-EI switch in a 23-inch or 24-inch rack requires an optional bracket kit not included with the switch. You can order a kit containing the 23-inch or 24-inch rack-mounting brackets and hardware from Cisco (part number RCKMNT-1RU=).

Attaching the Brackets to the Switch

The bracket orientation and the screws that you use depend on whether you are attaching the brackets to a 19-, 23-, or 24-inch rack. Follow these guidelines:

- When mounting a switch other than a Catalyst 2950G-48-EI switch in a 19-inch rack, use two Phillips flat-head screws to attach the long side of the 19- or 24-inch bracket to the switch. See Figure 2-5, Figure 2-6, and Figure 2-7.
- When mounting a Catalyst 2950G-48-EI switch in a 19-inch rack, use three Phillips flat-head screws to attach the long side of the 19- or 24-inch bracket to the switch. See Figure 2-8, Figure 2-9, and Figure 2-10.
- When mounting a Catalyst 2950G-24-EI-DC switch in a 23-inch rack, use two Phillips truss-head screws to attach the 23-inch bracket to the switch. See Figure 2-11, Figure 2-12, and Figure 2-13.
- When mounting a switch other than a Catalyst 2950G-48-EI switch in a 24-inch rack, use two Phillips truss-head screws to attach the 19- or 24-inch bracket to the switch. See Figure 2-14, Figure 2-15, and Figure 2-16.
- When mounting a Catalyst 2950G-48-EI switch in a 24-inch rack, use three Phillips flat-head screws to attach the 24-inch bracket (part number RCKMNT-1RU=) to the switch. See Figure 2-17, Figure 2-18, and Figure 2-19.

Figure 2-5 to Figure 2-19 show how to attach a bracket to one side of the switch. Follow the same steps to attach the second bracket to the opposite side of the switch.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1019
Nº 3702
Doc:

16.771
2

Figure 2-5 Attaching Brackets on the Switch in a 19-Inch Rack (Front Panel Forward)

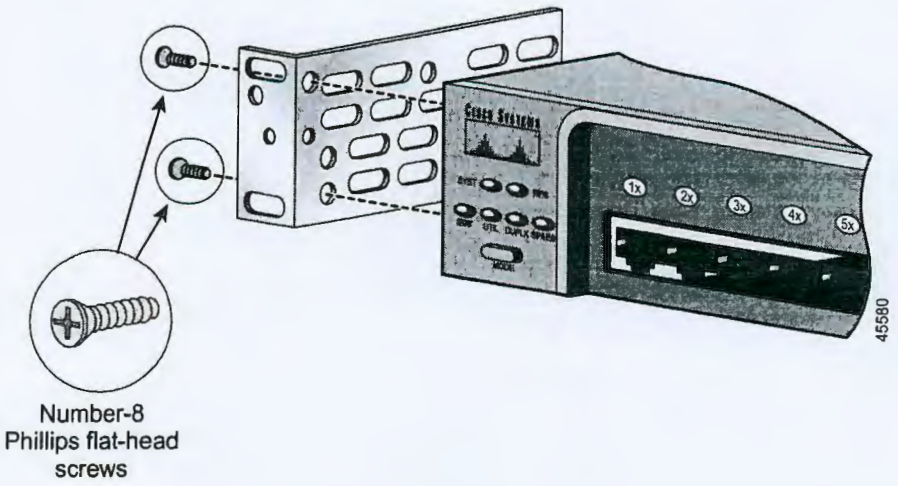
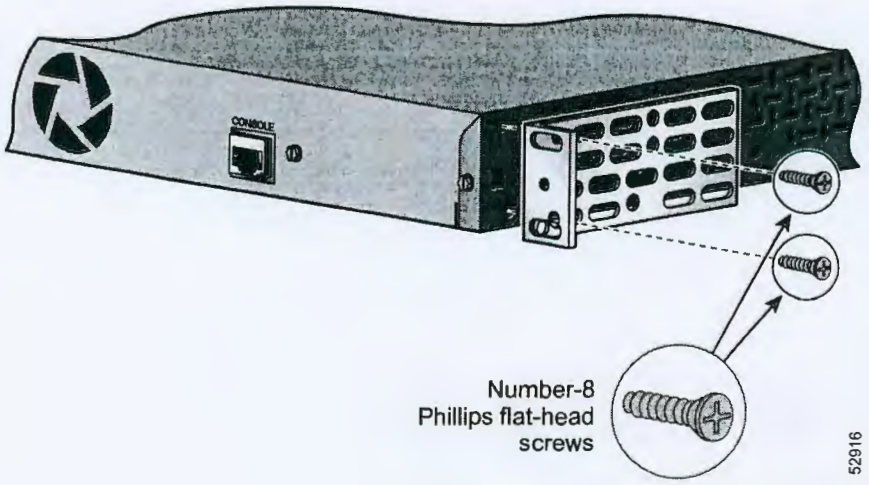


Figure 2-6 Attaching Brackets on the Switch in a 19-Inch Rack (Rear Panel Forward)



RQS nº 03/2005 - CN -
CPMI - CORREIOS
1020
Fls Nº
3702
Doc:

16.770
L

Figure 2-7 Attaching Brackets on the Switch in a 19-Inch Telco Rack

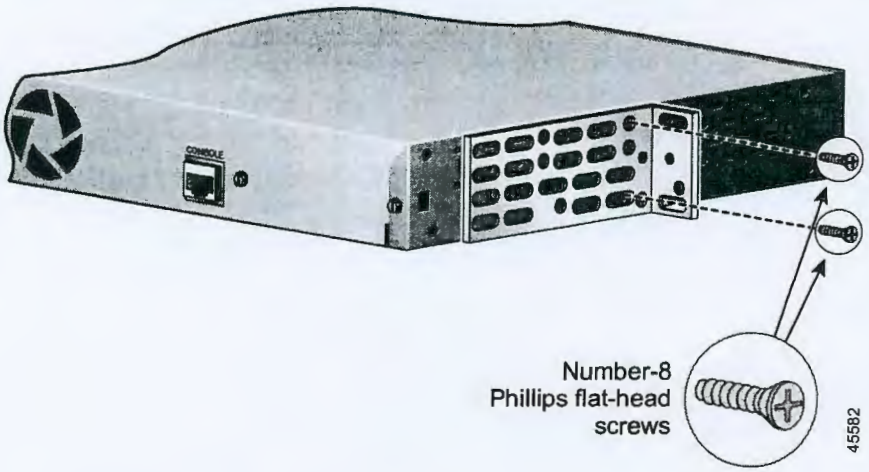
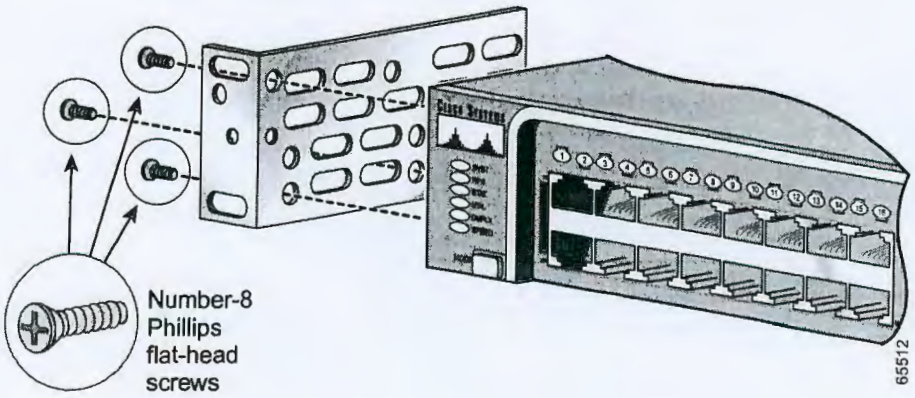


Figure 2-8 Attaching Brackets on the Catalyst 2950G-48-EI Switch in a 19-Inch Rack (Front Panel Forward)



RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1021
3702
Doc:

16.769

Figure 2-9 Attaching Brackets on the Catalyst 2950G-48-EI Switch in a 19-Inch Rack (Rear Panel Forward)

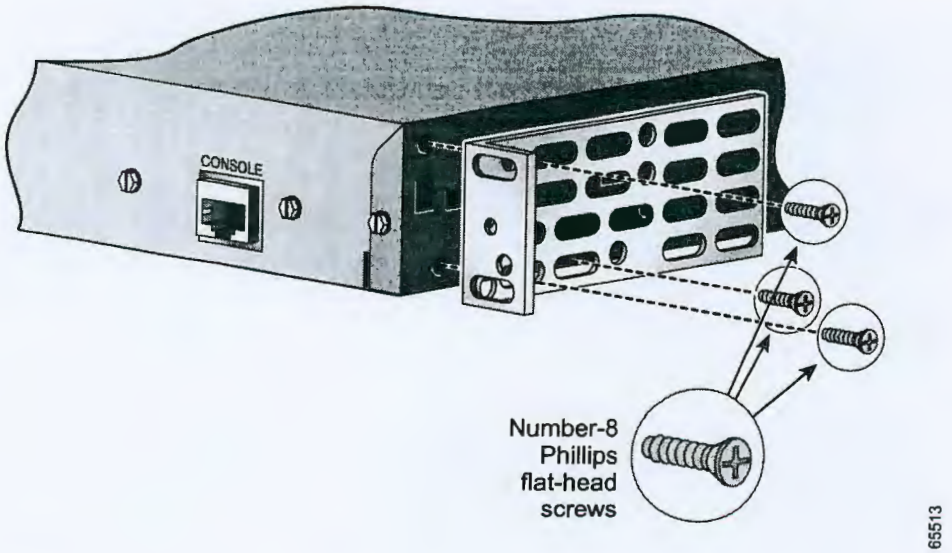
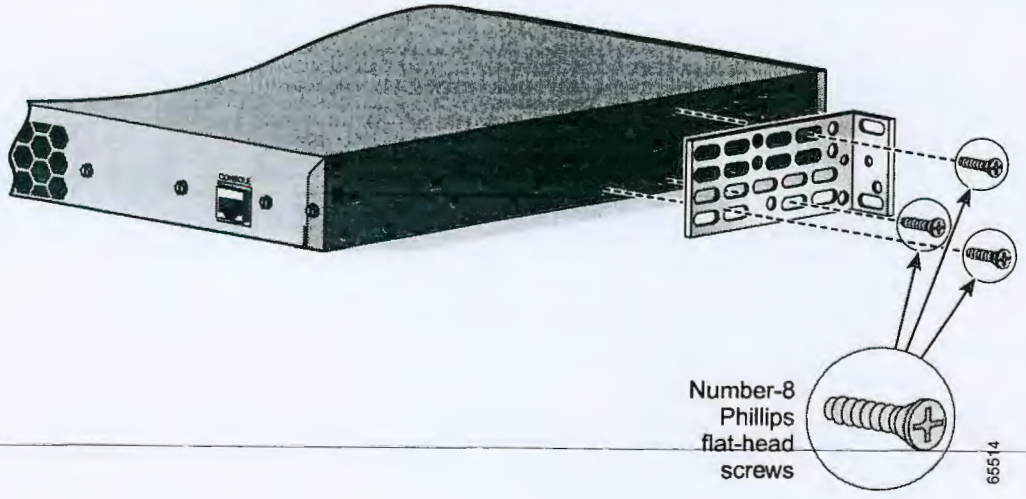


Figure 2-10 Attaching Brackets on the Catalyst 2950G-48-EI Switch in a 19-Inch Telco Rack



RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1022
3702

16.768
L

Figure 2-11 Attaching Brackets on the Catalyst 2950G-24-EI-DC Switch in a 23-Inch Telco Rack (Front Panel Forward)

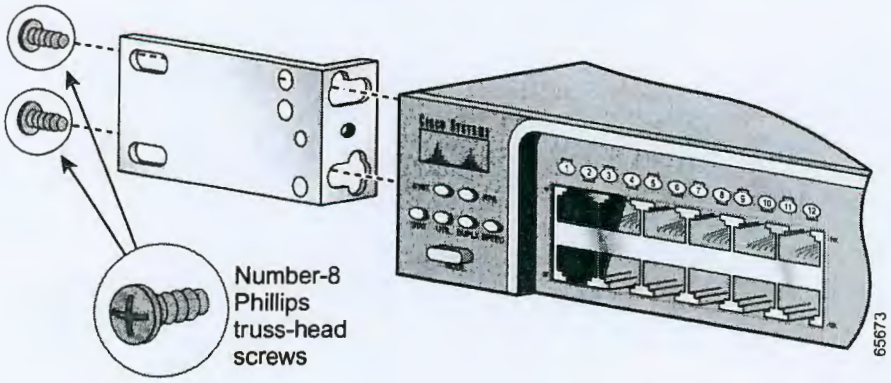
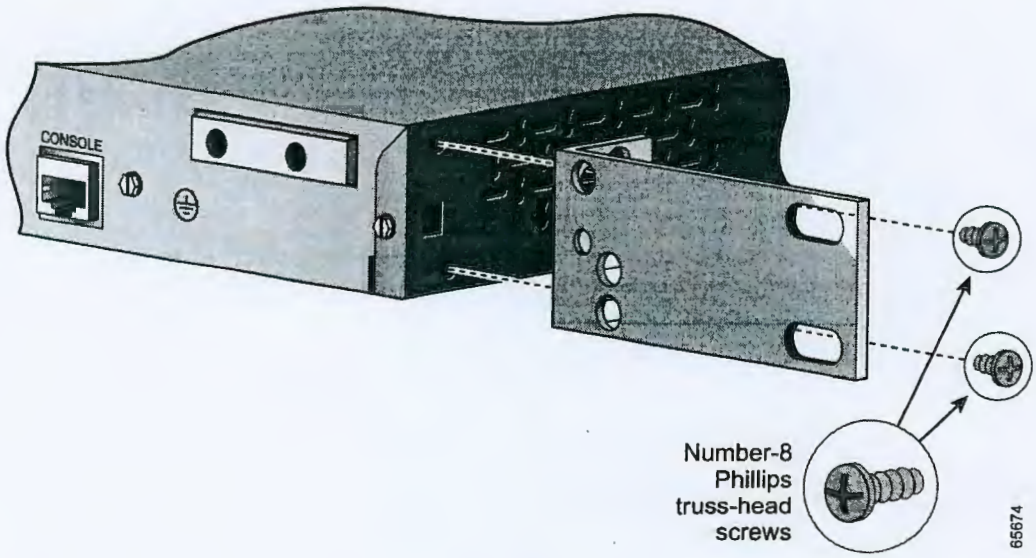


Figure 2-12 Attaching Brackets on the Catalyst 2950G-24-EI-DC Switch in a 23-Inch Telco Rack (Rear Panel Forward)



RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1023
3702

16.767

Figure 2-13 Attaching Brackets on the Catalyst 2950G-24-EI-DC Switch in a 23-Inch Telco Rack

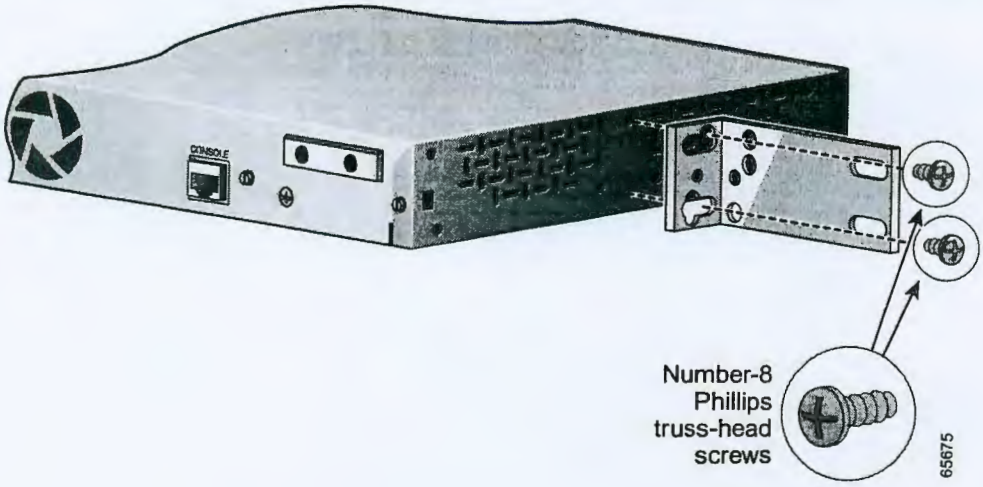
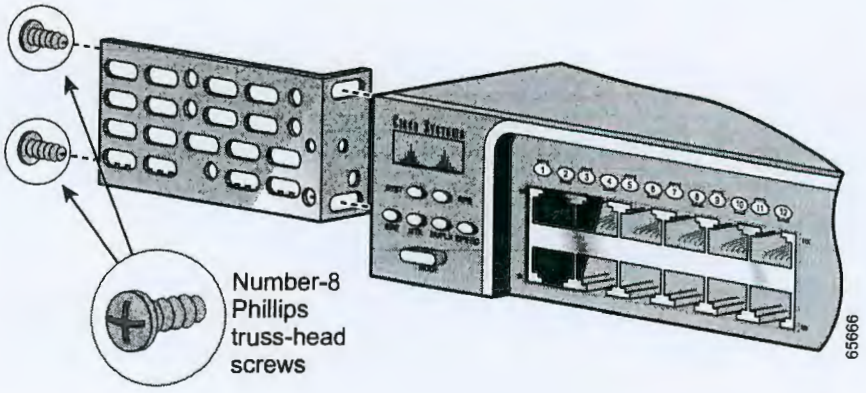


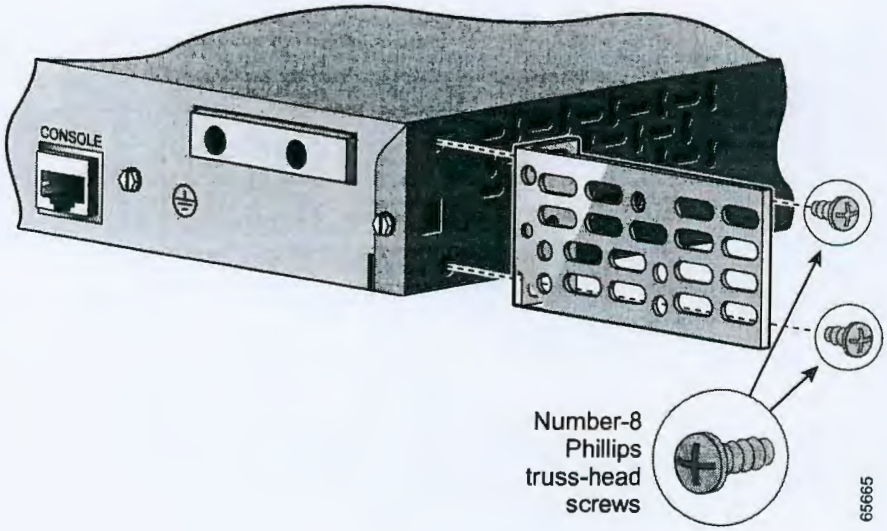
Figure 2-14 Attaching Brackets on the Switch in a 24-Inch Rack (Front Panel Forward)



RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1024
Nº 3702
Doc:

16.766

Figure 2-15 Attaching Brackets on the Switch in a 24-Inch Rack (Rear Panel Forward)



RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1025
Nº 3702
Doc:

16.765
2

Figure 2-16 Attaching Brackets on the Switch in a 24-Inch Telco Rack

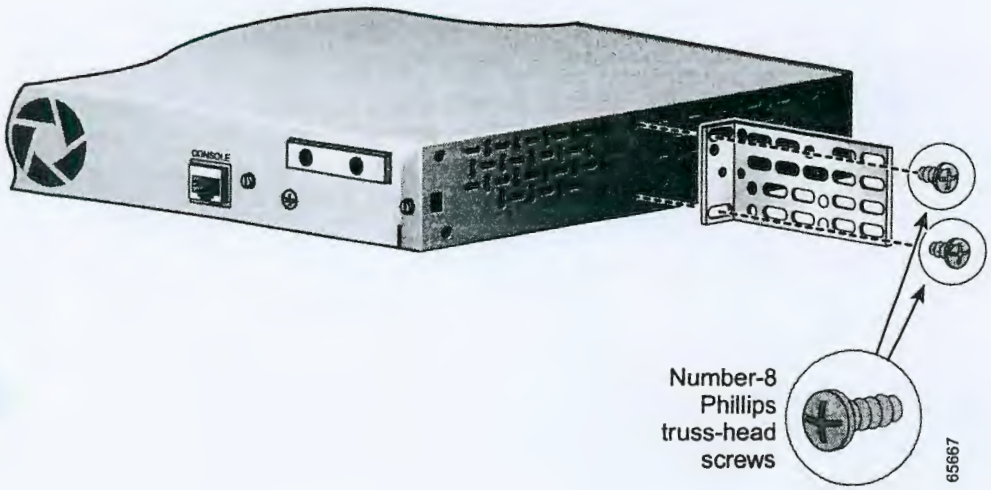
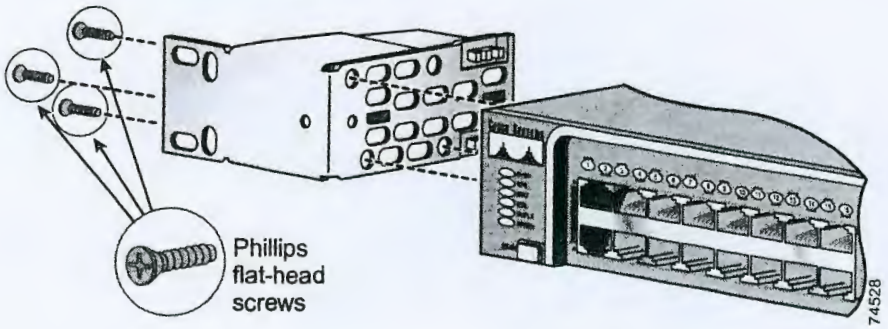


Figure 2-17 Attaching Brackets on the Catalyst 2950G-48-EI Switch in a 24-Inch Rack (Front Panel Forward)



RQS nº 03/20
CPMI - C
Fls Nº 1026
Doc: 3

16.764
2

Figure 2-18 Attaching Brackets on the Catalyst 2950G-48-EI Switch in a 24-Inch Rack (Rear Panel Forward)

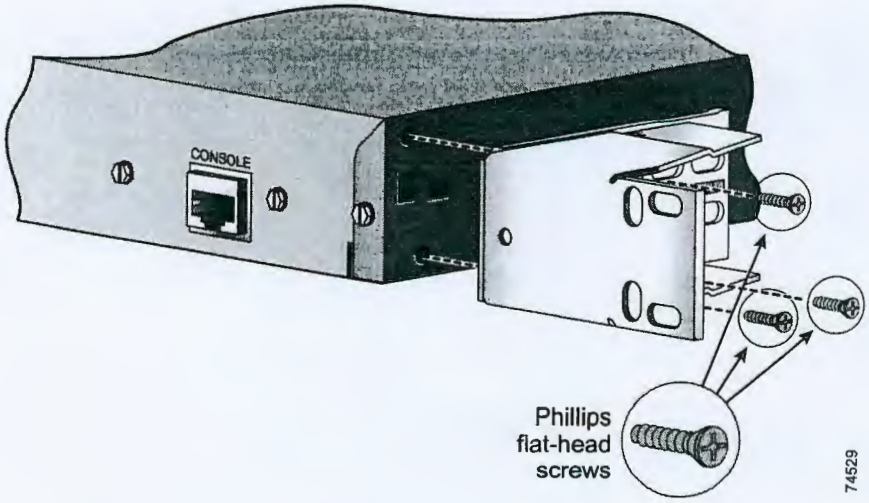
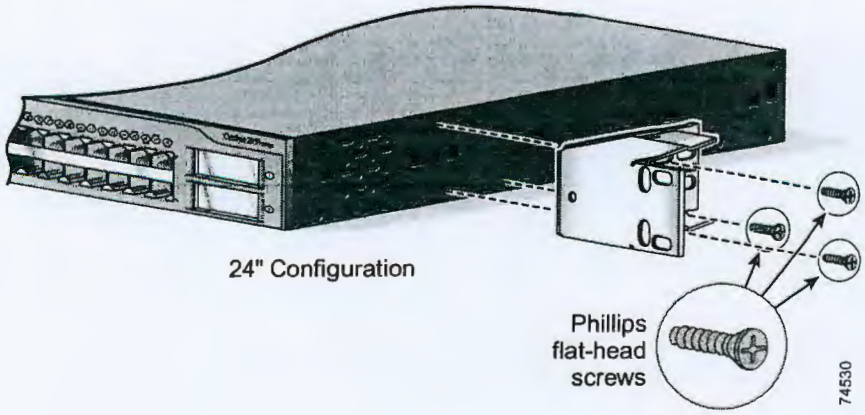


Figure 2-19 Attaching Brackets on the Catalyst 2950G-48-EI Switch in a 24-Inch Telco Rack



RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1027
3702
Doc:

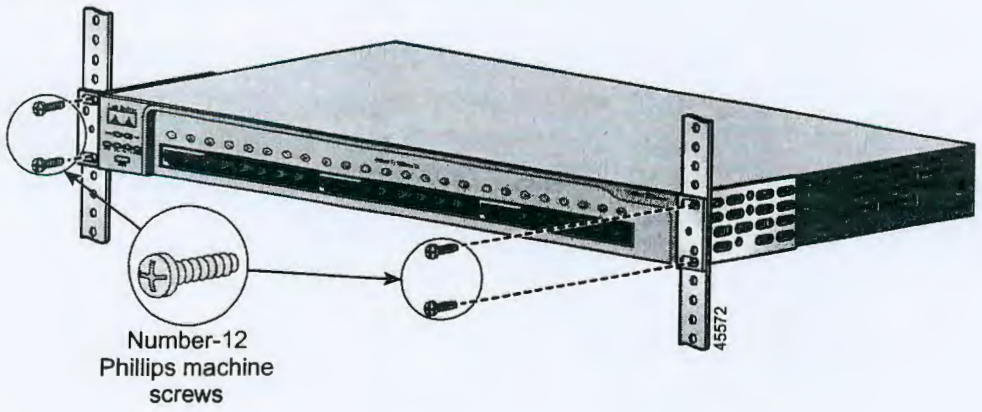
16.763
2

Mounting the Switch in a Rack

After attaching the brackets, use the four Phillips machine screws to securely attach the brackets to the rack, as shown in Figure 2-20.

To prevent the cables from obscuring the switch and other devices in the rack, you can also attach the cable guide to the rack. See the"Attaching the Optional Cable Guide" section for instructions.

Figure 2-20 Mounting the Switch in a Rack



After mounting the switch in the rack, start the terminal-emulation software, and provide power to the switch. See the "Powering On the Switch and Running POST" section on page 2-14 for instructions.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1028
3702
Doc:

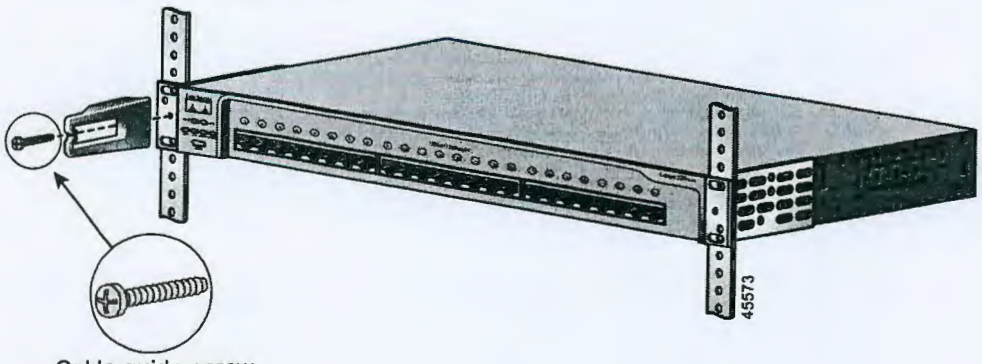
16.762

Attaching the Optional Cable Guide

We recommend attaching the cable guide to prevent the cables from obscuring the front panels of the switch and other devices installed in the rack. Use the supplied black Phillips machine screw to attach the cable guide to the left or right bracket, as shown in Figure 2-21.

Note You cannot use the cable guide with Catalyst 2950 LRE switches.

Figure 2-21 Attaching the Cable Guide



Installing the Switch on a Table, Shelf, or Desk

Before placing the switch on a table, shelf, or desk, locate the adhesive strip with rubber feet in the mounting-kit envelope, and attach four rubber feet to the recessed areas on the switch bottom. Place the switch on a table, shelf, or desk near an AC power source or DC-input power source.

Start the terminal-emulation software and provide power to the switch. See the "Powering On the Switch and Running POST" section for instructions.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1029
Nº 3702 Doc:

16.761
2

Installing the Switch on a Wall

Warning **To comply with safety regulations, mount switches on a wall with the front panel facing up.**

Warning **If a redundant power system (RPS) is not connected to the switch, install an RPS connector cover on the back of the switch.**

You can mount the Catalyst 2950 switch to a wall in a face-up configuration. To attach the switch to a wall, follow the procedures in this section.

- Attaching the brackets to the switch
- Attaching the RPS Connector Cover
- Attaching the switch to a wall

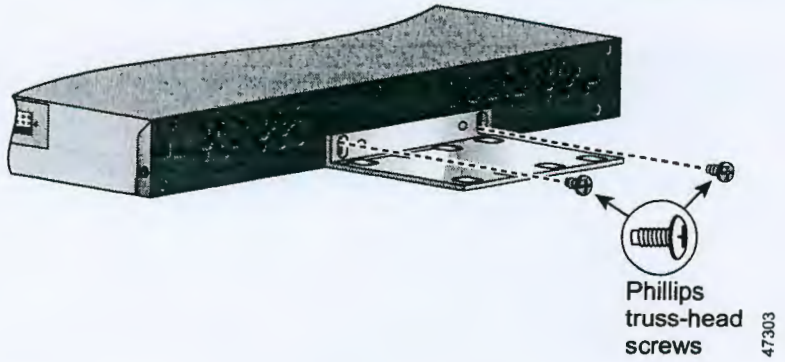
Attaching the Brackets to the Switch

Use the supplied Phillips flat-head screws to attach the long side of the bracket to the switch. Figure 2-22 shows how to attach the brackets to one side of the switch. Follow the same steps to attach the second bracket to the opposite side of the switch.

RQS Nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1030
Doc: 3702

16.760

Figure 2-22 Attaching Brackets for Wall-Mounting for the Catalyst 2950 Switch

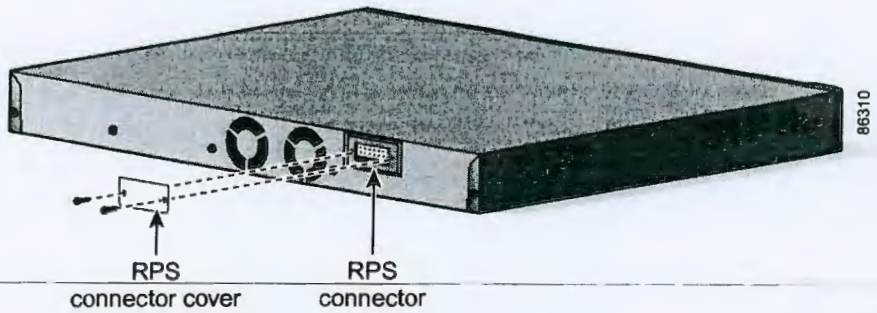


Attaching the RPS Connector Cover

If you are not using a redundant power system (RPS) with your switch, use two number-4 Phillips pan-head screws to install an RPS connector cover to the back of the switch. (See Figure 2-23.) The pan-head screws are included in the accessory kit.

Warning **If an RPS is not connected to the switch, install an RPS connector cover on the back of the switch.**

Figure 2-23 Attaching the RPS Connector Cover



RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1031
Doc: 3702

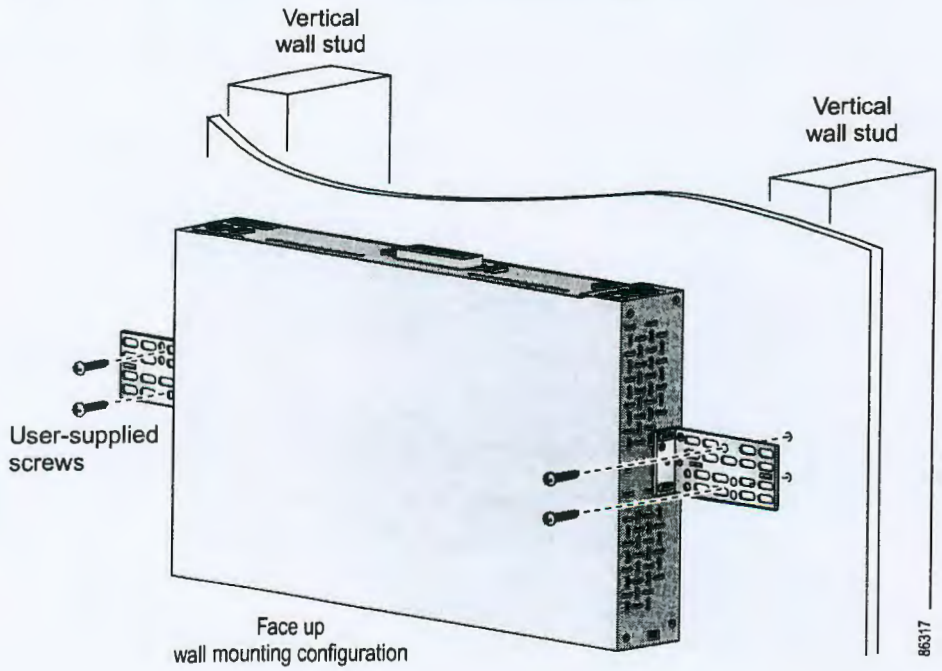
16.759
L

Mounting the Switch to a Wall

Warning **To comply with safety regulations, mount switches on a wall with the front panel facing up.**

For the best support of the switch and cables, make sure the switch is attached securely to a wall stud or to a firmly attached plywood mounting backboard, as shown in Figure 2-24.

Figure 2-24 Mounting a Catalyst 2950 Switch to a Wall



After the switch is mounted on the wall, power the switch as described in "Powering On the Switch and Running POST" section on page 2-14.

03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1032
Doc: 3702

16 753
2

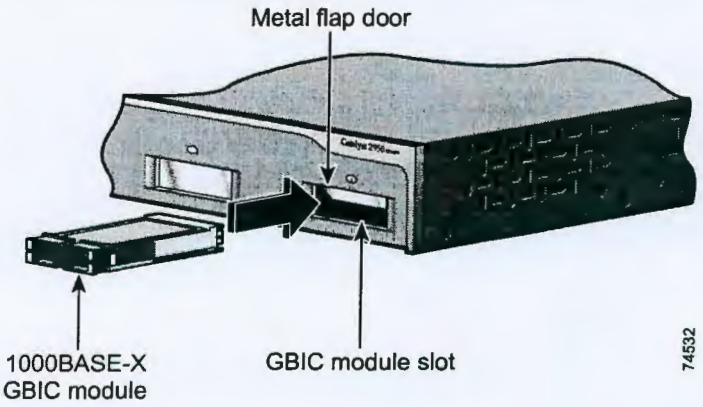
Installing the GBIC Modules

Figure 2-25, Figure 2-26, and Figure 2-27 show how to insert a GBIC module in a GBIC module slot on the switch. For instructions on how to install a CWDM GBIC module in a GBIC module slot, refer to the documentation that came with that GBIC module.

For detailed instructions on installing, removing, and cabling the GBIC module (the 1000BASE-X module, the 1000BASE-T module, the CWDM GBIC module, or the GigaStack module), refer to your GBIC documentation.

Caution To prevent electrostatic-discharge (ESD) damage when installing GBIC modules, follow your normal board and component handling procedures.

Figure 2-25 Installing a 1000BASE-X GBIC Module in a Switch



RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1033
Doc: 3702

16.757
2

Figure 2-26 Installing a 1000BASE-T GBIC Module in a Switch

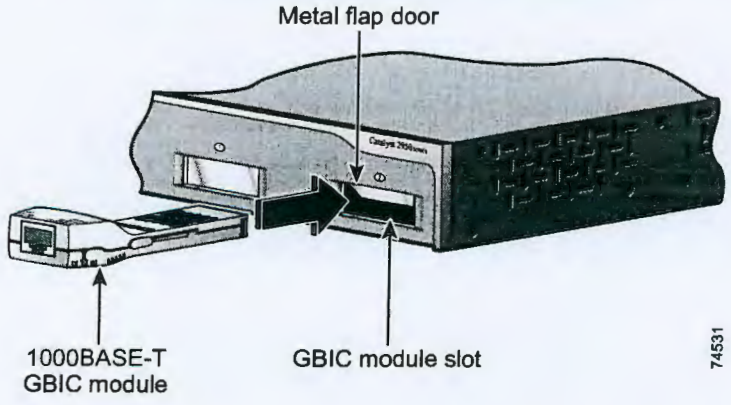
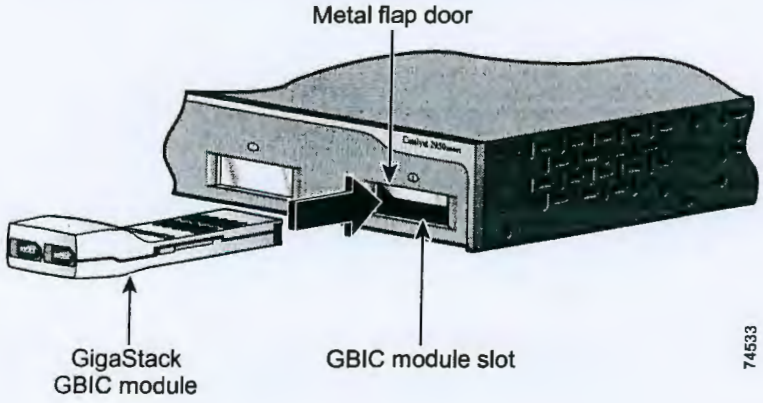


Figure 2-27 Installing a GigaStack GBIC Module in a Switch



03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1034
Doc: 3702

16.756
2

Installing and Removing SFP Modules

These sections describe how to install and remove SFP modules. SFP modules are inserted into SFP module slots on the front of the Catalyst 2950 LRE switches. These field-replaceable modules provide the uplink optical interfaces, laser send (TX) and laser receive (RX).

You can use any combination of SFP modules. Refer to the Catalyst 2950 release notes for the list of SFP modules that the Catalyst 2950 LRE switch supports. The only restriction is that each port must match the wave-length specifications on the other end of the cable, and the cable must not exceed the stipulated cable length for reliable communications. Refer to Table 1-2 for cable stipulations for SFP connections.

Use only Cisco SFP modules on the Catalyst 2950 LRE switch. Each SFP module has an internal serial EEPROM that is encoded with security information. This encoding provides a way for Cisco to identify and validate that the SFP module meets the requirements for the switch.

For detailed instructions on installing, removing, and cabling the SFP module, refer to your SFP module documentation.

Installing SFP Modules into SFP Module Slots

SFP modules use different types of latches for their installation and extraction. Determine which type of latch your SFP module uses before following the installation procedure:

- Figure 2-28 shows an SFP module with a Mylar tab latch.
- Figure 2-29 shows an SFP module with an actuator button latch.
- Figure 2-30 shows an SFP module that has a bale-clasp latch.

Caution We strongly recommend that you do not install or remove the SFP module with fiber-optic cables attached to it because of the potential damage to the cables, the cable connector, or the optical interfaces in the SFP module. Disconnect all cables before removing or installing an SFP module.

Removing and installing an SFP module can shorten its useful life. Do not remove and insert SFP modules more often than is absolutely necessary.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1035
Doc: 3702

16.755

Figure 2-28 SFP Module with a Mylar Tab Latch

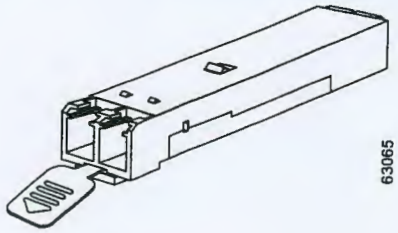


Figure 2-29 SFP Module with an Actuator Button Latch

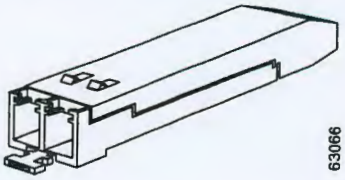
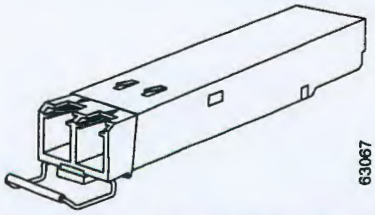


Figure 2-30 SFP Module with a Bale-Clasp Latch



To insert an SFP module into the SFP module slot, follow these steps:

Step 1 Attach an ESD-preventive wrist strap to your wrist and to a bare metal surface on the chassis.

Step 2 Find the send (TX) and receive (RX) markings that identify the top side of the SFP module.

Note On some SFP modules, the send and receive (TX and RX) markings might be replaced by arrows that show the direction of the connection, either send or receive (TX or RX).

RQS nº 03/2005 - CN - CPMI - CORREIOS
1036
Fls Nº
3702
Doc:

16.754

Step 3 Align the SFP module in front of the slot opening.

Step 4 Insert the SFP module into the slot until you feel the connector on the module snap into place in the rear of the slot.

Figure 2-31 Installing an SFP Module into an SFP Module Slot

Step 5 Remove the dust plugs from the SFP module optical ports and store them for later use.

Caution Do not remove the dust plugs from the SFP module port or the rubber caps from the fiber-optic cable until you are ready to connect the cable. The plugs and caps protect the SFP module ports and cables from contamination and ambient light.

Step 6 Insert the LC into the SFP module.

Removing SFP Modules from SFP Module Slots

To remove an SFP module from a module receptacle, follow these steps:

Step 1 Attach an ESD-preventive wrist strap to your wrist and to a bare metal surface on the chassis.

Step 2 Disconnect the LC from the SFP module.

Tip For reattachment, note which cable connector plug is send (TX) and which is receive (RX).

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1037
3702
Doc

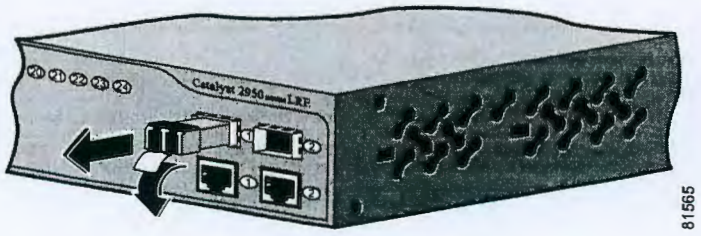
16.753
L

Step 3 Insert a dust plug into the optical ports of the SFP module to keep the optical interfaces clean.

Step 4 Unlock and remove the SFP module, as shown in Figure 2-32, Figure 2-33, and Figure 2-34.

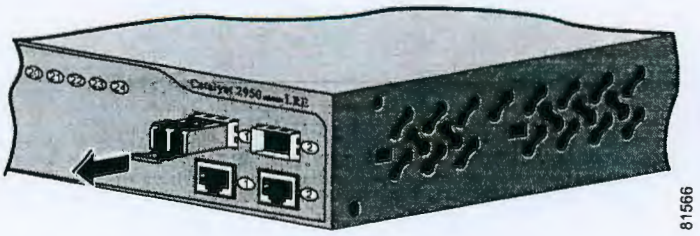
- If the module has a Mylar tab latch, pull the tab straight out so that you remove the SFP module from the port in a parallel direction. Do not twist or pull the tab because you could disconnect it from the SFP module.

Figure 2-32 Using the Mylar Tab Latch to Remove an SFP Module from a Slot



- If the module has an actuator button latch, use your thumb to push inward on the wedge to free the locking pin, and use your index finger to grip the ridge on top of the SFP module. Pull straight out to remove the module.

Figure 2-33 Using the Actuator Button Latch to Remove an SFP Module from an SFP Module Slot

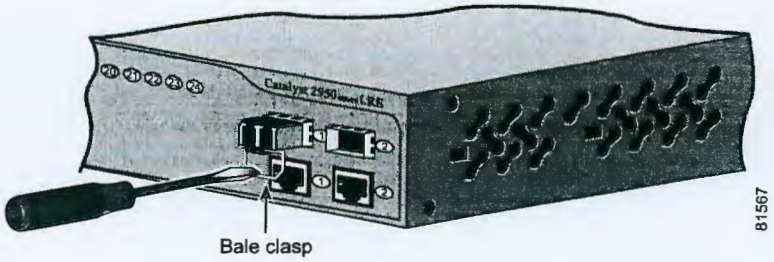


- If the module has a bale-clasp latch, pull the bale out and down to eject the module.If the bale-clasp latch is obstructed and you cannot use your index finger to open it, use a small, flat-blade screwdriver or other long, narrow instrument to open the bale-clasp latch.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1038
Doc: 3702

16.752
L

Figure 2-34 Removing a Bale-Clasp Latch SFP Module by Using a Flat-Blade Screwdriver



Step 5 Grasp the SFP module between your thumb and index finger, and carefully remove it from the module slot.

Step 6 Place the removed SFP module in an antistatic bag or other protective environment.

Connecting to 10/100 and 10/100/1000 Ports

The 10/100 ports configure themselves to operate at the speed and duplex settings of attached devices.They operate at 10 or 100 Mbps in half- or full-duplex mode. If the attached devices do not support autonegotiation, you can explicitly set the speed and duplex parameters.

The 10/100/1000 ports configure themselves to operate at the speed setting of attached devices.These ports on Catalyst 2950T-24 switches operate at 10, 100, or 1000 Mbps in full-duplex mode. If the attached devices do not support autonegotiation, you can set the speed.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1039
Doc: 3702

16 751
L

Note On the Catalyst 2950 LRE switches, the four input uplink ports are bundled as two logical ports, each consisting of a copper 10/100/1000 port and a fiber-optic small form-factor pluggable (SFP) module slot, respectively.

Within each logical port, you can use only the copper or the fiber-optic port at one time. If the Catalyst 2950 LRE switch senses more than two connections for both logical ports, the switch chooses the fiber-optic connections over the copper connections in default operation.

See the "SFP Module Slots" section on page 1-13 for more information on LRE uplink logical ports.

Connecting devices that do not autonegotiate or devices with manually set speed and duplex parameters can reduce performance or result in link failures between the devices. To maximize performance, choose one of these methods for configuring the ports:

- Let the ports autonegotiate both speed and duplex for 10/100 ports and only speed for 10/100/1000 ports.
- Set the speed and duplex parameters on both ends of the connection.

When connecting the ports on the Catalyst 2950G-24-EI-DC switches to other devices, follow these guidelines:

Caution To comply with the intrabuilding lightning surge requirements, intrabuilding wiring must be shielded, and the shield for the wiring must be grounded at both ends.

Caution The Catalyst 2950G-24-EI-DC switch is suitable only for intrabuilding or nonexposed wiring connections.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
1040
Fls. Nº
Doc: 3702

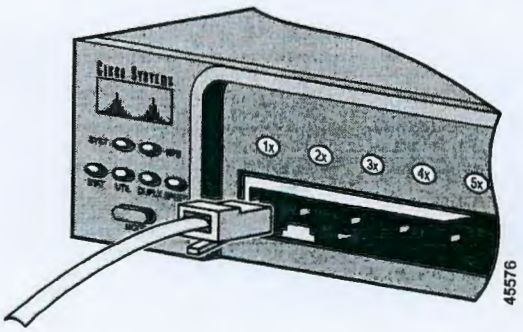
Follow these steps to connect the switch to 10BASE-T, 100BASE-TX, or 1000BASE-T devices:

Caution To prevent electrostatic-discharge (ESD) damage, follow your normal board and component handling procedures.

Step 1 When connecting to servers, workstations, and routers, insert a twisted-pair straight-through cable in a front-panel RJ-45 connector, as shown in Figure 2-35, Figure 2-36, and Figure 2-37. When connecting to switches or repeaters, insert a twisted-pair crossover cable. (See the "Cable and Adapter Specifications" section on page B-9 for cable-pinout descriptions.)

Note When connecting to 1000BASE-T devices, be sure to use a four twisted-pair, Category 5 cable.

Figure 2-35 Connecting to a Port on Catalyst 2950-12, 2950-24, 2950C-24, 2950SX-24, and 2950T-24 Switches



RQS nº 03/2005 - CN - CPMI - CORREIOS
1041
Fls Nº
3702
Doc:

16.749
2

Figure 2-36 Connecting to a Port on Catalyst 2950G-12-EI, 2950G-24-EI, and 2950G-24-EI-DC Switches

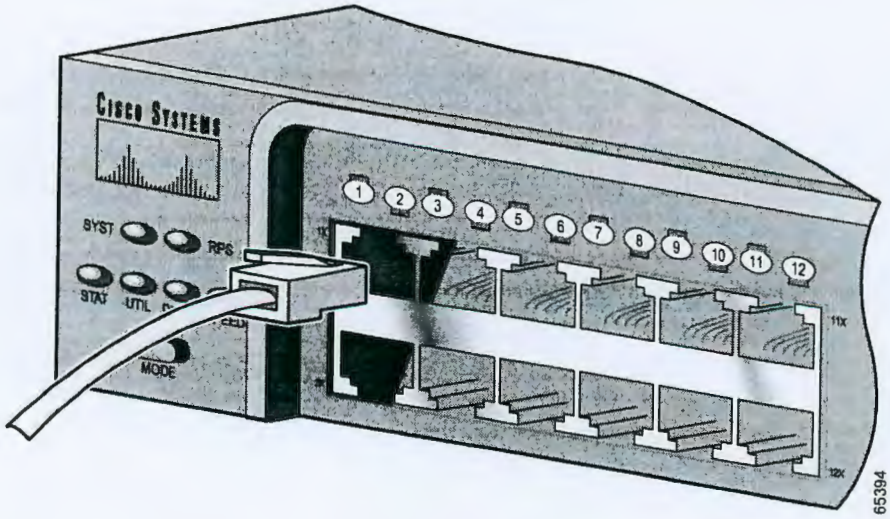
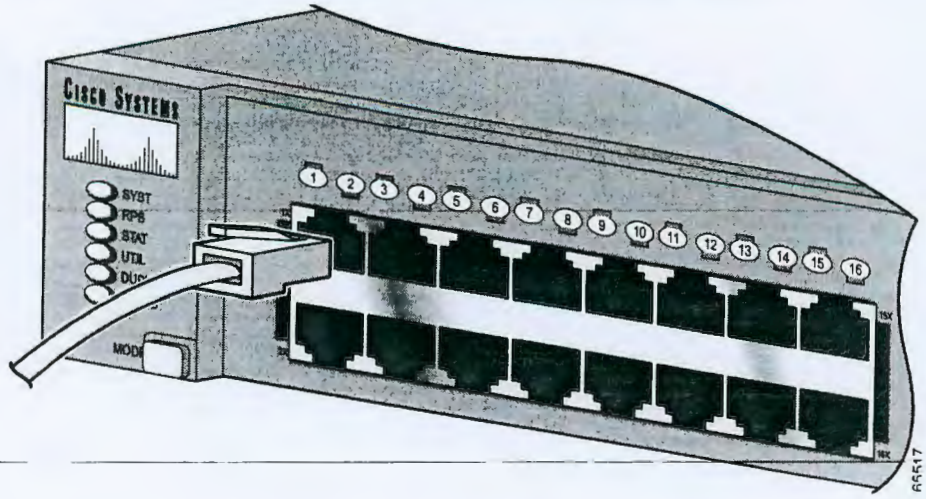


Figure 2-37 Connecting to a Port on Catalyst 2950G-48-EI Switches



Step 2 Insert the other cable end in an RJ-45 connector on the target device.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1042
3702
Doc:

16.718

Step 3 Observe the port status LED.

The LED turns green when the switch and the target device have an established link.

The LED turns amber while Spanning Tree Protocol (STP) discovers the network topology and searches for loops. This process takes about 30 seconds, and then the LED turns green.

If the LED is off, the target device might not be turned on, there might be a cable problem, or there might be a problem with the adapter installed in the target device. See Chapter 3, "Troubleshooting," for solutions to cabling problems.

Step 4 Reconfigure and restart the target device if necessary.

Step 5 Repeat Steps 1 through 4 to connect each port.

Connecting to 100BASE-FX and 1000BASE-SX Ports

The 100BASE-FX and 1000BASE-SX ports operate only in full-duplex mode.

You can connect a 100BASE-FX or 1000BASE-SX port to an SC or ST port on another device by using one of the MT-RJ fiber-optic patch cables listed in Table 2-1. Use the Cisco part numbers in Table 2-1 to order the patch cables that you need.

Caution Do not remove the dust plugs from the fiber-optic ports or the rubber caps from the fiber-optic cable until you are ready to connect the cable. The plugs and caps protect the fiber-optic ports and cables from contamination and ambient light.

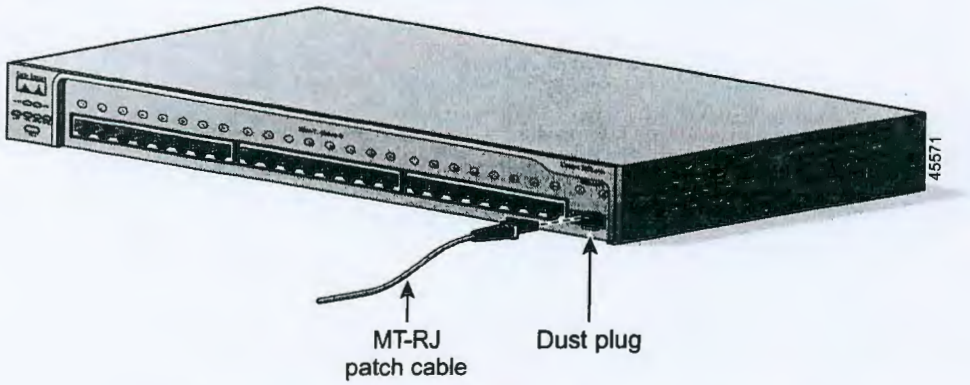
RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1043
3702
Doc:

Follow these steps to connect the switch to a 100BASE-FX or 1000BASE-SX device:

Step 1 Remove the dust plugs from the 100BASE-FX or 1000BASE-SX port and the rubber caps from the MT-RJ patch cable. Store them for future use.

Step 2 Insert the cable in a 100BASE-FX or 1000BASE-SX port. (See .)

Figure 2-38 Connecting to a 100BASE-FX or 1000BASE-SX Port



Step 3 Insert the other cable end in an SC or ST port on the target device.

Step 4 Observe the port status LED.

The LED turns green when the switch and the target device have an established link.

The LED turns amber while STP discovers the network topology and searches for loops. This process takes about 30 seconds, and then the port LED turns green.

If the LED is off, the target device might not be turned on, there might be a cable problem, or there might be a problem with the adapter installed in the target device. See Chapter 3, "Troubleshooting," for solutions to cabling problems.

Step 5 Reconfigure and restart the target device if necessary.

Step 6 Repeat Steps 1 through 5 to connect each port.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1044
Doc: 3702

16.740

Connecting to an LRE Port

Depending on the switch model, you can connect the LRE port to up to 8 or up to 24 LRE customer premises equipment (CPE) devices through a patch panel.

Note You can connect both Cisco 575 LRE CPE and Cisco 585 LRE CPE devices to your LRE switch, and you can hot swap the CPE devices without powering down the switch or disrupting the other switch ports.

If telephone services, such as voice or integrated services digital network (ISDN), use the same cabling as the LRE traffic, you must connect the LRE to a plain old telephone service (POTS) splitter. The splitter routes LRE data (high-frequency) and voice (low-frequency) traffic from the telephone line to the switch and private branch exchange (PBX) switch or PSTN.

If the other telephone services are connected through a PBX switch, you can use a Cisco LRE 48 POTS Splitter. The PBX routes voice traffic to private telephone networks and the PSTN. For more information about the Cisco LRE 48 POTS Splitter (PS-1M-LRE-48), refer to the *Installation Notes for the Cisco LRE 48 POTS Splitter*.

If the installation does not have a PBX, you need to use a homologated POTS splitter to connect to the PSTN. For more information about homologated POTS splitters, contact your Cisco sales representative.

Note If a connection to a telephone network is not required, you do not need a splitter, and you can connect the switch to the patch panel.

Note Cisco LRE products are designed to share lines with analog, ISDN, and digital PBX switch telephones that use the 0 to 700 kHz frequency range. Digital telephones connected to digital PBX switches that use frequencies above 700 kHz do not work when sharing a line with LRE signals. Due to the proprietary nature of digital PBX switches, some digital PBX switch services use frequencies above 700 kHz.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1045
Doc: 3702

Connecting the LRE port to a patch panel or a POTS splitter requires a male-to-male RJ-21 cable, Category 3 or above. You can order RJ-21 cables from your cable vendor, or you can order these cables from your Cisco sales representative:

- CAB-5-M120M120-5= (Category 5 cable with 90-degree, male-to-male RJ-21 connectors)
- CAB-5-M180M120-5= (Category 5 cable with 120-degree, male-to-male RJ-21 connectors)

The screws that you need to secure the cable to the switch are shipped with the cable. Contact your Cisco sales representative for more information.

To connect the LRE port to a patch panel or POTS splitter, follow these steps:

Step 1 Connect one end of a cable connected to the wiring trunk to the RJ-21 connector (the LRE port) on the switch. (See Figure 2-39.)

Step 2 Referring to Figure 2-39, secure the cable to the switch:

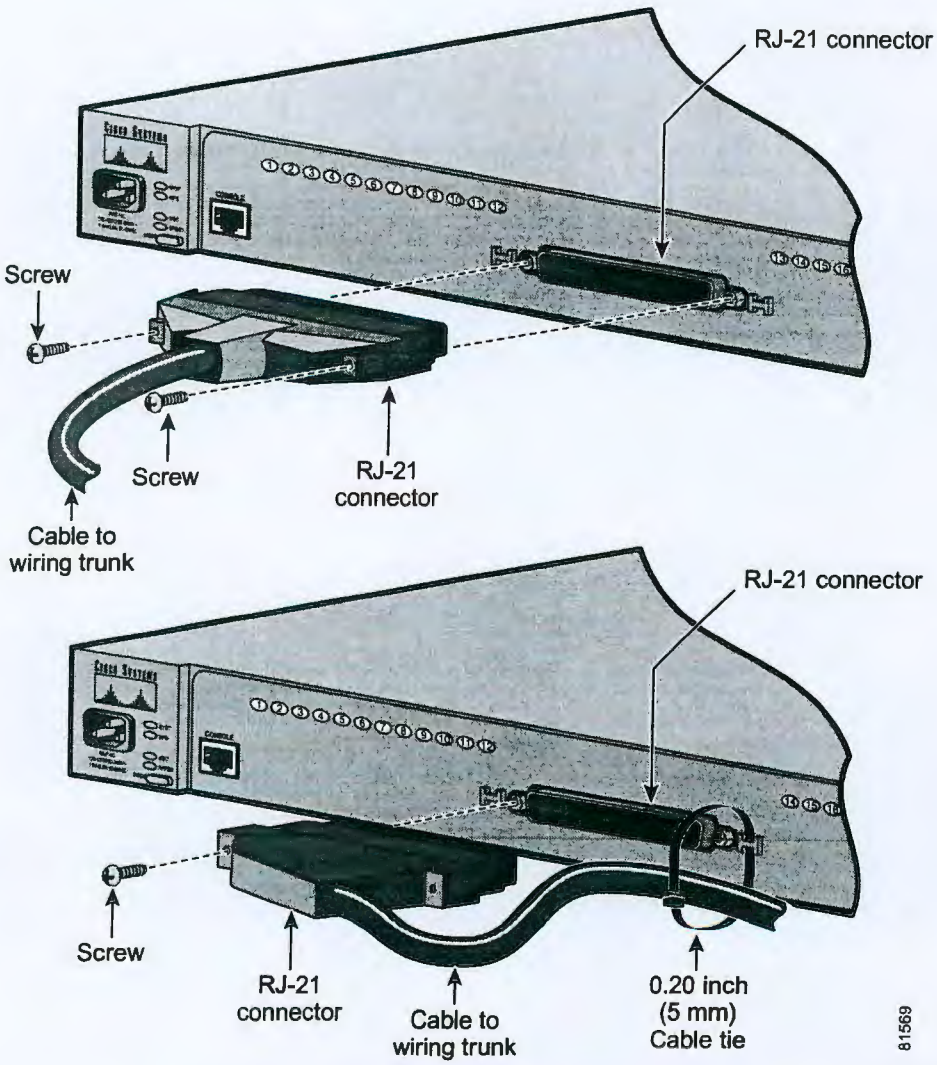
- For a 90-degree connector, see the top of .
- For a 12-degree connector, see the bottom of .

Note The cable tie is not included with the connector and cable assembly.

Step 3 Connect the other end of the cable to the patch panel or POTS splitter.

03/2005 - CN - CPMI - CORREIOS
Fls Nº 1046
Doc: 3702

Figure 2-39 Connecting to an LRE Port



Each LRE port status LED turns on when it establishes a link with a Cisco LRE CPE device. For more information about the LRE link between the switch LRE port and the CPE, as well as information about the configuration and management of CPE devices, refer to the switch software configuration guide.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1047
3702
Doc:

16.743

For more information about the Cisco LRE CPE devices, refer to the *Cisco LRE CPE Hardware Installation Guide.*

Connecting to GBIC Module Ports

These sections describe how to connect to a GBIC module port.

- Connecting to 1000BASE-X GBIC Module Ports, page 2-46
- Connecting to 1000BASE-T GBIC Module Ports, page 2-47
- Connecting to GigaStack GBIC Module Ports, page 2-49

For instructions about how to connect to the CWDM GBIC module ports, refer to the documentation that came with that GBIC module.

For detailed instructions about installing, removing, and connecting to the GBIC module (the 1000BASE-X module, the 1000BASE-T module, the CWDM GBIC module, or the GigaStack module), refer to the GBIC documentation.

When connecting the ports on the Catalyst 2950G-24-EI-DC switches to other devices, follow these guidelines:

Caution To comply with the intrabuilding lightning surge requirements, intrabuilding wiring must be shielded, and the shield for the wiring must be grounded at both ends.

Caution The Catalyst 2950G-24-EI-DC switch is suitable only for intrabuilding or nonexposed wiring connections.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1048
Doc: 3702

16.742

Connecting to 1000BASE-X GBIC Module Ports

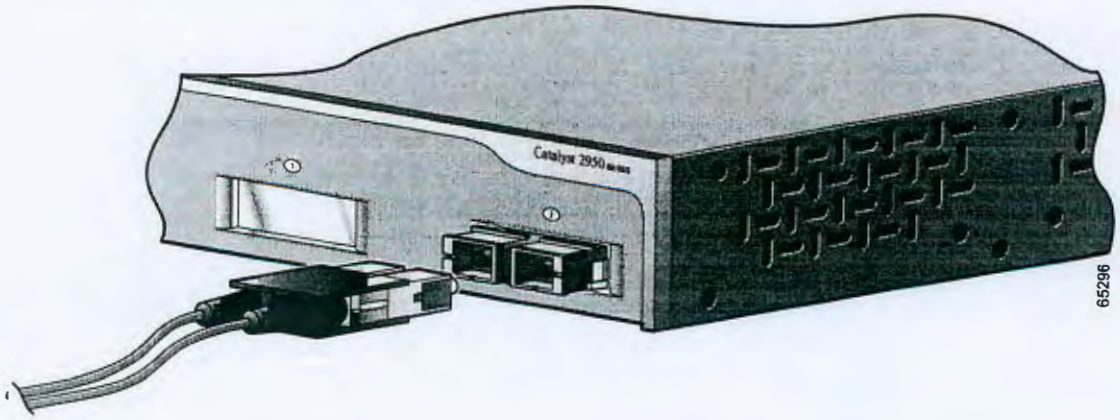
Caution Do not remove the rubber plugs from the GBIC module port or the rubber caps from the fiber-optic cable until you are ready to connect the cable. The plugs and caps protect the GBIC module ports and cables from contamination and ambient light.

After installing the 1000BASE-X GBIC in the GBIC module slot, follow these steps:

Step 1 Remove the rubber plugs from the GBIC module port, and store them for future use.

Step 2 Insert the SC connector in the fiber-optic receptacle (see Figure 2-40).

Figure 2-40 Connecting to a 1000 BASE-X GBIC Port



Step 3 Insert the other cable end in a fiber-optic receptacle on a target device.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1049
Nº Doc: 3702

Step 4 Observe the port status LED.

The LED turns green when the switch and the target device have an established link.

The LED turns amber while STP discovers the network topology and searches for loops. This process takes about 30 seconds, and then the port LED turns green.

If the LED is off, the target device might not be turned on, there might be a cable problem, or there might be problem with the adapter installed in the target device. See Chapter 3, "Troubleshooting," for solutions to cabling problems.

Step 5 Reconfigure and restart the switch or target device if necessary.

Connecting to 1000BASE-T GBIC Module Ports

After installing the 1000BASE-T GBIC in the GBIC module slot, follow these steps:

Caution To prevent ESD damage, follow your normal board and component handling procedures.

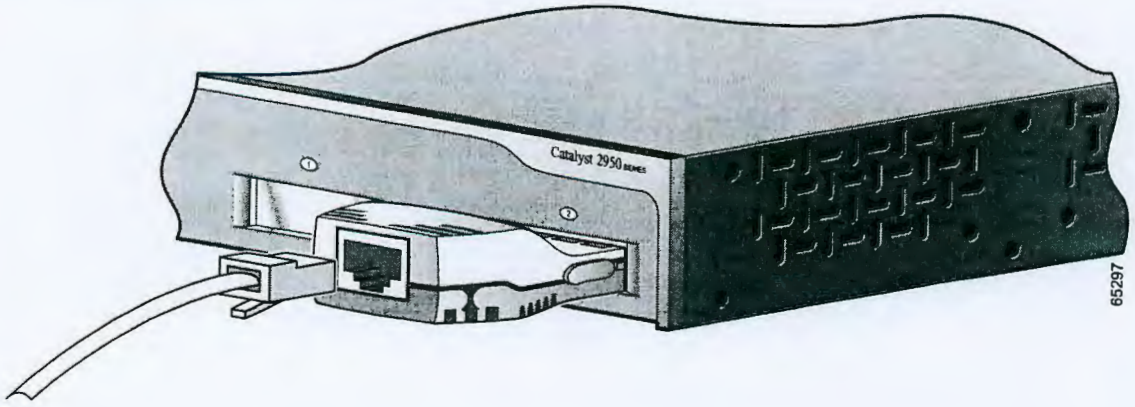
Step 1 When connecting to servers, workstations, and routers, insert a four twisted-pair, straight-through cable in the RJ-45 connector. When connecting to switches or repeaters, insert a four twisted-pair, crossover cable (see Figure 2-41).

Note When connecting to a 1000BASE-T device, be sure to use a four twisted-pair, Category 5 cable.

RQ 2-47 005 - CN - CPMI - CORREIOS
Fls Nº 1050
Doc: 3702

16 740

Figure 2-41 Connecting to a 1000BASE-T GBIC Port



Step 2 Insert the other cable end in an RJ-45 connector on a target device.

Step 3 Observe the port status LED.

The LED turns green when the switch and the target device have an established link.

The LED turns amber while STP discovers the network topology and searches for loops. This process takes about 30 seconds, and then the LED turns green.

If the LED is off, the target device might not be turned on, there might be a cable problem, or there might be a problem with the adapter installed in the target device. See Chapter 3, "Troubleshooting," for solutions to cabling problems.

Step 4 Reconfigure and restart the switch or target device, if necessary.

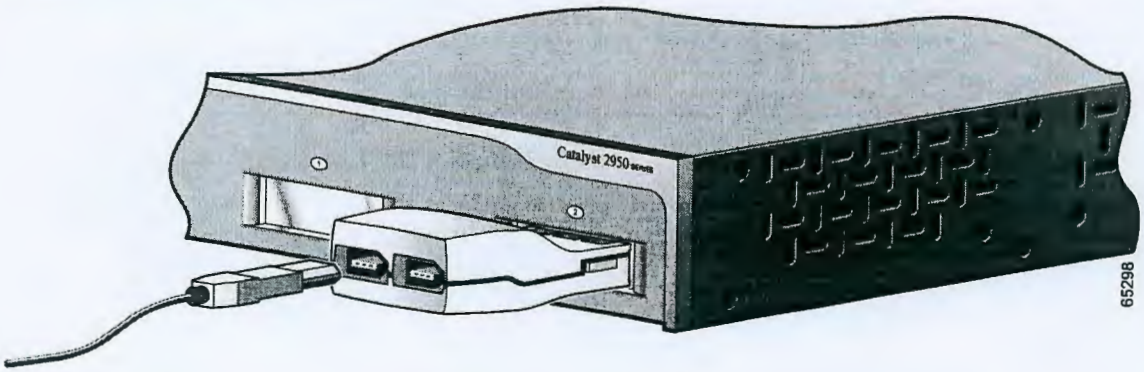
78-11187-04
RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1051
Doc: 3702

Connecting to GigaStack GBIC Module Ports

After installing the GigaStack GBIC in the GBIC module slot, follow these steps:

Step 1 Insert the GigaStack cable connector in the GBIC (see Figure 2-42).

Figure 2-42 Connecting to a GigaStack GBIC Port



Step 2 Insert the other cable end in a port on a target device.

Step 3 Observe the port status LED.

The LED turns green when the switch and the target device have an established link.

The LED turns amber while STP discovers the network topology and searches for loops. This process takes about 30 seconds, and then the port LED turns green.

If the LED is off, the target device might not be turned on, there might be a cable problem, or there might be a problem with the adapter installed in the target device. See Chapter 3, "Troubleshooting," for solutions to cabling problems.

Step 4 Reconfigure and restart the switch or target device, if necessary.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1052
3702

16.738

Connecting to an SFP Module

This section describes how to connect to an SFP module. For instructions about how to install or remove an SFP module, see the "Installing and Removing SFP Modules" section on page 2-32.

Caution Do not remove the rubber plugs from the SFP module port or the rubber caps from the fiber-optic cable until you are ready to connect the cable. The plugs and caps protect the SFP module ports and cables from contamination and ambient light.

Before connecting to an SFP module, be sure that you understand the port and cabling stipulations in Table 1-2 on page 1-15 and in the "SFP Module Slots" section on page 1-13. See **Appendix B, "Connectors and Cables"** for information about the LC on the SFP module.

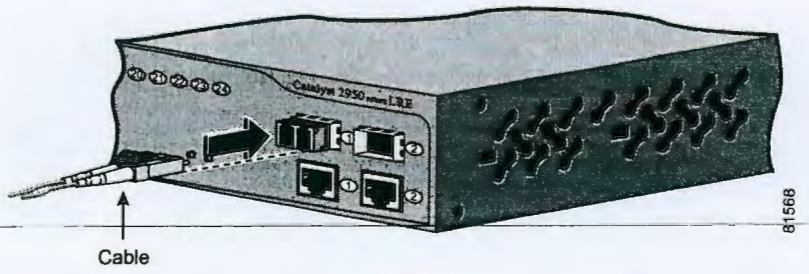
Note Refer to the Catalyst 2950 release notes for the list of supported SFP modules.

Follow these steps to connect a fiber-optic cable to an SFP module:

Step 1 Remove the rubber plugs from the module port and fiber-optic cable, and store them for future use.

Step 2 Insert one end of the fiber-optic cable into the SFP module port (see Figure 2-43).

Figure 2-43 Connecting to an SFP Module Port



Step 3 Insert the other cable end in a fiber-optic receptacle on a target device.

ECT 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1053
3702

16-737
L

Step 4 Observe the port status LED.

The LED turns green when the switch and the target device have an established link.

The LED turns amber while the STP discovers the network topology and searches for loops. This process takes about 30 seconds, and then the port LED turns green.

If the LED is off, the target device might not be turned on, there might be a cable problem, or there might be problem with the adapter installed in the target device. See Chapter 3, "Troubleshooting," for solutions to cabling problems.

Step 5 If necessary, reconfigure and restart the switch or target device.

Where to Go Next

For information about starting up the switch, refer to the release notes for the Catalyst 2950 switch.

For information about configuring the switch, refer to the switch software configuration guide.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1054
3702
Doc:

16.736

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1055
Doc: 3702

ANEXO (14D)

16.735

Configuring VLANs

This chapter describes how to configure normal-range VLANs (VLAN IDs 1 to 1005) and extended-range VLANs (VLAN IDs 1006 to 4094) on your Catalyst 2950 or Catalyst 2955 switch. It includes information about VLAN modes and the VLAN Membership Policy Server (VMPS).

Note For complete syntax and usage information for the commands used in this chapter, refer to the command reference for this release.

The chapter includes these sections:

- Understanding VLANs, page 15-1
- Configuring Normal-Range VLANs, page 15-4
- Configuring Extended-Range VLANs, page 15-12
- Displaying VLANs, page 15-14
- Configuring VLAN Trunks, page 15-15
- Configuring VMPS, page 15-25

Understanding VLANs

A VLAN is a switched network that is logically segmented by function, project team, or application, without regard to the physical locations of the users. VLANs have the same attributes as physical LANs, but you can group end stations even if they are not physically located on the same LAN segment. Any switch port can belong to a VLAN, and unicast, broadcast, and multicast packets are forwarded and flooded only to end stations in the VLAN. Each VLAN is considered a logical network, and packets destined for stations that do not belong to the VLAN must be forwarded through a router or bridge as shown in Figure 15-1. Because a VLAN is considered a separate logical network, it contains its own bridge Management Information Base (MIB) information and can support its own implementation of spanning tree. See Chapter 12, "Configuring STP" and Chapter 13, "Configuring RSTP and MSTP."

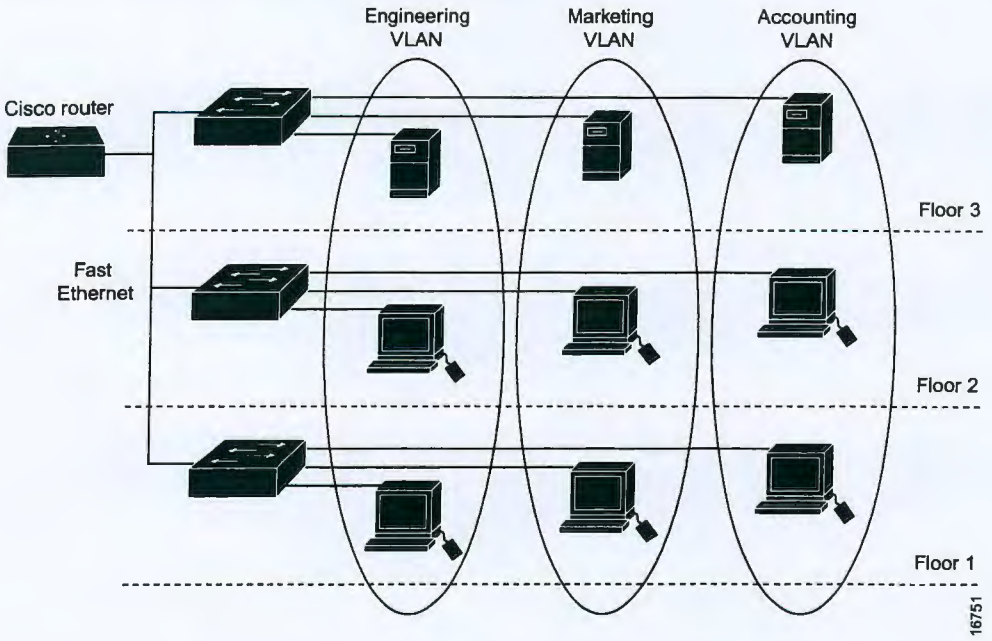
Note Before you create VLANs, you must decide whether to use VLAN Trunking Protocol (VTP) to maintain global VLAN configuration for your network. For more information on VTP, see Chapter 16, "Configuring VTP."

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1056
3702
Doc:

16.734
L

Figure 15-1 shows an example of VLANs segmented into logically defined networks.

Figure 15-1 VLANs as Logically Defined Networks



VLANs are often associated with IP subnetworks. For example, all the end stations in a particular IP subnet belong to the same VLAN. Interface VLAN membership on the switch is assigned manually on an interface-by-interface basis. When you assign switch interfaces to VLANs by using this method, it is known as interface-based, or static, VLAN membership.

Supported VLANs

Catalyst 2950 switches that run the standard software image (SI) support 64 VLANs; Catalyst 2950 and Catalyst 2955 switches that run the enhanced software image (EI) support 250 VLANs. Refer to the release notes for the list of switches that support each image. VLANs are identified with a number from 1 to 4094 when the EI is installed and 1 to 1005 when the SI is installed. VLAN IDs 1002 through 1005 are reserved for Token Ring and FDDI VLANs. VTP only learns normal-range VLANs, with VLAN IDs 1 to 1005; VLAN IDs greater than 1005 are extended-range VLANs and are not stored in the VLAN database. The switch must be in VTP transparent mode when you create VLAN IDs from 1006 to 4094.

The switch supports per-VLAN spanning tree (PVST) and per-VLAN rapid spanning tree (PVRST) with a maximum of 64 spanning-tree instances. One spanning-tree instance is allowed per VLAN. See the "Normal-Range VLAN Configuration Guidelines" section on page 15-5 for more information about the number of spanning-tree instances and the number of VLANs. The switch supports IEEE 802.1Q trunking for sending VLAN traffic over Ethernet ports.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1057
3702
Doc:

16.733
L

VLAN Port Membership Modes

You configure a port to belong to a VLAN by assigning a membership mode that determines the kind of traffic the port carries and the number of VLANs to which it can belong. Table 15-1 lists the membership modes and membership and VTP characteristics.

Table 15-1 Port Membership Modes

Membership Mode	VLAN Membership Characteristics	VTP Characteristics
Static-access	A static-access port can belong to one VLAN and is manually assigned to that VLAN. For more information, see the "Assigning Static-Access Ports to a VLAN" section on page 15-11.	VTP is not required. If you do not want VTP to globally propagate information, set the VTP mode to transparent to disable VTP. To participate in VTP, there must be at least one trunk port on the switch connected to a trunk port of a second switch.
802.1Q trunk	A trunk port is a member of all VLANs by default, including extended-range VLANs, but membership can be limited by configuring the allowed-VLAN list. You can also modify the pruning-eligible list to block flooded traffic to VLANs on trunk ports that are included in the list. For information about configuring trunk ports, see the "Configuring an Ethernet Interface as a Trunk Port" section on page 15-17.	VTP is recommended but not required. VTP maintains VLAN configuration consistency by managing the addition, deletion, and renaming of VLANs on a network-wide basis. VTP exchanges VLAN configuration messages with other switches over trunk links.
Dynamic access	A dynamic-access port can belong to one normal-range VLAN (VLAN ID 1 to 1005) and is dynamically assigned by a VMPS. The VMPS can be a Catalyst 5000 or Catalyst 6000 series switch, for example, but never a Catalyst 2950 or 2955 switch. You can have dynamic-access ports and trunk ports on the same switch, but you must connect the dynamic-access port to an end station and not to another switch. For configuration information, see the "Configuring Dynamic Access Ports on VMPS Clients" section on page 15-29.	VTP is required. Configure the VMPS and the client with the same VTP domain name. You can change the reconfirmation interval and retry count on the VMPS client switch.
Voice VLAN	A voice VLAN port is an access port attached to a Cisco IP Phone, configured to use one VLAN for voice traffic and another VLAN for data traffic from a device attached to the phone. For more information about voice VLAN ports, see Chapter 17, "Configuring Voice VLAN."	VTP is not required; it has no affect on voice VLAN.

For more detailed definitions of the modes and their functions, see Table 15-4 on page 15-16.

When a port belongs to a VLAN, the switch learns and manages the addresses associated with the port on a per-VLAN basis. For more information, see the "Managing the MAC Address Table" section on page 8-20.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1058
3702

16.732

Configuring Normal-Range VLANs

Normal-range VLANs are VLANs with VLAN IDs 1 to 1005. If the switch is in VTP server or transparent mode, you can add, modify or remove configurations for VLANs 2 to 1001 in the VLAN database. (VLAN IDs 1 and 1002 to 1005 are automatically created and cannot be removed.)

Note When the switch is in VTP transparent mode and the EI is installed, you can also create extended-range VLANs (VLANs with IDs from 1006 to 4094), but these VLANs are not saved in the VLAN database. See the "Configuring Extended-Range VLANs" section on page 15-12.

Configurations for VLAN IDs 1 to 1005 are written to the file *vlan.dat* (VLAN database), and you can display them by entering the **show vlan** privileged EXEC command. The *vlan.dat* file is stored in nonvolatile RAM (NVRAM).

Caution You can cause inconsistency in the VLAN database if you attempt to manually delete the *vlan.dat* file. If you want to modify the VLAN configuration, use the commands described in these sections and in the command reference for this release. To change the VTP configuration, see Chapter 16, "Configuring VTP."

You use the interface configuration mode to define the port membership mode and to add and remove ports from VLANs. The results of these commands are written to the running-configuration file, and you can display the file by entering the **show running-config** privileged EXEC command.

You can set these parameters when you create a new normal-range VLAN or modify an existing VLAN in the VLAN database:

- VLAN ID
- VLAN name
- VLAN type (Ethernet, Fiber Distributed Data Interface [FDDI], FDDI network entity title [NET], TrBRF, or TrCRF, Token Ring, Token Ring-Net)
- VLAN state (active or suspended)
- Maximum transmission unit (MTU) for the VLAN
- Security Association Identifier (SAID)
- Bridge identification number for TrBRF VLANs
- Ring number for FDDI and TrCRF VLANs
- Parent VLAN number for TrCRF VLANs
- Spanning Tree Protocol (STP) type for TrCRF VLANs
- VLAN number to use when translating from one VLAN type to another

Note This section does not provide configuration details for most of these parameters. For complete information on the commands and parameters that control VLAN configuration, refer to the command reference for this release.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1059
Nº Doc 3702

This section includes information about these topics about normal-range VLANs:

- Token Ring VLANs, page 15-5
- Normal-Range VLAN Configuration Guidelines, page 15-5
- VLAN Configuration Mode Options, page 15-6
- Saving VLAN Configuration, page 15-7
- Default Ethernet VLAN Configuration, page 15-7
- Creating or Modifying an Ethernet VLAN, page 15-8
- Deleting a VLAN, page 15-10
- Assigning Static-Access Ports to a VLAN, page 15-11

Token Ring VLANs

Although the switch does not support Token Ring connections, a remote device such as a Catalyst 5000 series switch with Token Ring connections could be managed from one of the supported switches. Switches running VTP version 2 advertise information about these Token Ring VLANs:

- Token Ring TrBRF VLANs
- Token Ring TrCRF VLANs

For more information on configuring Token Ring VLANs, refer to the *Catalyst 5000 Series Software Configuration Guide*.

Normal-Range VLAN Configuration Guidelines

Follow these guidelines when creating and modifying normal-range VLANs in your network:

- See Table 15-1 for the maximum number of supported VLANs per switch model. On a switch supporting 250 VLANs, if VTP reports that there are 250 active VLANs, four of the active VLANs (1002 to 1005) are reserved for Token Ring and FDDI.
- Normal-range VLANs are identified with a number between 1 and 1001. VLAN numbers 1002 through 1005 are reserved for Token Ring and FDDI VLANs.
- VLAN configuration for VLANs 1 to 1005 are always saved in the VLAN database. If VTP mode is transparent, VTP and VLAN configuration is also saved in the switch running configuration file.
- The switch also supports VLAN IDs 1006 through 4094 in VTP transparent mode (VTP disabled) when the EI is installed. These are extended-range VLANs and configuration options are limited. Extended-range VLANs are not saved in the VLAN database. See the "Configuring Extended-Range VLANs" section on page 15-12.
- Before you can create a VLAN, the switch must be in VTP server mode or VTP transparent mode. If the switch is a VTP server, you must define a VTP domain or VTP will not function.
- The switch does not support Token Ring or FDDI media. The switch does not forward FDDI, FDDI-Net, TrCRF, or TrBRF traffic, but it does propagate the VLAN configuration through VTP.
- The switch supports 64 spanning-tree instances. If a switch has more active VLANs than supported spanning-tree instances, spanning tree can be enabled on 64 VLANs and is disabled on the remaining VLANs. If you have already used all available spanning-tree instances on a switch, adding another VLAN anywhere in the VTP domain creates a VLAN on that switch that is not running spanning-tree. If you have the default allowed list on the trunk ports of that switch (which

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1060
Doc 3702

is to allow all VLANs), the new VLAN is carried on all trunk ports. Depending on the topology of the network, this could create a loop in the new VLAN that would not be broken, particularly if there are several adjacent switches that all have run out of spanning-tree instances. You can prevent this possibility by setting allowed lists on the trunk ports of switches that have used up their allocation of spanning-tree instances.

If the number of VLANs on the switch exceeds the number of supported spanning tree instances, we recommend that you configure the IEEE 802.1S Multiple STP (MSTP) on your switch to map multiple VLANs to a single STP instance. For more information about MSTP, see Chapter 13, "Configuring RSTP and MSTP."

VLAN Configuration Mode Options

You can configure normal-range VLANs (with VLAN IDs 1 to 1005) by using these two configuration modes:

- VLAN Configuration in config-vlan Mode, page 15-6

  You access config-vlan mode by entering the **vlan** *vlan-id* global configuration command.

- VLAN Configuration in VLAN Configuration Mode, page 15-6

  You access VLAN database configuration mode by entering the **vlan database** privileged EXEC command.

VLAN Configuration in config-vlan Mode

To access config-vlan mode, enter the **vlan** global configuration command with a VLAN ID. Enter a new VLAN ID to create a VLAN or with an existing VLAN ID to modify the VLAN. You can use the default VLAN configuration (Table 15-2) or enter multiple commands to configure the VLAN. For more information about commands available in this mode, refer to the **vlan** global configuration command description in the command reference for this release. When you have finished the configuration, you must exit config-vlan mode for the configuration to take effect. To display the VLAN configuration, enter the **show vlan** privileged EXEC command.

You must use this config-vlan mode when creating extended-range VLANs (VLAN IDs greater than 1005). See the "Configuring Extended-Range VLANs" section on page 15-12.

VLAN Configuration in VLAN Configuration Mode

To access VLAN configuration mode, enter the **vlan database** privileged EXEC command. Then enter the **vlan** command with a new VLAN ID to create a VLAN or with an existing VLAN ID to modify the VLAN. You can use the default VLAN configuration (Table 15-2) or enter multiple commands to configure the VLAN. For more information about keywords available in this mode, refer to the **vlan** VLAN configuration command description in the command reference for this release. When you have finished the configuration, you must enter **apply** or **exit** for the configuration to take effect. When you enter the **exit** command, it applies all commands and updates the VLAN database. VTP messages are sent to other switches in the VTP domain, and the privileged EXEC mode prompt appears.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1061
Doc 3702

16.729

Saving VLAN Configuration

The configurations of VLAN IDs 1 to 1005 are always saved in the VLAN database (vlan.dat file). If VTP mode is transparent, they are also saved in the switch running configuration file and you can enter the **copy running-config startup-config** privileged EXEC command to save the configuration in the startup configuration file. You can use the **show running-config vlan** privileged EXEC command to display the switch running configuration file. To display the VLAN configuration, enter the **show vlan** privileged EXEC command.

When you save VLAN and VTP information (including extended-range VLAN configuration information) in the startup configuration file and reboot the switch, the switch configuration is determined as follows:

- If the VTP mode is transparent in the startup configuration, and the VLAN database and the VTP domain name from the VLAN database matches that in the startup configuration file, the VLAN database is ignored (cleared), and the VTP and VLAN configurations in the startup configuration file are used. The VLAN database revision number remains unchanged in the VLAN database.
- If the VTP mode or domain name in the startup configuration does not match the VLAN database, the domain name and VTP mode and configuration for the first 1005 VLANs use the VLAN database information.
- If VTP mode is server, the domain name and VLAN configuration for the first 1005 VLANs use the VLAN database information
- If the switch is running IOS Release 12.1(9)EA1 or later and you use an older startup configuration file to boot up the switch, the configuration file does not contain VTP or VLAN information, and the switch uses the VLAN database configurations.
- If the switch is running an IOS release earlier than 12.1(9)EA1 and you use a startup configuration file from IOS Release 12.1(9)EA1 or later to boot up the switch, the image on the switch does not recognize the VLAN and VTP configurations in the startup configuration file, so the switch uses the VLAN database configuration.

Caution If the VLAN database configuration is used at startup and the startup configuration file contains extended-range VLAN configuration, this information is lost when the system boots up.

Default Ethernet VLAN Configuration

Table 15-2 shows the default configuration for Ethernet VLANs.

Note The switch supports Ethernet interfaces exclusively. Because FDDI and Token Ring VLANs are not locally supported, you only configure FDDI and Token Ring media-specific characteristics for VTP global advertisements to other switches.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1062
Nº 3702
Doc:

Table 15-2 Ethernet VLAN Defaults and Ranges

Parameter	Default	Range
VLAN ID	1	1 to 4094 when the EI is installed and 1 to 1005 when the SI is installed. **Note** Extended-range VLANs (VLAN IDs 1006 to 4094) are not saved in the VLAN database.
VLAN name	*VLANxxxx*, where *xxxx* represents four numeric digits (including leading zeros) equal to the VLAN ID number	No range
802.10 SAID	100001 (100000 plus the VLAN ID)	1–4294967294
MTU size	1500	1500–18190
Translational bridge 1	0	0–1005
Translational bridge 2	0	0–1005
VLAN state	active	active, suspend
Remote SPAN	disabled	enabled, disabled

Creating or Modifying an Ethernet VLAN

Each Ethernet VLAN in the VLAN database has a unique, 4-digit ID that can be a number from 1 to 1001. VLAN IDs 1002 to 1005 are reserved for Token Ring and FDDI VLANs. To create a normal-range VLAN to be added to the VLAN database, assign a number and name to the VLAN.

Note When the switch is in VTP transparent mode and the EI is installed, you can assign VLAN IDs greater than 1006, but they are not added to the VLAN database. See the "Configuring Extended-Range VLANs" section on page 15-12.

For the list of default parameters that are assigned when you add a VLAN, see the "Configuring Normal-Range VLANs" section on page 15-4.

Beginning in privileged EXEC mode, follow these steps to use config-vlan mode to create or modify an Ethernet VLAN:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**vlan** *vlan-id*	Enter a VLAN ID, and enter config-vlan mode. Enter a new VLAN ID to create a VLAN, or enter an existing VLAN ID to modify a VLAN. **Note** The available VLAN ID range for this command is 1 to 1005 when the SI is installed and 1 to 4094 when the EI is installed. For information about adding VLAN IDs greater than 1005 (extended-range VLANs), see the "Configuring Extended-Range VLANs" section on page 15-12.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1063
Doc 3702

16 727

	Command	Purpose
Step 3	**name** *vlan-name*	(Optional) Enter a name for the VLAN. If no name is entered for the VLAN, the default is to append the *vlan-id* with leading zeros to the word VLAN. For example, VLAN0004 is a default VLAN name for VLAN 4.
Step 4	**mtu** *mtu-size*	(Optional) Change the MTU size (or other VLAN characteristic).
Step 5	**remote-span**	(Optional) Configure the VLAN as the RSPAN VLAN for a remote SPAN session. For more information on remote SPAN, see Chapter 22, "Configuring SPAN and RSPAN."
Step 6	**end**	Return to privileged EXEC mode.
Step 7	**show vlan** {**name** *vlan-name* / **id** *vlan-id*}	Verify your entries.
Step 8	**copy running-config startup config**	(Optional) If the switch is in VTP transparent mode, the VLAN configuration is saved in the running configuration file as well as in the VLAN database. This saves the configuration in the switch startup configuration file.

To return the VLAN name to the default settings, use the **no vlan name**, **no vlan mtu**, or **no remote span** config-vlan commands.

This example shows how to use config-vlan mode to create Ethernet VLAN 20, name it *test20,* and add it to the VLAN database:

```
Switch# configure terminal
Switch(config)# vlan 20
Switch(config-vlan)# name test20
Switch(config-vlan)# end
```

Beginning in privileged EXEC mode, follow these steps to use VLAN configuration mode to create or modify an Ethernet VLAN:

	Command	Purpose
Step 1	**vlan database**	Enter VLAN database configuration mode.
Step 2	**vlan** *vlan-id* **name** *vlan-name*	Add an Ethernet VLAN by assigning a number to it. The range is 1 to 1001; do not enter leading zeros. If no name is entered for the VLAN, the default is to append the *vlan-id* with leading zeros to the word VLAN. For example, VLAN0004 is a default VLAN name for VLAN 4.
Step 3	**vlan** *vlan-id* **mtu** *mtu-size*	(Optional) To modify a VLAN, identify the VLAN and change a characteristic, such as the MTU size.
Step 4	**exit**	Update the VLAN database, propagate it throughout the administrative domain, and return to privileged EXEC mode.
Step 5	**show vlan** {**name** *vlan-name* / **id** *vlan-id*}	Verify your entries.
Step 6	**copy running-config startup config**	(Optional) If the switch is in VTP transparent mode, the VLAN configuration is saved in the running configuration file as well as in the VLAN database. This saves the configuration in the switch startup configuration file.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1064
Nº - 3702
Doc:

16.720
2

Note You cannot configure an RSPAN VLAN in VLAN database configuration mode.

To return the VLAN name to the default settings, use the **no vlan** *vlan-id* **name** or **no vlan** *vlan-id* **mtu** VLAN configuration command.

This example shows how to use VLAN database configuration mode to create Ethernet VLAN 20, name it *test20*, and add it to the VLAN database:

```
Switch# vlan database
Switch(vlan)# vlan 20 name test20
Switch(vlan)# exit
APPLY completed.
Exiting....
Switch#
```

eleting a VLAN

When you delete a VLAN from a switch that is in VTP server mode, the VLAN is removed from the VLAN database for all switches in the VTP domain. When you delete a VLAN from a switch that is in VTP transparent mode, the VLAN is deleted only on that specific switch.

You cannot delete the default VLANs for the different media types: Ethernet VLAN 1 and FDDI or Token Ring VLANs 1002 to 1005.

Caution When you delete a VLAN, any ports assigned to that VLAN become inactive. They remain associated with the VLAN (and thus inactive) until you assign them to a new VLAN.

Beginning in privileged EXEC mode, follow these steps to delete a VLAN on the switch by using global configuration mode:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**no vlan** *vlan-id*	Remove the VLAN by entering the VLAN ID.
p 3	**end**	Return to privileged EXEC mode.
Step 4	**show vlan brief**	Verify the VLAN removal.
Step 5	**copy running-config startup config**	(Optional) If the switch is in VTP transparent mode, the VLAN configuration is saved in the running configuration file as well as in the VLAN database. This saves the configuration in the switch startup configuration file.

To delete a VLAN when in VLAN database configuration mode, use the **vlan database** privileged EXEC command to enter VLAN database configuration mode and the **no vlan** *vlan-id* VLAN configuration command.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1065
Nº 3702
Doc:

16.725

Assigning Static-Access Ports to a VLAN

You can assign a static-access port to a VLAN without having VTP globally propagate VLAN configuration information by disabling VTP (VTP transparent mode). If you are assigning a port on a cluster member switch to a VLAN, first use the **rcommand** privileged EXEC command to log in to the member switch.

Note If you assign an interface to a VLAN that does not exist, the new VLAN is created. (See the "Creating or Modifying an Ethernet VLAN" section on page 15-8.)

Beginning in privileged EXEC mode, follow these steps to assign a port to a VLAN in the VLAN database:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode
Step 2	**interface** *interface-id*	Enter the interface to be added to the VLAN.
Step 3	**switchport mode access**	Define the VLAN membership mode for the port (Layer 2 access port).
Step 4	**switchport access vlan** *vlan-id*	Assign the port to a VLAN. Valid VLAN IDs are 1 to 4094.
Step 5	**end**	Return to privileged EXEC mode.
Step 6	**show running-config interface** *interface-id*	Verify the VLAN membership mode of the interface.
Step 7	**show interfaces** *interface-id* **switchport**	Verify your entries in the *Administrative Mode* and the *Access Mode VLAN* fields of the display.
Step 8	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To return an interface to its default configuration, use the **default interface** *interface-id* interface configuration command.

This example shows how to configure Fast Ethernet interface 0/1 as an access port in VLAN 2:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# interface fastethernet0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 2
Switch(config-if)# end
Switch#
```


RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1066
3702
Doc:

16.729
2

Configuring Extended-Range VLANs

When the switch is in VTP transparent mode (VTP disabled) and the EI is installed), you can create extended-range VLANs (in the range 1006 to 4094). Extended-range VLANs enable service providers to extend their infrastructure to a greater number of customers. The extended-range VLAN IDs are allowed for any switchport commands that allow VLAN IDs. You always use config-vlan mode (accessed by entering the **vlan** *vlan-id* global configuration command) to configure extended-range VLANs. The extended range is not supported in VLAN database configuration mode (accessed by entering the **vlan database** privileged EXEC command).

Extended-range VLAN configurations are not stored in the VLAN database, but because VTP mode is transparent, they are stored in the switch running configuration file, and you can save the configuration in the startup configuration file by using the **copy running-config startup-config** privileged EXEC command.

Note Although the switch supports 4094 VLAN IDs when the EI is installed, see the "Supported VLANs" section on page 15-2 for the actual number of VLANs supported.

This section includes this information about extended-range VLANs:

- Default VLAN Configuration, page 15-12
- Extended-Range VLAN Configuration Guidelines, page 15-12
- Creating an Extended-Range VLAN, page 15-13
- Displaying VLANs, page 15-14

Default VLAN Configuration

See Table 15-2 on page 15-8 for the default configuration for Ethernet VLANs. You can change only the MTU size on extended-range VLANs; all other characteristics must remain at the default state.

Extended-Range VLAN Configuration Guidelines

Follow these guidelines when creating extended-range VLANs:

- To add an extended-range VLAN, you must use the **vlan** *vlan-id* global configuration command and access config-vlan mode. You cannot add extended-range VLANs in VLAN database configuration mode (accessed by entering the **vlan database** privileged EXEC command).
- VLAN IDs in the extended range are not saved in the VLAN database and are not recognized by VTP.
- You cannot include extended-range VLANs in the pruning eligible range.
- The switch must be in VTP transparent mode when you create extended-range VLANs. If VTP mode is server or client, an error message is generated, and the extended-range VLAN is rejected.
- You can set the VTP mode to transparent in global configuration mode or in VLAN database configuration mode. See the "Disabling VTP (VTP Transparent Mode)" section on page 16-12. You should save this configuration to the startup configuration so that the switch will boot up in VTP transparent mode. Otherwise, you will lose extended-range VLAN configuration if the switch resets.

RQS nº 03/2005 - CN
CPMI - CORREIO
Fls Nº 1067
3702
Doc:

- VLANs in the extended range are not supported by VQP. They cannot be configured by VMPS.
- STP is enabled by default on extended-range VLANs, but you can disable it by using the **no spanning-tree vlan** *vlan-id* global configuration command. When the maximum number of spanning-tree instances (64) are on the switch, spanning tree is disabled on any newly created VLANs. If the number of VLANs on the switch exceeds the maximum number of spanning tree instances, we recommend that you configure the IEEE 802.1S Multiple STP (MSTP) on your switch to map multiple VLANs to a single STP instance. For more information about MSTP, see Chapter 13, "Configuring RSTP and MSTP."

Creating an Extended-Range VLAN

You create an extended-range VLAN in global configuration mode by entering the **vlan** global configuration command with a VLAN ID from 1006 to 4094. This command accesses the config-vlan mode. The extended-range VLAN has the default Ethernet VLAN characteristics (see Table 15-2) and the MTU size is the only parameter you can change. Refer to the description of the **vlan** global configuration command in the command reference for defaults of all parameters. If you enter an extended-range VLAN ID when the switch is not in VTP transparent mode, an error message is generated when you exit from config-vlan mode, and the extended-range VLAN is not created.

Extended-range VLANs are not saved in the VLAN database; they are saved in the switch running configuration file. You can save the extended-range VLAN configuration in the switch startup configuration file by using the **copy running-config startup-config** privileged EXEC command.

Note Before you create an extended-range VLAN, you can verify that the VLAN ID is not used internally by entering the **show vlan internal usage** privileged EXEC command. If the VLAN ID is used internally and you want to free it up, go to the"Displaying VLANs" section on page 15-14 before creating the extended-range VLAN.

Beginning in privileged EXEC mode, follow these steps to create an extended-range VLAN:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**vtp mode transparent**	Configure the switch for VTP transparent mode, disabling VTP.
Step 3	**vlan** *vlan-id*	Enter an extended-range VLAN ID and enter config-vlan mode. The range is 1006 to 4094.
Step 4	**mtu** *mtu-size*	(Optional) Modify the VLAN by changing the MTU size. **Note** Although all commands appear in the CLI help in config-vlan mode, only the **mtu** *mtu-size* command is supported for extended-range VLANs.
Step 5	**end**	Return to privileged EXEC mode.
Step 6	**show vlan id** *vlan-id*	Verify that the VLAN has been created.
Step 7	**copy running-config startup config**	Save your entries in the switch startup configuration file. To save extended-range VLAN configurations, you need to save the VTP transparent mode configuration and the extended-range VLAN configuration in the switch startup configuration file. Otherwise, if the switch resets, it will default to VTP server mode, and the extended-range VLAN IDs will not be saved.

16.423
RQS nº 03/2005 - CN - CPMI - CORREIOS
1068
Fls Nº
Doc: 3702

16.722

To delete an extended-range VLAN, use the **no vlan** *vlan-id* global configuration command.

The procedure for assigning static-access ports to an extended-range VLAN is the same as for normal-range VLANs. See the "Assigning Static-Access Ports to a VLAN" section on page 15-11.

This example shows how to create a new extended-range VLAN (when the EI is installed) with all default characteristics, enter config-vlan mode, and save the new VLAN in the switch startup configuration file:

```
Switch(config)# vtp mode transparent
Switch(config)# vlan 2000
Switch(config-vlan)# end
Switch# copy running-config startup config
```

Displaying VLANs

Use the **show vlan** privileged EXEC command to display a list of all VLANs on the switch, including extended-range VLANs. The display includes VLAN status, ports, and configuration information. To view normal-range VLANs in the VLAN database (1 to 1005,) use the **show** VLAN configuration command (accessed by entering the **vlan database** privileged EXEC command). For a list of the VLAN IDs on the switch, use the **show running-config vlan** privileged EXEC command, optionally entering a VLAN ID range.

Table 15-3 lists the commands for monitoring VLANs.

Table 15-3 VLAN Monitoring Commands

Command	Command Mode	Purpose
show	VLAN configuration	Display status of VLANs in the VLAN database.
show current [*vlan-id*]	VLAN configuration	Display status of all or the specified VLAN in the VLAN database.
show interfaces [**vlan** *vlan-id*]	Privileged EXEC	Display characteristics for all interfaces or for the specified VLAN configured on the switch.
show running-config vlan	Privileged EXEC	Display all or a range of VLANs on the switch.
show vlan [**id** *vlan-id*]	Privileged EXEC	Display parameters for all VLANs or the specified VLAN on the switch.

For more details about the show command options and explanations of output fields, refer to the command reference for this release.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1069
Doc 3702

16.720
L

To avoid this, you should configure interfaces connected to devices that do not support DTP to not forward DTP frames, that is, to turn off DTP.

- If you do not intend to trunk across those links, use the **switchport mode access** interface configuration command to disable trunking.
- To enable trunking to a device that does not support DTP, use the **switchport mode trunk** and **switchport nonegotiate** interface configuration commands to cause the interface to become a trunk but to not generate DTP frames.

Note On GigaStack GBICs, dynamic trunking is only supported when only one port of a GigaStack GBIC is being used. If trunking is required on a GigaStack GBIC where both ports are in use, use the **switchport mode trunk** and **switchport nonegotiate** interface configuration commands on both GBIC interfaces to cause the interfaces to become trunks.

e 15-4 Layer 2 Interface Modes

Mode	Function
switchport mode access	Puts the interface (access port) into permanent nontrunking mode and negotiates to convert the link into a nontrunk link. The interface becomes a nontrunk interface even if the neighboring interface is not a trunk interface.
switchport mode dynamic desirable	Makes the interface actively attempt to convert the link to a trunk link. The interface becomes a trunk interface if the neighboring interface is set to *trunk*, *desirable*, or *auto* mode. The default switch-port mode for all Ethernet interfaces is **dynamic desirable**.
switchport mode dynamic auto	Makes the interface able to convert the link to a trunk link. The interface becomes a trunk interface if the neighboring interface is set to *trunk* or *desirable* mode.
switchport mode trunk	Puts the interface into permanent trunking mode and negotiates to convert the link into a trunk link. The interface becomes a trunk interface even if the neighboring interface is not a trunk interface.
switchport nonegotiate	Prevents the interface from generating DTP frames. You can use this command only when the interface switchport mode is **access** or **trunk**. You must manually configure the neighboring interface as a trunk interface to establish a trunk link.

1Q Configuration Considerations

802.1Q trunks impose these limitations on the trunking strategy for a network:

- In a network of Cisco switches connected through 802.1Q trunks, the switches maintain one instance of spanning tree for each VLAN allowed on the trunks. Non-Cisco devices might support one spanning-tree instance for all VLANs.

  When you connect a Cisco switch to a non-Cisco device through an 802.1Q trunk, the Cisco switch combines the spanning-tree instance of the VLAN of the trunk with the spanning-tree instance of the non-Cisco 802.1Q switch. However, spanning-tree information for each VLAN is maintained by Cisco switches separated by a cloud of non-Cisco 802.1Q switches. The non-Cisco 802.1Q cloud separating the Cisco switches is treated as a single trunk link between the switches.

RQS nº 03/2005 - CN - CPMI - CORREIOS
78-11380-07
Fls Nº 1070
3702
Doc:

- Make sure the native VLAN for an 802.1Q trunk is the same on both ends of the trunk link. If the native VLAN on one end of the trunk is different from the native VLAN on the other end, spanning-tree loops might result.
- Disabling spanning tree on the native VLAN of an 802.1Q trunk without disabling spanning tree on every VLAN in the network can potentially cause spanning-tree loops. We recommend that you leave spanning tree enabled on the native VLAN of an 802.1Q trunk or disable spanning tree on every VLAN in the network. Make sure your network is loop-free before disabling spanning tree.

Default Layer 2 Ethernet Interface VLAN Configuration

Table 15-5 shows the default Layer 2 Ethernet interface VLAN configuration.

Table 15-5 Default Layer 2 Ethernet Interface VLAN Configuration

Feature	Default Setting
Interface mode	**switchport mode dynamic desirable**
Allowed VLAN range	VLANs 1 to 4094 when the EI is installed and 1 to 1005 when the SI is installed
VLAN range eligible for pruning	VLANs 2 to 1001
Default VLAN (for access ports)	VLAN 1
Native VLAN (for 802.1Q trunks)	VLAN 1

Configuring an Ethernet Interface as a Trunk Port

Because trunk ports send and receive VTP advertisements, to use VTP you must ensure that at least one trunk port is configured on the switch and that this trunk port is connected to the trunk port of a second switch. Otherwise, the switch cannot receive any VTP advertisements.

This section includes these procedures for configuring an Ethernet interface as a trunk port on the switch:

- Interaction with Other Features, page 15-18
- Defining the Allowed VLANs on a Trunk, page 15-19
- Changing the Pruning-Eligible List, page 15-20
- Configuring the Native VLAN for Untagged Traffic, page 15-21

Note The default mode for Layer 2 interfaces is **switchport mode dynamic desirable**. If the neighboring interface supports trunking and is configured to allow trunking, the link is a Layer 2 trunk.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1071
3702
Doc:

16:718

Interaction with Other Features

Trunking interacts with other features in these ways:

- A trunk port cannot be a secure port.
- Trunk ports can be grouped into EtherChannel port groups, but all trunks in the group must have the same configuration. When a group is first created, all ports follow the parameters set for the first port to be added to the group. If you change the configuration of one of these parameters, the switch propagates the setting you entered to all ports in the group:
  - allowed-VLAN list
  - STP port priority for each VLAN
  - STP Port Fast setting
  - trunk status: if one port in a port group ceases to be a trunk, all ports cease to be trunks.
- If you try to enable 802.1X on a trunk port, an error message appears, and 802.1X is not enabled. If you try to change the mode of an 802.1X-enabled port to trunk, the port mode is not changed.
- A port in dynamic mode can negotiate with its neighbor to become a trunk port. If you try to enable 802.1X on a dynamic port, an error message appears, and 802.1X is not enabled. If you try to change the mode of an 802.1X-enabled port to dynamic, the port mode is not changed.

Configuring a Trunk Port

Beginning in privileged EXEC mode, follow these steps to configure a port as 802.1Q trunk port:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Enter the interface configuration mode and the port to be configured for trunking.
Step 3	**switchport mode {dynamic {auto | desirable} | trunk}**	Configure the interface as a Layer 2 trunk (required only if the interface is a Layer 2 access port or to specify the trunking mode). • **dynamic auto**—Set the interface to a trunk link if the neighboring interface is set to trunk or desirable mode. • **dynamic desirable**—Set the interface to a trunk link if the neighboring interface is set to trunk, desirable, or auto mode. • **trunk**—Set the interface in permanent trunking mode and negotiate to convert the link to a trunk link even if the neighboring interface is not a trunk interface.
Step 4	**switchport access vlan** *vlan-id*	(Optional) Specify the default VLAN, which is used if the interface stops trunking.
Step 5	**switchport trunk native vlan** *vlan-id*	Specify the native VLAN.
Step 6	**end**	Return to privileged EXEC mode.
Step 7	**show interfaces** *interface-id* **switchport**	Display the switchport configuration of the interface in the *Administrative Mode* and the *Administrative Trunking Encapsulation* fields of the display.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1072
3702
Doc:

16.717
L.

	Command	Purpose
Step 8	**show interfaces** *interface-id* **trunk**	Display the trunk configuration of the interface.
Step 9	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To return an interface to its default configuration, use the **default interface** *interface-id* interface configuration command. To reset all trunking characteristics of a trunking interface to the defaults, use the **no switchport trunk** interface configuration command. To disable trunking, use the **switchport mode access** interface configuration command to configure the port as a static-access port.

This example shows how to configure the Fast Ethernet interface 0/4 as an 802.1Q trunk. The example assumes that the neighbor interface is configured to support 802.1Q trunking.

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# interface fastethernet0/4
Switch(config-if)# switchport mode dynamic desirable
Switch(config-if)# end
```

Defining the Allowed VLANs on a Trunk

By default, a trunk port sends traffic to and receives traffic from all VLANs. All VLAN IDs, 1 to 4094 when the EI is installed, and 1 to 1005 when the SI is installed, are allowed on each trunk. However, you can remove VLANs from the allowed list, preventing traffic from those VLANs from passing over the trunk. To restrict the traffic a trunk carries, use the **switchport trunk allowed vlan remove** *vlan-list* interface configuration command to remove specific VLANs from the allowed list.

Note You cannot remove VLAN 1 or VLANs 1002 to 1005 from the allowed VLAN list.

A trunk port can become a member of a VLAN if the VLAN is enabled, if VTP knows of the VLAN, and if the VLAN is in the allowed list for the port. When VTP detects a newly enabled VLAN and the VLAN is in the allowed list for a trunk port, the trunk port automatically becomes a member of the enabled VLAN. When VTP detects a new VLAN and the VLAN is not in the allowed list for a trunk port, the trunk port does not become a member of the new VLAN.

Beginning in privileged EXEC mode, follow these steps to modify the allowed list of an 802.1Q trunk:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Enter interface configuration mode and the port to be configured.
Step 3	**switchport mode trunk**	Configure the interface as a VLAN trunk port.
Step 4	**switchport trunk allowed vlan** {**add** | **all** | **except** | **remove**} *vlan-list*	(Optional) Configure the list of VLANs allowed on the trunk. For explanations about using the **add**, **all**, **except**, and **remove** keywords, refer to the command reference for this release. The *vlan-list* parameter is either a single VLAN number from 1 to 4094 or a range of VLANs described by two VLAN numbers, the lower one first, separated by a hyphen. Do not enter any spaces between comma-separated VLAN parameters or in hyphen-specified ranges. All VLANs are allowed by default. You cannot remove any of the default VLANs (1 or 1002 to 1005) from a trunk.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1073
Doc 702

	Command	Purpose
Step 5	**end**	Return to privileged EXEC mode.
Step 6	**show interfaces** *interface-id* **switchport**	Verify your entries in the *Trunking VLANs Enabled* field of the display.
Step 7	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To return to the default allowed VLAN list of all VLANs, use the **no switchport trunk allowed vlan** interface configuration command.

This example shows how to remove VLAN 2 from the allowed VLAN list:

```
Switch(config)# interface fastethernet0/1
Switch(config-if)# switchport trunk allowed vlan remove 2
Switch(config-if)# end
Switch#
```

Changing the Pruning-Eligible List

The pruning-eligible list applies only to trunk ports. Each trunk port has its own eligibility list. VTP pruning must be enabled for this procedure to take effect. The "Enabling VTP Pruning" section on page 16-14 describes how to enable VTP pruning.

Beginning in privileged EXEC mode, follow these steps to remove VLANs from the pruning-eligible list on a trunk port:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Enter interface configuration mode, and select the trunk port for which VLANs should be pruned.
Step 3	**switchport trunk pruning vlan {add | except | none | remove}** *vlan-list* [,*vlan*[,*vlan*[,,,]]	Configure the list of VLANs allowed to be pruned from the trunk. (See the "VTP Pruning" section on page 16-4). For explanations about using the **add**, **except**, **none**, and **remove** keywords, refer to the command reference for this release. Separate nonconsecutive VLAN IDs with a comma and no spaces; use a hyphen to designate a range of IDs. Valid IDs are from 2 to 1001. Extended-range VLANs (VLAN IDs 1006 to 4094) cannot be pruned. VLANs that are pruning-ineligible receive flooded traffic. The default list of VLANs allowed to be pruned contains VLANs 2 to 1001.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show interfaces** *interface-id* **switchport**	Verify your entries in the *Pruning VLANs Enabled* field of the display.
Step 6	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To return to the default pruning-eligible list of all VLANs, use the **no switchport trunk pruning vlan** interface configuration command.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1074
3702
Doc:

Configuring the Native VLAN for Untagged Traffic

A trunk port configured with 802.1Q tagging can receive both tagged and untagged traffic. By default, the switch forwards untagged traffic in the native VLAN configured for the port. The native VLAN is VLAN 1 by default.

Note The native VLAN can be assigned any VLAN ID; it is not dependent on the management VLAN.

For information about 802.1Q configuration issues, see the "802.1Q Configuration Considerations" section on page 15-16.

Beginning in privileged EXEC mode, follow these steps to configure the native VLAN on an 802.1Q trunk:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Enter interface configuration mode, and define the interface that is configured as the 802.1Q trunk.
Step 3	**switchport trunk native vlan** *vlan-id*	Configure the VLAN that is sending and receiving untagged traffic on the trunk port. For *vlan-id*, the range is 1 to 4094 when the EI is installed, and 1 to 1005 when the SI is installed.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show interfaces** *interface-id* **switchport**	Verify your entries in the *Trunking Native Mode VLAN* field.
Step 6	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To return to the default native VLAN, VLAN 1, use the **no switchport trunk native vlan** interface configuration command.

If a packet has a VLAN ID that is the same as the outgoing port native VLAN ID, the packet is sent untagged; otherwise, the switch sends the packet with a tag.

Load Sharing Using STP

Load sharing divides the bandwidth supplied by parallel trunks connecting switches. To avoid loops, STP normally blocks all but one parallel link between switches. Using load sharing, you divide the traffic between the links according to which VLAN the traffic belongs.

You configure load sharing on trunk ports by using STP port priorities or STP path costs. For load sharing using STP port priorities, both load-sharing links must be connected to the same switch. For load sharing using STP path costs, each load-sharing link can be connected to the same switch or to two different switches. For more information about STP, see Chapter 12, "Configuring STP."

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1075
3702
Doc:

Load Sharing Using STP Port Priorities

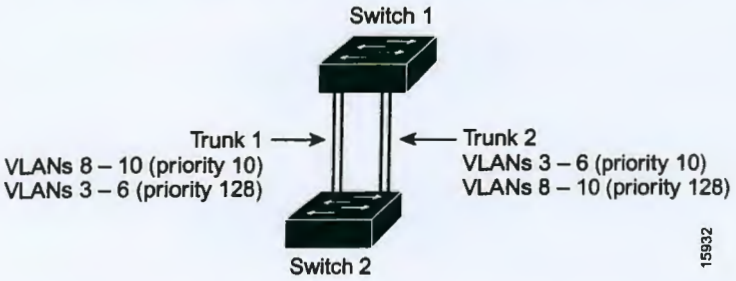
When two ports on the same switch form a loop, the STP port priority setting determines which port is enabled and which port is in a blocking state. You can set the priorities on a parallel trunk port so that the port carries all the traffic for a given VLAN. The trunk port with the higher priority (lower values) for a VLAN is forwarding traffic for that VLAN. The trunk port with the lower priority (higher values) for the same VLAN remains in a blocking state for that VLAN. One trunk port sends or receives all traffic for the VLAN.

Figure 15-3 shows two trunks connecting supported switches. In this example, the switches are configured as follows:

- VLANs 8 through 10 are assigned a port priority of 10 on Trunk 1.
- VLANs 3 through 6 retain the default port priority of 128 on Trunk 1.
- VLANs 3 through 6 are assigned a port priority of 10 on Trunk 2.
- VLANs 8 through 10 retain the default port priority of 128 on Trunk 2.

In this way, Trunk 1 carries traffic for VLANs 8 through 10, and Trunk 2 carries traffic for VLANs 3 through 6. If the active trunk fails, the trunk with the lower priority takes over and carries the traffic for all of the VLANs. No duplication of traffic occurs over any trunk port.

Figure 15-3 Load Sharing by Using STP Port Priorities



Beginning in privileged EXEC mode, follow these steps to configure the network shown in Figure 15-3.

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode on Switch 1.
Step 2	**vtp domain** *domain-name*	Configure a VTP administrative domain. The domain name can be from 1 to 32 characters.
Step 3	**vtp mode server**	Configure Switch 1 as the VTP server.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show vtp status**	Verify the VTP configuration on both Switch 1 and Switch 2. In the display, check the *VTP Operating Mode* and the *VTP Domain Name* fields.
Step 6	**show vlan**	Verify that the VLANs exist in the database on Switch 1.
Step 7	**configure terminal**	Enter global configuration mode.
Step 8	**interface fastethernet 0/1**	Enter interface configuration mode, and define Fast Ethernet port 0/1 as the interface to be configured as a trunk.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1076
Nº 3702
Doc:

	Command	Purpose
Step 9	**switchport mode trunk**	Configure the port as a trunk port.
Step 10	**end**	Return to privilege EXEC mode.
Step 11	**show interfaces fastethernet0/1 switchport**	Verify the VLAN configuration.
Step 12		Repeat Steps 7 through 11 on Switch 1 for Fast Ethernet port 0/2.
Step 13		Repeat Steps 7 through 11 on Switch 2 to configure the trunk ports on Fast Ethernet ports 0/1 and 0/2.
Step 14	**show vlan**	When the trunk links come up, VTP passes the VTP and VLAN information to Switch 2. Verify that Switch 2 has learned the VLAN configuration.
Step 15	**configure terminal**	Enter global configuration mode on Switch 1.
Step 16	**interface fastethernet0/1**	Enter interface configuration mode, and define the interface to set the STP port priority.
Step 17	**spanning-tree vlan 8 port-priority 10**	Assign the port priority of 10 for VLAN 8.
Step 18	**spanning-tree vlan 9 port-priority 10**	Assign the port priority of 10 for VLAN 9.
Step 19	**spanning-tree vlan 10 port-priority 10**	Assign the port priority of 10 for VLAN 10.
Step 20	**exit**	Return to global configuration mode.
Step 21	**interface fastethernet0/2**	Enter interface configuration mode, and define the interface to set the STP port priority.
Step 22	**spanning-tree vlan 3 port-priority 10**	Assign the port priority of 10 for VLAN 3.
Step 23	**spanning-tree vlan 4 port-priority 10**	Assign the port priority of 10 for VLAN 4.
Step 24	**spanning-tree vlan 5 port-priority 10**	Assign the port priority of 10 for VLAN 5.
Step 25	**spanning-tree vlan 6 port-priority 10**	Assign the port priority of 10 for VLAN 6.
Step 26	**end**	Return to privileged EXEC mode.
Step 27	**show running-config**	Verify your entries.
Step 28	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Load Sharing Using STP Path Cost

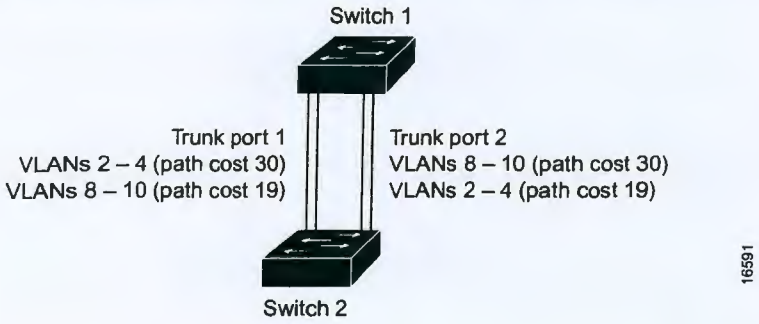
You can configure parallel trunks to share VLAN traffic by setting different path costs on a trunk and associating the path costs with different sets of VLANs. The VLANs keep the traffic separate. Because no loops exist, STP does not disable the ports, and redundancy is maintained in the event of a lost link.

In Figure 15-4, Trunk ports 1 and 2 are 100BASE-T ports. The path costs for the VLANs are assigned as follows:

- VLANs 2 through 4 are assigned a path cost of 30 on Trunk port 1.
- VLANs 8 through 10 retain the default 100BASE-T path cost on Trunk port 1 of 19.
- VLANs 8 through 10 are assigned a path cost of 30 on Trunk port 2.
- VLANs 2 through 4 retain the default 100BASE-T path cost on Trunk port 2 of 19.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 3702
Doc:

Figure 15-4 Load-Sharing Trunks with Traffic Distributed by Path Cost



Beginning in privileged EXEC mode, follow these steps to configure the network shown in Figure 15-4:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode on Switch 1.
Step 2	**interface fastethernet 0/1**	Enter interface configuration mode, and define Fast Ethernet port 0/1 as the interface to be configured as a trunk.
Step 3	**switchport mode trunk**	Configure the port as a trunk port.
Step 4	**exit**	Return to global configuration mode.
Step 5		Repeat Steps 2 through 4 on Switch 1 interface Fast Ethernet 0/2.
Step 6	**end**	Return to privileged EXEC mode.
Step 7	**show running-config**	Verify your entries. In the display, make sure that interfaces Fast Ethernet 0/1 and Fast Ethernet 0/2 are configured as trunk ports.
Step 8	**show vlan**	When the trunk links come up, Switch 1 receives the VTP information from the other switches. Verify that Switch 1 has learned the VLAN configuration.
Step 9	**configure terminal**	Enter global configuration mode.
Step 10	**interface fastethernet 0/1**	Enter interface configuration mode, and define Fast Ethernet port 0/1 as the interface to set the STP cost.
Step 11	**spanning-tree vlan 2 cost 30**	Set the spanning-tree path cost to 30 for VLAN 2.
Step 12	**spanning-tree vlan 3 cost 30**	Set the spanning-tree path cost to 30 for VLAN 3.
Step 13	**spanning-tree vlan 4 cost 30**	Set the spanning-tree path cost to 30 for VLAN 4.
Step 14	**end**	Return to global configuration mode.
Step 15		Repeat Steps 9 through 11 on Switch 1 interface Fast Ethernet 0/2, and set the spanning-tree path cost to 30 for VLANs 8, 9, and 10.
Step 16	**exit**	Return to privileged EXEC mode.
Step 17	**show running-config**	Verify your entries. In the display, verify that the path costs are set correctly for interfaces Fast Ethernet 0/1 and 0/2.
Step 18	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

RQS nº 03/2005 - CN - CPMI - CORREIOS
1078
Fls nº 11380-07
Doc: 3702

16.711

Configuring VMPS

The switch cannot be a VMPS server but can act as a client to the VMPS and communicate with it through the VLAN Query Protocol (VQP). VMPS dynamically assigns dynamic access port VLAN membership.

This section includes this information about configuring VMPS:

- "Understanding VMPS" section on page 15-25
- "Default VMPS Configuration" section on page 15-28
- "VMPS Configuration Guidelines" section on page 15-28
- "Configuring the VMPS Client" section on page 15-29
- "Monitoring the VMPS" section on page 15-31
- "Troubleshooting Dynamic Port VLAN Membership" section on page 15-32
- "VMPS Configuration Example" section on page 15-32

Understanding VMPS

When the VMPS receives a VQP request from a client switch, it searches its database for a MAC-address-to-VLAN mapping. The server response is based on this mapping and whether or not the server is in secure mode. Secure mode determines whether the server shuts down the port when a VLAN is not allowed on it or just denies the port access to the VLAN.

In response to a request, the VMPS takes one of these actions:

- If the assigned VLAN is restricted to a group of ports, the VMPS verifies the requesting port against this group and responds as follows:
  - If the VLAN is allowed on the port, the VMPS sends the VLAN name to the client in response.
  - If the VLAN is not allowed on the port and the VMPS is not in secure mode, the VMPS sends an *access-denied* response.
  - If the VLAN is not allowed on the port and the VMPS is in secure mode, the VMPS sends a *port-shutdown* response.
- If the VLAN in the database does not match the current VLAN on the port and active hosts exist on the port, the VMPS sends an *access-denied* or a *port-shutdown* response, depending on the secure mode of the VMPS.

If the switch receives an *access-denied* response from the VMPS, it continues to block traffic from the MAC address to or from the port. The switch continues to monitor the packets directed to the port and sends a query to the VMPS when it identifies a new address. If the switch receives a *port-shutdown* response from the VMPS, it disables the port. The port must be manually re-enabled by using the CLI, CMS, or SNMP.

You can also use an explicit entry in the configuration table to deny access to specific MAC addresses for security reasons. If you enter the **none** keyword for the VLAN name, the VMPS sends an *access-denied* or *port-shutdown* response, depending on the VMPS secure mode setting.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1079
Fls Nº 3702
Doc:

16710

Dynamic Port VLAN Membership

A dynamic (nontrunking) port on the switch can belong to only one VLAN, with a VLAN ID from 1 to 1005. When the link comes up, the switch does not forward traffic to or from this port until the VMPS provides the VLAN assignment. The VMPS receives the source MAC address from the first packet of a new host connected to the dynamic port and attempts to match the MAC address to a VLAN in the VMPS database.

If there is a match, the VMPS sends the VLAN number for that port. If the client switch was not previously configured, it uses the domain name from the first VTP packet it receives on its trunk port from the VMPS. If the client switch was previously configured, it includes its domain name in the query packet to the VMPS to obtain its VLAN number. The VMPS verifies that the domain name in the packet matches its own domain name before accepting the request and responds to the client with the assigned VLAN number for the client. If there is no match, the VMPS either denies the request or shuts down the port (depending on the VMPS secure mode setting).

Multiple hosts (MAC addresses) can be active on a dynamic port if they are all in the same VLAN; however, the VMPS shuts down a dynamic port if more than 20 hosts are active on the port.

If the link goes down on a dynamic port, the port returns to an isolated state and does not belong to a VLAN. Any hosts that come online through the port are checked again through the VQP with the VMPS before the port is assigned to a VLAN.

VMPS Database Configuration File

The VMPS contains a database configuration file that you create. This ASCII text file is stored on a switch-accessible TFTP server that functions as a server for VMPS. The file contains VMPS information, such as the domain name, the fallback VLAN name, and the MAC-address-to-VLAN mapping. The switch cannot act as the VMPS, but you can use a Catalyst 5000 or Catalyst 6000 series switch as the VMPS.

You can configure a fallback VLAN name. If you connect a device with a MAC address that is not in the database, the VMPS sends the fallback VLAN name to the client. If you do not configure a fallback VLAN and the MAC address does not exist in the database, the VMPS sends an *access-denied* response. If the VMPS is in secure mode, it sends a *port-shutdown* response.

Whenever port names are used in the VMPS database configuration file, the server must use the switch convention for naming ports. For example, Fa0/4 is fixed Fast Ethernet port number 4. If the switch is a cluster member, the command switch adds the name of the switch before the type. For example, *es3%Fa0/4* refers to fixed Fast Ethernet port 4 on member switch 3. When port names are required, these naming conventions must be followed in the VMPS database configuration file when it is configured to support a cluster.

This example shows a example of a VMPS database configuration file as it appears on a Catalyst 6000 series switch. The file has these characteristics:

- The security mode is open.
- The default is used for the fallback VLAN.
- MAC address-to-VLAN name mappings—The MAC address of each host and the VLAN to which each host belongs is defined.
- Port groups are defined.
- VLAN groups are defined.
- VLAN port policies are defined for the ports associated with restricted VLANs.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1080
Doc: 3702

```
!VMPS File Format, version 1.1
! Always begin the configuration file with
! the word "VMPS"
!
!vmps domain <domain-name>
! The VMPS domain must be defined.
!vmps mode {open | secure}
! The default mode is open.
!vmps fallback <vlan-name>
!vmps no-domain-req { allow | deny }
!
! The default value is allow.
vmps domain DSBU
vmps mode open
vmps fallback default
vmps no-domain-req deny
!
!
!MAC Addresses
!
vmps-mac-addrs
!
! address <addr> vlan-name <vlan_name>
!
address 0012.2233.4455 vlan-name hardware
address 0000.6509.a080 vlan-name hardware
address aabb.ccdd.eeff vlan-name Green
address 1223.5678.9abc vlan-name ExecStaff
address fedc.ba98.7654 vlan-name --NONE--
address fedc.ba23.1245 vlan-name Purple
!
!Port Groups
!
!vmps-port-group <group-name>
! device <device-id> { port <port-name> | all-ports }
!
vmps-port-group WiringCloset1
 device 198.92.30.32 port 0/2
 device 172.20.26.141 port 0/8
vmps-port-group "Executive Row"
 device 198.4.254.222 port 0/2
 device 198.4.254.222 port 0/3
 device 198.4.254.223 all-ports
!
!
!VLAN groups
!
!vmps-vlan-group <group-name>
! vlan-name <vlan-name>
!
vmps-vlan-group Engineering
vlan-name hardware
vlan-name software
!
!
!VLAN port Policies
!
!vmps-port-policies {vlan-name <vlan_name> | vlan-group <group-name> }
! { port-group <group-name> | device <device-id> port <port-name> }
!
vmps-port-policies vlan-group Engineering
 port-group WiringCloset1
```


RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1081
3702

16 708

```
vmps-port-policies vlan-name Green
 device 198.92.30.32 port 0/8
vmps-port-policies vlan-name Purple
 device 198.4.254.22 port 0/2
 port-group "Executive Row"
```

Default VMPS Configuration

Table 15-6 shows the default VMPS and dynamic port configuration on client switches.

Table 15-6 Default VMPS Client and Dynamic Port Configuration

Feature	Default Setting
VMPS domain server	None
VMPS reconfirm interval	60 minutes
VMPS server retry count	3
Dynamic ports	None configured

VMPS Configuration Guidelines

These guidelines and restrictions apply to dynamic access port VLAN membership:

- You should configure the VMPS before you configure ports as dynamic.
- The communication between a cluster of switches and VMPS is managed by the command switch and includes port-naming conventions that are different from standard port names. For the cluster-based port-naming conventions, see the "VMPS Database Configuration File" section on page 15-26.
- When you configure a port as a dynamic access port, the spanning-tree Port Fast feature is automatically enabled for that port. The Port Fast mode accelerates the process of bringing the port into the forwarding state.
- 802.1X ports cannot be configured as dynamic access ports. If you try to enable 802.1X on a dynamic-access (VQP) port, an error message appears, and 802.1X is not enabled. If you try to change an 802.1X-enabled port to dynamic VLAN assignment, an error message appears, and the VLAN configuration is not changed.
- Trunk ports cannot be dynamic access ports, but you can enter the **switchport access vlan dynamic** interface configuration command for a trunk port. In this case, the switch retains the setting and applies it if the port is later configured as an access port.

  You must turn off trunking on the port before the dynamic access setting takes effect.
- Dynamic access ports cannot be network ports or monitor ports.
- Secure ports cannot be dynamic access ports. You must disable port security on a port before it becomes dynamic.
- Dynamic access ports cannot be members of an EtherChannel group.
- Port channels cannot be configured as dynamic access ports.
- The VTP management domain of the VMPS client and the VMPS server must be the same.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1082
Doc: 3702

16.707
L

- VQP does not support extended-range VLANs (VLAN IDs higher than 1006). Extended-range VLANs cannot be configured by VMPS.
- The VLAN configured on the VMPS server should not be a voice VLAN.

Configuring the VMPS Client

You configure dynamic VLANs by using the VMPS (server). The switch can be a VMPS client; it cannot be a VMPS server.

Entering the IP Address of the VMPS

You must first enter the IP address of the server to configure the switch as a client.

Note If the VMPS is being defined for a cluster of switches, enter the address on the command switch.

Beginning in privileged EXEC mode, follow these steps to enter the IP address of the VMPS:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**vmps server** *ipaddress* **primary**	Enter the IP address of the switch acting as the primary VMPS server.
Step 3	**vmps server** *ipaddress*	Enter the IP address of the switch acting as a secondary VMPS server. You can enter up to three secondary server addresses.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show vmps**	Verify your entries in the *VMPS Domain Server* field of the display.
Step 6	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Note The switch port that is connected to the VMPS server cannot be a dynamic access port. It can be either a static access port or a trunk port. See the "Configuring an Ethernet Interface as a Trunk Port" section on page 15-17.

Configuring Dynamic Access Ports on VMPS Clients

If you are configuring a port on a cluster member switch as a dynamic port, first use the **rcommand** privileged EXEC command to log into the member switch.

Caution Dynamic port VLAN membership is for end stations or hubs connected to end stations. Connecting dynamic access ports to other switches can cause a loss of connectivity.

RQS nº 03/2005 - CN - CPMI - CORREIOS
1083
Fls Nº 15-29
Nº 3702
Doc:

Beginning in privileged EXEC mode, follow these steps to configure a dynamic access port on a VMPS client switch:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Enter interface configuration mode and the switch port that is connected to the end station.
Step 3	**switchport mode access**	Set the port to access mode.
Step 4	**switchport access vlan dynamic**	Configure the port as eligible for dynamic VLAN membership. The dynamic access port must be connected to an end station.
Step 5	**end**	Return to privileged EXEC mode.
Step 6	**show interfaces** *interface-id* **switchport**	Verify your entries in the *Operational Mode* field of the display.
Step 7	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To return an interface to its default configuration, use the **default interface** *interface-id* interface configuration command. To return an interface to its default switchport mode (dynamic desirable), use the **no switchport mode** interface configuration command. To reset the access mode to the default VLAN for the switch, use the **no switchport access** interface configuration command.

Note When you configure a dynamic access port by using the **switchport access vlan dynamic** interface configuration command, the port might allow unauthorized users to access network resources if the interface changes from access mode to trunk mode through the DTP negotiation. The workaround is to configure the port as a static access port.

Reconfirming VLAN Memberships

Beginning in privileged EXEC mode, follow these steps to confirm the dynamic port VLAN membership assignments that the switch has received from the VMPS:

	Command	Purpose
Step 1	**vmps reconfirm**	Reconfirm dynamic port VLAN membership.
Step 2	**show vmps**	Verify the dynamic VLAN reconfirmation status.

Changing the Reconfirmation Interval

VMPS clients periodically reconfirm the VLAN membership information received from the VMPS. You can set the number of minutes after which reconfirmation occurs.

If you are configuring a member switch in a cluster, this parameter must be equal to or greater than the reconfirmation setting on the command switch. You must also first use the **rcommand** privileged EXEC command to log into the member switch.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1084
Doc: 3702

Beginning in privileged EXEC mode, follow these steps to change the reconfirmation interval:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**vmps reconfirm** *minutes*	Enter the number of minutes between reconfirmations of the dynamic VLAN membership. Enter a number from 1 to 120. The default is 60 minutes.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show vmps**	Verify the dynamic VLAN reconfirmation status in the *Reconfirm Interval* field of the display.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To return the switch to its default setting, use the **no vmps reconfirm** global configuration command.

Changing the Retry Count

Beginning in privileged EXEC mode, follow these steps to change the number of times that the switch attempts to contact the VMPS before querying the next server:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**vmps retry** *count*	Change the retry count. The retry range is from 1 to 10; the default is 3.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show vmps**	Verify your entry in the *Server Retry Count* field of the display.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To return the switch to its default setting, use the **no vmps retry** global configuration command.

Monitoring the VMPS

You can display information about the VMPS by using the **show vmps** privileged EXEC command. The switch displays this information about the VMPS:

VMPS VQP Version — The version of VQP used to communicate with the VMPS. The switch queries the VMPS that is using VQP version 1.

Reconfirm Interval — The number of minutes the switch waits before reconfirming the VLAN-to-MAC-address assignments.

Server Retry Count — The number of times VQP resends a query to the VMPS. If no response is received after this many tries, the switch starts to query the secondary VMPS.

RQS nº 03/2005 - CN - CPMI - CORREIOS
1085
Fls Nº 15-31
3702

VMPS domain server	The IP address of the configured VLAN membership policy servers. The switch sends queries to the one marked *current*. The one marked *primary* is the primary server.
VMPS Action	The result of the most recent reconfirmation attempt. A reconfirmation attempt can occur automatically when the reconfirmation interval expired, or you can force it by entering the **vmps reconfirm** privileged EXEC command or its CMS or SNMP equivalent.

This is an example of output for the **show vmps** privileged EXEC command:

```
Switch# show vmps

VQP Client Status:
--------------------
VMPS VQP Version:   1
Reconfirm Interval: 60 min
Server Retry Count: 3
VMPS domain server: 172.20.128.86 (primary, current)
                    172.20.128.87

Reconfirmation status
---------------------
VMPS Action:         No Dynamic Port
```

Troubleshooting Dynamic Port VLAN Membership

The VMPS shuts down a dynamic port under these conditions:

- The VMPS is in secure mode, and it does not allow the host to connect to the port. The VMPS shuts down the port to prevent the host from connecting to the network.
- More than 20 active hosts reside on a dynamic port.

To re-enable a disabled dynamic port, enter the **no shutdown** interface configuration command.

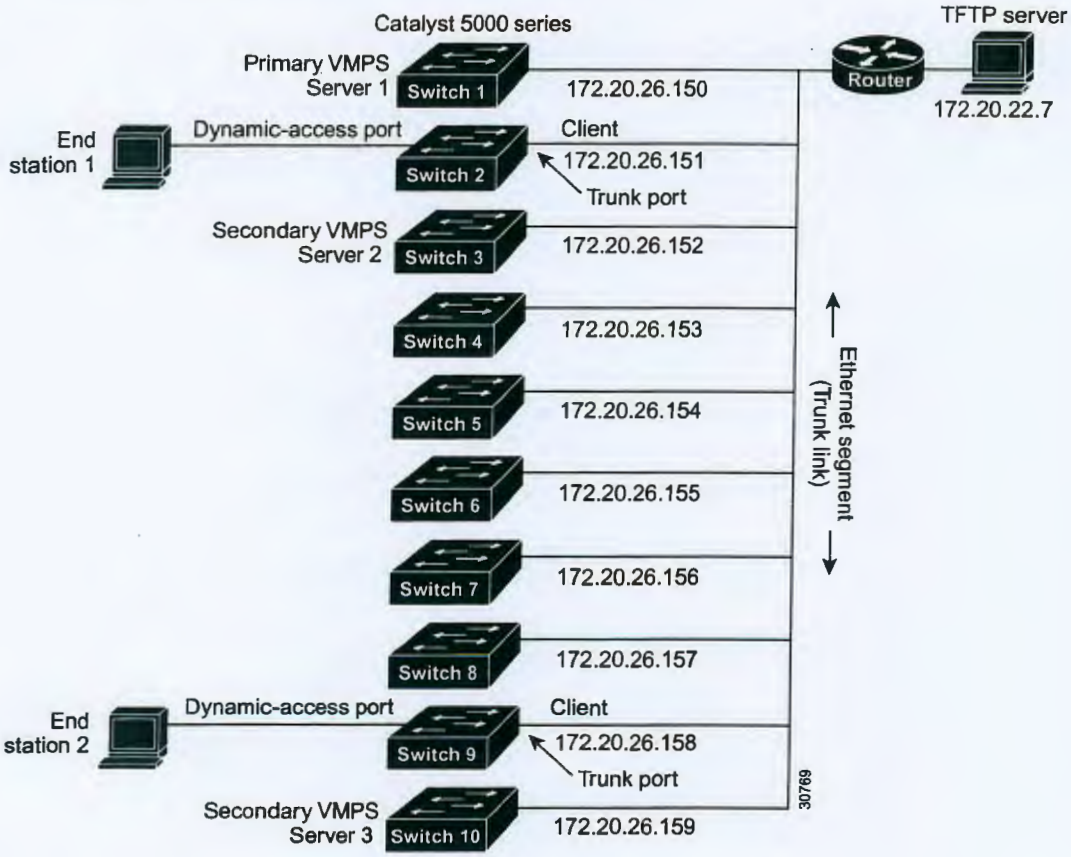
VMPS Configuration Example

Figure 15-5 shows a network with a VMPS server switch and VMPS client switches with dynamic ports. In this example, these assumptions apply:

- The VMPS server and the VMPS client are separate switches.
- The Catalyst 5000 series Switch 1 is the primary VMPS server.
- The Catalyst 5000 series Switch 3 and Switch 10 are secondary VMPS servers.
- The end stations are connected to these clients:
  - Catalyst 2950 Switch 2
  - Catalyst 3500 XL Switch 9
- The database configuration file is stored on the TFTP server with the IP address 172.20.22.7.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1086
3702

Figure 15-5 Dynamic Port VLAN Membership Configuration



RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1088
Doc: 3702

16.701

TECHNOLOGIES
LAN SWITCHING
PROTOCOL GROUPS
SPANNING TREE PROTOCOL
PROTOCOLS
Common Spanning Tree (CST)
Multiple Instance STP (MISTP) / 802.1s
Per VLAN Spanning Tree (PVST)
Per VLAN Spanning Tree Plus (PVST+)
Rapid STP (RSTP) / 802.1w
Spanning Tree Protocol (STP) / 802.1D

PER VLAN SPANNING TREE (PVST)

Search:
Search A
Toolkit:
Related T
Dynamic
Software

Introduction

Per-VLAN Spanning Tree (PVST) maintains a spanning tree instance for each VLAN configured in the network. It uses ISL Trunking and allows a VLAN trunk to be forwarding for some VLANs while blocking for other VLANs. Since PVST treats each VLAN as a separate network, it has the ability to load balance traffic (at layer-2) by forwarding some VLANs on one trunk and other Vlans on another trunk without causing a Spanning Tree loop.

© 1992-2003 Cisco Systems, Inc. All rights reserved. Important Notices, Privacy Statement, and Trademark

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1089
3702
Doc: 22/7/2003

TECHNOLOGIES
LAN SWITCHING
PROTOCOL GROUPS
SPANNING TREE PROTOCOL
PROTOCOLS
Common Spanning Tree (CST)
Multiple Instance STP (MISTP) / 802.1s
Per VLAN Spanning Tree (PVST)
Per VLAN Spanning Tree Plus (PVST+)
Rapid STP (RSTP) / 802.1w
Spanning Tree Protocol (STP) / 802.1D

PER VLAN SPANNING TREE PLUS (PVST+)

Introduction

Per VLAN Spanning Tree Plus (PVST+) provides the same functionality as PVST using 802.1Q trunking technology rather than ISL. PVST+ is an enhancement to the 802.1Q specification and is not supported on non-Cisco devices.

© 1992-2003 Cisco Systems, Inc. All rights reserved. Important Notices, Privacy Statement, and Trademark

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1090
3702
Nº
Doc:

COBRA TECNOLOGIA
Integradora de Soluções em TI e Serviços

16.699
L

ANEXO SWITCH TIPO 03
PARTE 1

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

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1091
Doc: 5702

ATRIBUTO	ATRIBUTOS OFERTADOS	ATRIBUTOS OFERTADOS ADICIONALMENTE	CONFIMA ATENDIMENTO (SIM/NÃO)	PAGINA DA DOCUMENTAÇÃO TÉCNICA
1 – Recursos Básicos	a) 64 portas FibreChannel operando 2Gbit/s **b) suporte aos servidores Intel e Risc fornecidos** c) suporte ao Storage IBM ESS 21. d) suporte ao backup fornecido e) possibilidade de configurar portas de forma independente f) portas hot-swappable/hot-pluggable g) modularidade **h) RACKS de 19" ou RACK do próprio fabricante**	INTERLIGAÇÃO COM SAN IBM 2105 F20 ???	SIM SIM SIM SIM SIM SIM SIM SIM	a) Connectrix ED-12000B Hardware Reference Manual – pg: 1.2 **b)** Vide ANEXO Unidade de Backup Robotizado, Parte B, ao final (ESS Interoperability Matrix) pg. 11 e 39. c) EMC Support Matrix pg.745/746 d) EMC Support Matrix pg.746/756 e) Connectrix ED-12000B Hardware Reference Manual – pg: 1.2 f) Connectrix ED-12000B Hardware Reference Manual – pg: 1.2 g) Connectrix ED-12000B Hardware Reference Manual – pg: 2.3 **h)** Connectrix ED-12000B Hardware Reference Manual – pg: B-2 – respostas questionamentos item 18.
2 – Portas Ethernet	Interface Fast-Ethernet 10/100 autosensing, com protocolo SNMP para gerência.		SIM	Connectrix ED-12000B Hardware Reference Manual – pg: 1.3 / 2.6 / EMC Connectrix B Series Management Information Base (MIB) Reference Manual
3 – Cabeamento	**555 cabos de Fibra Ótica Multi Mode com conectores LC**		SIM	**Vide seção 17.7 da Proposta TÉCNICA**

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1092
Doc. 3702

16648

4 – Recursos	a) Os equipamentos deverão ser acompanhados de todos os recursos de hardware, software, cabos, manuais, etc necessários a sua total instalação, configuração, gerenciamento e utilização b) Deverá for fornecida pela CONTRATADA ferramenta que implemente o gerenciamento da Rede SAN, contemplando todos os agentes e consoles necessários ao seu pleno funcionamento.Esta ferramenta deve: b.1) Permitir descoberta automática dos elementos que compõe a SAN, baseado em protocolo SNMP ou agentes da própria ferramenta; b.2) Permitir a visão lógica da topologia dos elementos que compões a SAN, de forma gráfica, incluindo as interconexões FC, switches, servidores e devices de storage em uma única console; b.3) Ter a capacidade de apresentar detalhes sobre		SIM SIM SIM SIM SIM	**a) Vide seção 13 da Proposta TÉCNICA** b) software Fabric Manager e Fabric Watch - Connectrix B Fabric Manager Release Notes e Connectrix B Series Fabric Watch Reference Manual b.1) Connectrix B Fabric Manager Release Notes – pg: 3 / Connectrix B Fabric Manager User Guide pg.4.2 / 4.3 / 14.5 b.2) Connectrix B Fabric Manager User Guide – pg: 1.2 / 4.7/13.6/ b.3) Connectrix B Fabric User Guide – pg: 4.7 b.4) Connectrix B Fabric Manager User Guide pg. C-10 / C-15 b.5) Connectrix B Series Fabric Watch Reference Manual pg: 1.13 / 1.14 **c) Vide seção 13 da Proposta TÉCNICA**

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1093
Doc: 3702

16.697

	as conexões das portas FC; b.4) Ter a capacidade de receber eventos provenientes dos elementos constantes na topologia SAN; b.5) Possibilitar o envio dos eventos recebidos através de protocolo SNMP ou agentes próprios. **c) deverão ser montados 02 (dois) ambientes de gerenciamento da Rede SAN, sendo 1 (um) no CCD de Brasilia e 01 (um) no CCD de São Paulo.**		SIM SIM SIM	

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1094
Doc: 3702

1664

5 – Compatibilidade e Integração	a) Os equipamentos deverão ser totalmente compatíveis e fornecer suporte total aos padrões FIBRE CHANNEL. b) Os equipamentos fornecidos deverão integrar-se aos equipamentos já existentes na CONTRATANTE, formando uma única rede SAN em cada localidade Brasília-DF e São Paulo-SP. As versões dos equipamentos existentes são as seguintes: • Switches: Modelo IBM 2109-S16; Fabricante IBM (OEM Brocade 2800 SilkWorm); • Storage: Modelo 2105-F20 (IBM) (2 dispositivos de armazenamento); • HBA´s: Modelo QLOGIC QLA 2200 - PCI Fibre Channel Adapte.		SIM SIM	a) Connectrix ED-12000B Hardware Reference Manual – pg: II / III / A-8 / A9 / A16 / A17 / A18 / A19 / B4 / ; b) EMC Support Matrix pg.743 / 745 / 746, Connectrix B Fabric Manager User Guide – pg: 4.2 / Vide ANEXO Unidade de Backup Robotizado, Parte A, ao final. / Vide ANEXO Unidade de Backup Robotizado, Parte B, ao final (IBM ESS Interoperability Matrix) pg. 39

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1095
Doc: 3704

16.695

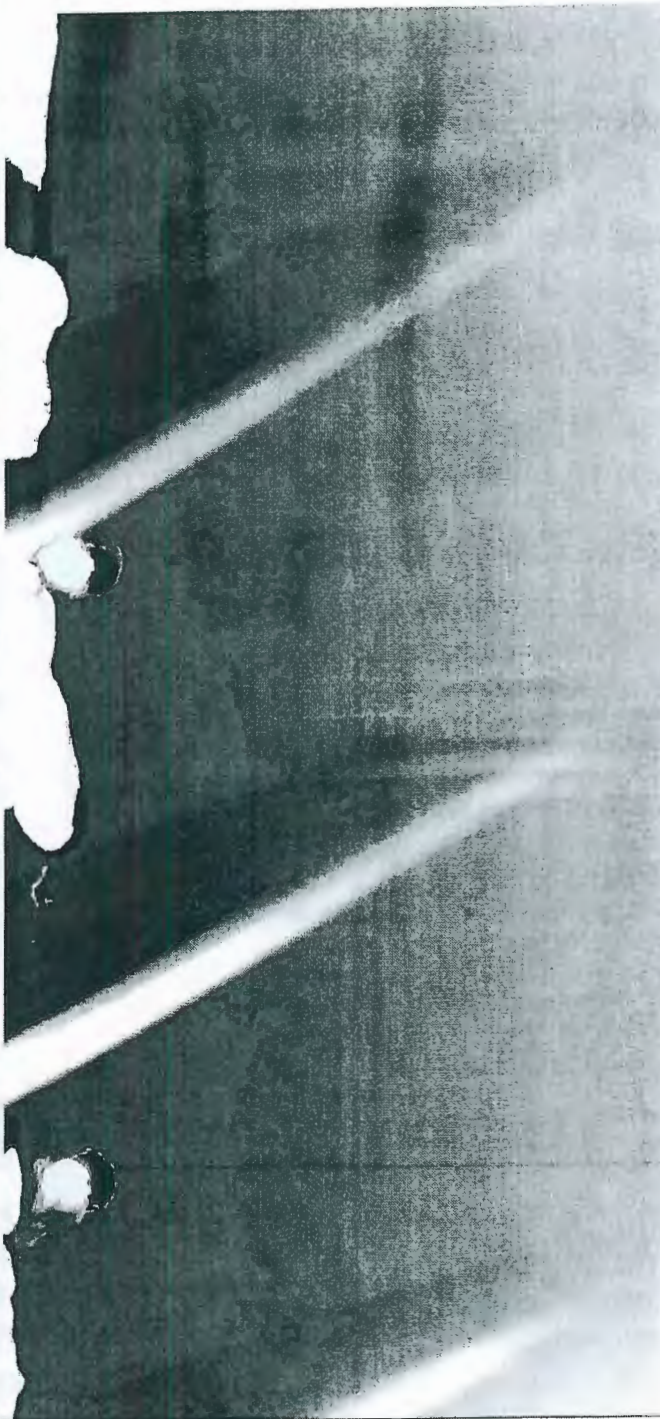
6 – Fonte de Alimentação	Fontes instaladas na configuração máxima do equipamento, com recurso de troca sem interrupção (HOT-SWAPPABLE/HOT-PLUGGABLE) e alimentação elétrica de acordo com a localidade onde serão instalados os equipamentos, conforme subitem 2.5., freqüência de 60 (sessenta) Hertz; As fontes de alimentação deverão ser redundantes por fontes internas independentes, com alimentação redundante, de tal forma que, em caso de falha de uma das fontes por defeito ou por falta de alimentação elétrica em um dos 2 (dois) circuitos, o equipamento continue a funcionar sem prejuízo das aplicações.		SIM	Connectrix ED-12000B Hardware Reference Manual – pg: 1.2 / 2.8 / 4.33 / 4.35 / 2.8 / A-5

2

ECT nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1096
Doc: 3702

16.694

16.69
2



EMC Connectrix Enterprise Director ED-12000B

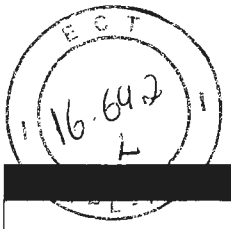
Version 4.1

HARDWARE REFERENCE MANUAL

P/N 300-000-635
REV A03

EMC Corporation
Corporate Headquarters:
Hopkinton, MA 01748 -9103
1-508 -435 -1000
www.EMC.com

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1097
Doc: 702



Copyright © 2000 – 2003 EMC Corporation. All rights reserved.

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 Enterprise Director Model 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。

16691
2.

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

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.

ECT - CPMI - CORREIOS
Fls Nº 1098
Doc: 3702

Contents

Preface xiii

Chapter 1 Introducing the ED-12000B Switch

Overview 1-2
- Port Side of Chassis 1-3
- Blower Assembly Side of Chassis 1-5

Monitoring and Managing the ED-12000B 1-6

Chapter 2 Starting and Operating the ED-12000B Switch

Turning the ED-12000B On and Off 2-2
Operating Information for System Components 2-3
- 16-Port Cards 2-3
- Trunking and Cabling Recommendations 2-4
- Determining the Status of a Port Card 2-4
- Control Processor Cards 2-4
- Determining the Status of a CP Card 2-6
- Connecting Modems to the CP Cards 2-6

Operating Information for the Power Supplies 2-8
- Determining the Status of a Power Supply 2-8
- AC Power Input Connectors and AC Power Switches 2-8

Operating Information for the Blower Assemblies 2-10
- Determining the Status of a Blower Assembly 2-10

Operating Information for the WWN Card and Bezel 2-12
Operating Information for the Chassis 2-13
- Determining the Status of the Chassis 2-13
- Managing Cables 2-13

Interpreting LED Activity 2-16
- LEDs on the 16-Port Card 2-16

RQS nº 03/2005 - SN
CPMI - CORREIOS
Fls Nº 1099
Doc. 3702

LEDs on the Control Processor Card 2-20
LEDs on the Power Supplies 2-22
LEDs on the Blower Assemblies 2-24
Determining the Status of the WWN Card 2-25
LEDs on the WWN Card and Bezel 2-25
Interpreting POST Results 2-27

Chapter 3 Configuring the ED-12000B Switch

Configuring the ED-12000B 3-2
Overview 3-2
Items Required 3-3
Configuration Procedure 3-4

Chapter 4 Maintaining the ED-12000B Switch

Overview 4-2
Performing Diagnostic Tests 4-3
Environmental Status and Maintenance Commands 4-4
Removing and Installing a 16-Port Card or Filler Panel 4-8
Removing, and Installing a Control Processor Card 4-17
Replacing a CP Card 4-18
Confirming a Failed CP Card 4-21
Recording Critical Switch Information 4-21
Removing a CP Card 4-25
Installing a CP Card 4-26
Verifying Operation of the New CP Card 4-26
Removing and Installing a Power Supply 4-33
Removing and Installing a Blower Assembly 4-36
Removing and Installing Cable Management Tray 4-39
Replacing the Cable Management Guides 4-42
Replacing the Chassis Door 4-43
Replacing the WWN Card 4-45
Replacing the Chassis 4-47
Replacing the 14U Rack Kit 4-48

Appendix A Product Specifications for the ED-12000B

ED-12000B Components A-2
Physical Dimensions A-3
ED-12000B and Component Weights A-3
Facility Requirements A-4
Power Specifications A-5
Environmental Requirements A-7

DOC.
000233

CPL/AC

PREGÃO 050/2003

LOCAÇÃO DE EQUIPAMENTOS DE INFORMÁTICA INCLUINDO ASSISTÊNCIA TÉCNICA E TREINAMENTO

COBRA TECNOLOGIA – MANUAL VOLUME 1

2003
PASTA 29

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1100
3702
Doc:

COBRA TECNOLOGIA

Integradora de Soluções em TI e Serviços

ANEXO UNIDADE DE BACKUP ROBOTIZADO
PARTE A

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

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1101
Nº 3702
Doc:

COMPROVAÇÃO DAS ESPECIFICAÇÕES EXIGIDAS NO EDITAL

5. UNIDADE DE BACKUP

ATRIBUTO	ATRIBUTOS OFERTADOS	ATRIBUTOS OFERTADOS ADICIONALMENTE	CONFIRMA ATENDIMENTO (SIM / NÃO)	PÁGINA DA DOCUMENTAÇÃO TÉCNICA
1 – Descrição	a) Deverão ser fornecidos 2 (dois) sistemas automatizados de armazenamento de dados em cartuchos padrão .LTO Ultrium 2., incorporando controladora robotizada, gabinete e software de gerenciamento. Sendo 1 (um) sistema para o CCD de Brasília-DF e 1(um) sistema para o CCD de São Paulo-SP.		**SIM**	**a) Vide seção 11.12 da Proposta TÉCNICA. Vide Anexo Unidade de Backup Robotizado, Parte M, pg.2**

ROS nº 03/2005 - CPMI - CORREIOS
Fls Nº 1102
Doc. 3702

2 – Capacidade da Biblioteca	a) Para o CCD de Brasília, o equipamento deverá possuir capacidade de armazenamento e recuperação de dados para a tecnologia .LTO Ultrium 2. de, no mínimo, 60TB (sessenta Terabytes), sem compressão (nativo); b) Para o CCD de São Paulo, o equipamento deverá possuir capacidade de armazenamento e recuperação de dados para a tecnologia .LTO Ultrium 2. de, no mínimo, 40TB (sessenta Terabytes), sem compressão (nativo); - Não será considerada para efeito de cálculo da capacidade solicitada tecnologia de compactação e/ou compressão.		**SIM**	**a)Vide Anexo Unidade de Backup Robotizado, Parte A, pg.18, Parte R, pg. 1** **(400slots X 200GB) sem compressão por cartucho = 80TB sem compressão.** **a) Vide Anexo Unidade de Backup Robotizado, Parte M, pg.2 e 9, Parte R,pg. 1** **(400slots X 200GB) sem compressão por cartucho = 80TB sem compressão.**
3 – Capacidade dos Cartuchos	a) O cartucho .LTO Ultrium 2. deverá possuir capacidade mínima de 200GBytes (sem compressão).		**SIM**	**a) Vide Anexo Unidade de Backup Robotizado, Parte R, pg.1**

ECT - DR/AC - CPL - Fls. 17.746 - Paula

ECT - DR/AC - CPL - Fls Nº 11037 - RQS nº 03/2005 - CN - CPMI - CORREIOS - Doc. 3702

4 – Compatibilidade	a) O hardware deve ser compatível com o padrão .LTO Ultrium., permitindo a leitura de cartuchos, neste padrão, instalados na fitoteca atualmente instalada nos Correios (.3583-L72 IBM LTO Ultrium.).		**SIM**	**a) Conforme a FAQ da Tecnologia Ultrium em www.ultrium.com; ver impressão de " LTO – About the Technology – FAQS" ao final do Anexo Unidade de Backup Robotizado, Parte U.**
5 – Quantidade de SLOTS	a) Deverá possuir um mínimo de SLOTS que disponibilize a capacidade total solicitada de cada fitoteca dividida pela capacidade dos cartuchos cotados, ou seja: **Num. Slots = Capacidade Solicitada da Biblioteca / Capacidade do Cartucho.** 1. Quantidade de slots Brasília = 60TB / 200GB= 300 slots 2. Quantidade de slots São Paulo = 40 TB / 200 GB = 200 slots		**SIM**	**a)Quantidade de slots Brasília = 60TB / 200GB= 300 slots Quantidade de slots São Paulo = 40 TB / 200 GB = 200 slots Vide seção 11.12 da Proposta Técnica**

RQS nº 03/2005 CN CPMI - CORREIOS
Fls Nº 1104
Doc: 3702

6 – Quantidade de Cartuchos	a) O número de cartuchos a ser fornecido para cada equipamento deverá ser igual ao **dobro** do número de SLOTS solicitados, calculados no item anterior. Estes deverão ser testados e garantidos contra erros por um período mínimo de 10 (DEZ) anos, sem manutenção.		**SIM**	**a) Estão sendo ofertados 600 cartuchos para Brasília e 400 cartuchos para São Paulo (igual ao dobro do número de slots solicitados). Vide seção 11.12 da Proposta TÉCNICA** **- Os cartuchos são testados e garantidos contra erros por um período mínimo de 30 (trinta) anos, sem manutenção.** **Vide Anexo Unidade de Backup Robotizado, Parte R, pg.2**
7 – THROUGHPUT por drive	a) Os drivers deverão apresentar performance nominal de 30MB/segundo para gravação, sem compactação, utilizando cartuchos padrão .LTO Ultrium 2..			**a) Vide Anexo Unidade de Backup Robotizado, Parte R, pg.1**

CPL 17.7711 Paula

RGS nº 0220/2003 - CN CPMI - CORREIOS Fls Nº 140 3702 1105 Doc:

8 – Número de DRIVES	a) Para o **CCD de Brasília**, o equipamento deverá possuir no mínimo **20 (vinte) drives**, devendo atingir o THROUGHPUT nominal de 600 (seiscentos) MB/segundo, utilizando tecnologia de gravação linear, permitindo operação simultânea de todos os drives. b) Para o **CCD de São Paulo**, o equipamento deverá possuir no mínimo **12 (doze) drives**, devendo atingir o THROUGHPUT nominal de 360 (trezentos e sessenta) MB/segundo, utilizando tecnologia de gravação linear, permitindo operação simultânea de todos os drives.		**SIM**	**a) ESL9595 com 20 drives para Brasília, utilizando mecanismo de pass-through, atingindo throughput de 360 MB/séc sem compressão.** **b) ESL 9595 com 12 drives para São Paulo, atingindo throughput de 600 MB/séc sem compressão.** **Vide Anexo Unidade de Backup Robotizado, Parte R, pg.1, Parte M, pg.3 scalability.**
9 – Conectividade	a) Fibre Channel, operando a 2 Gbit/sec, entre os servidores e a unidade de backup.		**SIM**	**a) Vide Anexo Unidade de Backup Robotizado, Parte M, pg.4**

17.773 Paula AC

Nº 3702 Fls. 1106 PMI CORREIOS nº 02/2005 - CN

10 – Recursos de Hardware	a) Possuir a capacidade de manutenção/substituição de cartuchos, sem interrupção dos processos de BACKUP ou RESTORE em curso; Possuir no mínimo 1 (uma) Porta de comunicação para diagnósticos; Sistema de leitura de código de barras; b) Os rótulos dos cartuchos . LABEL, deverão seguir padrão definido pela **CONTRATANTE**.			**a) Vide Anexo Unidade de Backup Robotizado, Parte A, pg.30, primeiro parágrafo (bar code reader), pg.104, library diagnostics, pg.18, features and benefits, sétimo bullet (load port).**
11 – Retirada das Fitas	a) Os equipamentos e softwares fornecidos deverão permitir a realização da cópia dos dados armazenados nos cartuchos em cartuchos novos; Os equipamentos e softwares fornecidos deverão permitir que a **CONTRATANTE** realize a retirada dos cartuchos duplicados sem que esta operação interrompa os demais processos de BACKUP ou RESTORE em curso.			**a) Vide Anexo Unidade de Backup Robotizado, Parte A, pg.18, features and benefits, sétimo bullet (load port), Parte D/2, pg.143**

RQS nº 03/2005 - CPMI - CORREIOS
Fls Nº 3702
Doc:

15 – Geral	a) Deverão ser fornecidos 2 (dois) servidores RISC para o CCD de Brasília, em alta disponibilidade, para abrigar os softwares gerenciadores das fitotecas e os softwares gerenciadores do backup; Deverão ser fornecidos 2 (dois) servidores RISC para o CCD de São Paulo, em alta disponibilidade, para abrigar o software gerenciador da fitoteca e o software gerenciador do backup; Os servidores deverão estar dimensionados de tal forma que suportem o gerenciamento de, no mínimo, 150 clientes de backup, individualmente.			**a) Vide seção 11.12 da Proposta TÉCNICA**

17768 Paula

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 3702
1108
Doc:

E C T
17.767
Paula

user guide

hp StorageWorks ESL9000 series tape library

Sixth Edition (April 2003)

Part Number: 243491-026

Product Regulatory Series ID Number: ED1002

This guide describes procedures for operating, maintaining, and troubleshooting the HP StorageWorks ESL9000 Series tape library.

invent

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1109
3702
Doc:

© Hewlett-Packard Company, 2003. All rights reserved.

Hewlett-Packard Company makes no warranty of any kind with regard to this material, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Hewlett-Packard shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

This document contains proprietary information, which is protected by copyright. No part of this document may be photocopied, reproduced, or translated into another language without the prior written consent of Hewlett-Packard. The information contained in this document is subject to change without notice.

Compaq Computer Corporation is a wholly-owned subsidiary of Hewlett-Packard Company.

All other product names mentioned herein may be trademarks of their respective companies.

Hewlett-Packard Company shall not be liable for technical or editorial errors or omissions contained herein. The information is provided "as is" without warranty of any kind and is subject to change without notice. The warranties for Hewlett-Packard Company products are set forth in the express limited warranty statements accompanying such products. Nothing herein should be construed as constituting an additional warranty.

Printed in the U.S.A.

HP StorageWorks ESL9000 Series Tape Library User Guide
Sixth Edition (April 2003)
Part Number: 243491-026

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1110
Nº 3702
Doc:

contents

About this Guide 9
Conventions 10
Document Conventions 10
Text Symbols 10
Equipment Symbols 11
Rack Stability 12
Getting Help 13
HP Technical Support 13
HP Storage Website 13
HP Authorized Reseller 14

1 **Library Description** 15
Library Models 16
Features and Benefits 18
Library Components 19
Cabinet 19
Cabinet (Front Panel) 19
Cabinet (Rear Panel) 22
Storage Bins (ESL9322) 24
Storage Bins (ESL9595) 26
Control Panel 28
Robotics 29
Tape Drives 30
Ultrium Tape Drives 31
Ultrium Tape Cartridges 32
SDLT Tape Drives 34
SDLT Tape Cartridges 35
Load Port 36
Optional Pass-Through Mechanism (PTM) 36
Optional Network Storage Router 37

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1111
Doc: 3702

2 Preparing the Library for Operation 39
Opening the Library Doors and Access Panels 40
Connecting SCSI Cables 41
ESL9322 SCSI Cable Configurations 41
ESL9595 SCSI Cable Configurations 43
Default SCSI IDs 46
Preparing Tape Cartridges 47
Labeling Tape Cartridges 47
SDLT Bar Code Labels 48
Ultrium Bar Code Labels 49
Media Label Identifiers 50
Setting the Write-Protect Switch 51
Write-Protecting SDLT Tape Cartridges 51
Write-Protecting Ultrium Tape Cartridges 52
Inserting and Removing Tape Cartridges 53
Placing Tape Cartridges into Fixed Storage Bins 53
Using the Load Port 54
Using the Load Pack Magazine 56
Adding a Cartridge to a Magazine 56
Removing a Cartridge from a Magazine 56
Turning the Library On and Off 57
Turning the Library On 57
Placing the Library On-line or Off-line 57
Turning the Library Off 58

3 Operating the Control Panel 59
Using the Control Panel 60
Basic Operation 63
Opening a Screen 63
Navigating from Screen to Screen 63
Exiting a Screen 64
Library Controls 64
Obtaining Library Status 66
Overview Screen 66
Drive Status 67
Activity Status 68
Load Port Status 68
Tapes Screen 69
Viewing Storage and Load Port Elements 69

RQS nº 03/2005 - CN - CPMI - CORREIOS
1112
Fls Nº 3702
Doc:

Changing the Control Panel Security Levels 70
Securing the Control Panel. 70
Changing Security Levels 71

4 Operator Commands 73
Opening the Operator Screen 74
Configuring the Library 76
SCSI ID Assignment Guidelines 78
PTM Configuration 78
Configuring Library Options 79
Configuring a Library Option 80
Viewing the Error Log 82
Calibrating the Library 83
Performing an Inventory. 84
Moving Cartridges 85
Unloading a Drive. 87
Unloading the Load Port. 88

5 Maintenance and Troubleshooting 89
Troubleshooting Common Problems 90
Start Up Problems 90
Control Panel Problems 91
Robotics Problems 92
Operating Problems 94
Tape Drive Problems 96
Tape Drive Interface LED Problems 97
Maintaining Tape Cartridges 98
Cleaning Tape Drives 100
Cleaning SDLT Tape Drives 100
Cleaning Ultrium Tape Drives 101
Using HP StorageWorks Library and Tape Tools 102

A Specifications 103
Physical Characteristics 104
Performance Characteristics 106
Environmental Specifications 106
Safety and Regulatory Specifications 107

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1113
3702
Doc:

B Regulatory Compliance Notices 109
Federal Communications Commission Notice 110
Class A Equipment 110
Class B Equipment 110
Modifications 111
Cables 111
Declaration of Conformity for products marked with the FCC logo - United States only 111
Canadian Notice (Avis Canadien) 112
Class A Equipment 112
Class B Equipment 112
European Union Notice 112
BSMI Class A Notice 113
Japanese Notice 113
Laser Device 113
Laser Safety Warnings 114
Compliance with CDRH Regulations 114
Compliance with International Regulations 114
Laser Specifications 114
Laser Regulation Labels 115
Product Conformation Label 115
Laser Caution Label 115
Exposure Caution Label 115

C Sense Data Values 117
Sense Data Values 118

D Capacity on Demand 135
Upgrading Your Capacity 136

Index 139

Figures

1 Cabinet front panel (ESL9322) 20
2 Cabinet front panel (ESL9595) 21
3 Cabinet rear panel (ESL9322) 22
4 Cabinet rear panel (ESL9595) 23
5 Storage bin numbering conventions (ESL9322) 25
6 Storage bin numbering conventions (ESL9595) 27
7 Control panel home screen (ESL9595 shown) 28

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1114
Nº 3702
Doc:

EP 1776 Paulo CPL - AC

8 Library robotics 29
9 Ultrium tape drive 31
10 HP Ultrium format trademark 32
11 SCSI ports (ESL9322) 41
12 Internal SCSI cabling configuration (ESL9322) 42
13 SCSI ports (ESL9595) 43
14 Internal SCSI cabling configuration (ESL9595) 44
15 Inserting an SDLT bar code label 48
16 Attaching an Ultrium bar code label 49
17 Proper Ultrium bar code label placement. 50
18 Write-protecting SDLT tape cartridges 51
19 Write-protecting Ultrium tape cartridges 52
20 Load port (ESL9322 shown) 55
21 Inserting a tape cartridge into a magazine 56
22 Control panel home screen (ESL9595 shown). 60
23 Library controls (ESL9595 shown) 64
24 Overview screen. 66
25 Tape drive status box 68
26 Tapes screen. 69
27 Change password screen 71
28 Operator password screen 74
29 Operator screen 75
30 Configure: library screen (ESL9595 shown) 76
31 Configure: library settings screen (ESL9595 shown) 77
32 Configure: options screen 80
33 Calibrate library screen 83
34 Control: move cartridge screen 85
35 Control: unload drive screen 87
36 Product conformation label 115
37 Laser light caution label. 115
38 Exposure caution label. 115
39 License screen (ESL9595 shown) 136

Tables

1 Document Conventions 10
2 Library Capacity (Fully Populated) 16
3 ESL9322 Library Model Numbers. 17
4 ESL9595 Library Model Numbers. 17

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1115
3702
Doc:

E C T
17.460
Paula
CPL - AC

5 Ultrium Tape Drive Capacity and Data Transfer Rate 32
6 SDLT Tape Drive Capacity and Data Transfer Rate 35
7 SCSI Ports and Device Connections (ESL9322) 42
8 SCSI Ports and Device Connections (ESL9595) 44
9 Default SCSI IDs 46
10 Media Label Identifiers 50
11 Control Panel Menus 61
12 Control Panel Navigation 62
13 Security Levels, Highest to Lowest 65
14 Start Up Problems 90
15 Control Panel Problems 91
16 Robotics Problems 92
17 Operating Problems 94
18 Tape Drive Problems 96
19 Tape Drive Interface LED Problems 97
20 Physical Characteristics (ESL9322) 104
21 Physical Characteristics (ESL9595) 105
22 Performance Characteristics 106
23 Environmental Specifications 106
24 Regulatory and Product Safety Certifications 107
25 Laser Specifications 114
26 Sense Data Values (Hexadecimal) 118

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1116
3702
Doc:

E C T
17.759
Paula
A C

about this guide

This user guide provides information to help you:

- Prepare the library for operation.
- Operate the control panel.
- Use operator commands.
- Maintain and troubleshoot the library.

"About this Guide" topics include:

- Conventions, page 10
- Rack Stability, page 12
- Getting Help, page 13

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1117
3702
Doc:

Conventions

Conventions consist of the following:

- Document Conventions
- Text Symbols
- Equipment Symbols

Document Conventions

The document conventions included in Table 1 apply in most cases.

Table 1: Document Conventions

Element	Convention
Cross-reference links	Blue text: Figure 1
Key and field names, menu items, buttons, and dialogue box titles	**Bold**
File names, application names, and text emphasis	*Italics*
User input, command and directory names, and system responses (output and messages)	`Monospace font` `COMMAND NAMES` are uppercase monospace font unless they are case sensitive
Variables	`<monospace, italic font>`
Website addresses	Blue, underlined sans serif font text: http://www.hp.com

Text Symbols

The following symbols may be found in the text of this guide. They have the following meanings.

WARNING: Text set off in this manner indicates that failure to follow directions in the warning could result in bodily harm or death.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1118
3702
Doc:

CPL - AT
47754
Paula

Caution: Text set off in this manner indicates that failure to follow directions could result in damage to equipment or data.

Note: Text set off in this manner presents commentary, sidelights, or interesting points of information.

Equipment Symbols

The following equipment symbols may be found on hardware for which this guide pertains. They have the following meanings.

Any enclosed surface or area of the equipment marked with these symbols indicates the presence of electrical shock hazards. Enclosed area contains no operator serviceable parts.

WARNING: To reduce the risk of personal injury from electrical shock hazards, do not open this enclosure.

Any RJ-45 receptacle marked with these symbols indicates a network interface connection.

WARNING: To reduce the risk of electrical shock, fire, or damage to the equipment, do not plug telephone or telecommunications connectors into this receptacle.

Any surface or area of the equipment marked with these symbols indicates the presence of a hot surface or hot component. Contact with this surface could result in injury.

WARNING: To reduce the risk of personal injury from a hot component, allow the surface to cool before touching.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1119
Nº 3702
Doc:

17.756 Paula

Power supplies or systems marked with these symbols indicate the presence of multiple sources of power.

WARNING: To reduce the risk of personal injury from electrical shock, remove all power cords to completely disconnect power from the power supplies and systems.

Any product or assembly marked with these symbols indicates that the component exceeds the recommended weight for one individual to handle safely.

WARNING: To reduce the risk of personal injury or damage to the equipment, observe local occupational health and safety requirements and guidelines for manually handling material.

Rack Stability

Rack stability protects personnel and equipment.

WARNING: To reduce the risk of personal injury or damage to the equipment, be sure that:

- The leveling jacks are extended to the floor.
- The full weight of the rack rests on the leveling jacks.
- In single rack installations, the stabilizing feet are attached to the rack.
- In multiple rack installations, the racks are coupled.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1120
Nº 3702
Doc:

17.155 Paula AC

Getting Help

If you still have a question after reading this guide, contact an HP authorized service provider or access our website: http://www.hp.com.

HP Technical Support

In North America, call technical support at 1-800-652-6672, available 24 hours a day, 7 days a week.

Note: For continuous quality improvement, calls may be recorded or monitored.

Outside North America, call technical support at the nearest location. Telephone numbers for worldwide technical support are listed on the HP website under support: http://www.hp.com/support.

Be sure to have the following information available before calling:

- Technical support registration number (if applicable)
- Product serial numbers
- Product model names and numbers
- Applicable error messages
- Operating system type and revision level
- Name and revision of application software

HP Storage Website

The HP website has the latest information on this product, as well as the latest drivers. Access storage at: http://www.hp.com/products/tapestorage. From this website, select the appropriate product or solution.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1121
Nº 3702 Doc

HP Authorized Reseller

For the name of your nearest HP authorized reseller:

- In the United States, call 1-800-345-1518
- In Canada, call 1-800-263-5868
- Elsewhere, see the HP website for locations and telephone numbers: http://www.hp.com/support.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1122
Nº Doc: 3702

CPL - EC
17-733
Paula

Library Description

1

This chapter describes the HP StorageWorks ESL9000 Series tape library and its components. Sections include:

- Library Models, page 16
- Features and Benefits, page 18
- Library Components, page 19:
  - Cabinet, page 19
  - Control Panel, page 28
  - Robotics, page 29
  - Tape Drives, page 30
  - Load Port, page 36
  - Optional Pass-Through Mechanism (PTM), page 36
  - Optional Network Storage Router, page 37

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1123
Doc: 3702

Library Models

The HP StorageWorks ESL9000 Series tape library is an automated storage and retrieval library. It contains up to 8 drives and 322 cartridges for the ESL9322 Series, and up to 16 tape drives and 595 cartridges for the ESL9595 Series.

The following ESL9000 Series tape library models support a wide range of storage and performance requirements.

Table 2: Library Capacity (Fully Populated)

Library	# Cartridges	Drive Type	Native Capacity	2:1 Compression Enabled
ESL9322	322 cartridges at 160 GB each	SDLT 320	51.52 TB (51,520 GB)	103.04 TB (103,040 GB)
ESL9322	322 cartridges at 100 GB each	Ultrium 230	32.2 TB (32,200 GB)	64.4 TB (64,400 GB)
ESL9322	322 cartridges at 200 GB each	Ultrium 460	64.4 TB (64,400 GB)	128.8 TB (128,800 GB)
ESL9595	595 cartridges at 110 GB each	SDLT 220	65.45 TB (65,450 GB)	130.9 TB (130,900 GB
ESL9595	595 cartridges at 160 GB each	SDLT 320	95.2 TB (95,200 GB)	190.40 TB (190,400 GB)
ESL9595	595 cartridges at 100 GB each	Ultrium 230	59.5 TB (59,500 GB)	119 TB 119,000 GB)
ESL9595	595 cartridges at 200 GB each	Ultrium 460	119 TB (119,000 GB)	238 TB (238,000 GB)

Note: Although the tape libraries support mixed media at the hardware level, your application software might not.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1124
Doc: 3702

E C
17-15
Paula
CPL

The model number defines:

- The standard inquiry string
- The default number of bins

The model number is set at the factory, and under normal circumstances, does not need to be changed.

Table 3: ESL9322 Library Model Numbers

Model Number	Model Name	Displayed Name	Product ID	Number of Drives	Storage Bins	Drive Type	SCSI Interface
6437080 (def)	ESL9322	ESL9322	ESL9000 SERIES	8	322	SDLT/ Ultrium	LVD
6437085	ESL9322	ESL9322	P4000 6437085	8	322	SDLT/ Ultrium	LVD

Table 4: ESL9595 Library Model Numbers

Model Number	Model Name	Displayed Name	Product ID	Number of Drives	Storage Bins	Drive Type	SCSI Interface
6438280 (def)	ESL9595	ESL9595	ESL9000 SERIES	16	595	SDLT/ Ultrium	LVD
6438081	ESL9595	ESL9595	ESL9000 SERIES	16	400	SDLT/ Ultrium	LVD
6438285	ESL9595	ESL9595	P7000 6438285	16	595	SDLT/ Ultrium	LVD

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1125
Nº 3702
Doc:

E C
17.750
CPL Paula
AC

Features and Benefits

Your tape library provides the following features and benefits:

- High-capacity, high-performance data storage and retrieval.
- Expandable configurations:

  Up to five ESL9322 tape libraries and up to four ESL9595 tape libraries can be joined together into one multi-unit library system. Tape cartridges can be shared between libraries using optional Pass Through Mechanisms (PTMs).
- Optional Fibre Channel upgrade kit.
- Reliable, versatile 120-240 volt AC auto-switching power supplies.
- Hot-pluggable, redundant DC power supplies to ensure library operations against power supply failure.
- Advanced cooling system to prevent overheating.
- On-line cartridge exchanges: load port with two stationary 4-cartridge magazines for easy insertion of cartridges without interrupting library operations.
- Easy serviceability and manageability:
  - — Hot-pluggable SDLT and Ultrium tape drives, DC power supplies, and fans allow repairs without taking the library off-line.
  - — Easy access and replacement of critical components.
  - — A control panel providing a wide range of configuration and service-related functions.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1126
3702
Doc:

CPL 17749 Paula

Library Components

The library consists of the following major components:

- Cabinet
- Control Panel
- Robotics
- Tape Drives
- Load Port
- Optional Pass-Through Mechanism (PTM)

Cabinet

The cabinet houses all library components including:

- Robotics
- Storage bins
- Control electronics
- Power supply and distribution equipment
- Fans
- Tape drives
- Optional Fibre Channel upgrade kit

Access these components through the front and back doors of the library cabinet.

Cabinet (Front Panel)

The front of the library cabinet provides access as follows (see Figure 1 on page 20 through Figure 2 on page 21):

- The front door(s) provide easy access to the gripper and robotics.
- The viewing windows make it possible to visually monitor library operations.
- A control panel on the right side of the cabinet lets you configure, control, and monitor the library.
- The load port provides easy insertion of additional tape cartridges while the library is in operation. The load port has either 8 or 12 shelf bins, depending on the drive technology being used (8 bins for Ultrium and 12 bins for SDLT).

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1127
3702
Doc:

- The power switch for the library is located behind a sliding panel on the front door below the control panel.

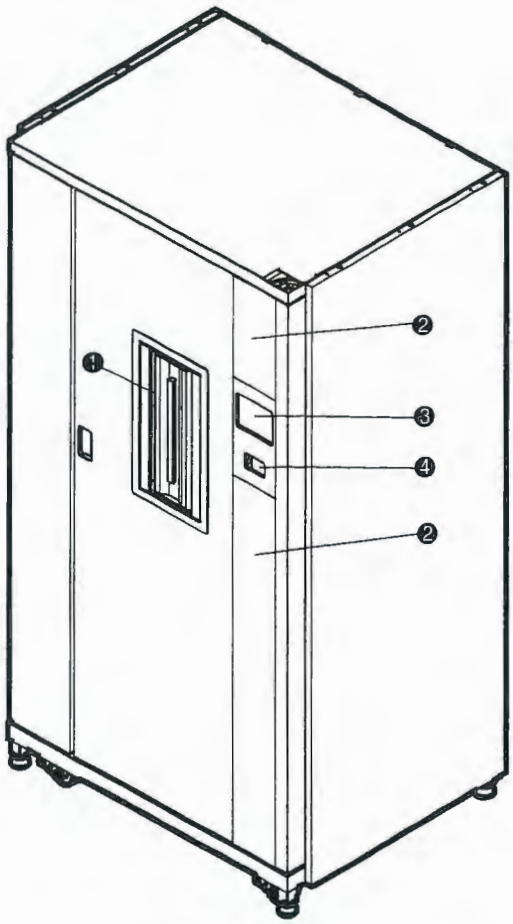


Figure 1: Cabinet front panel (ESL9322)

❶ Load port with magazines
❷ Viewing windows
❸ Control panel touch screen
❹ Power switch

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1128
Doc 3702

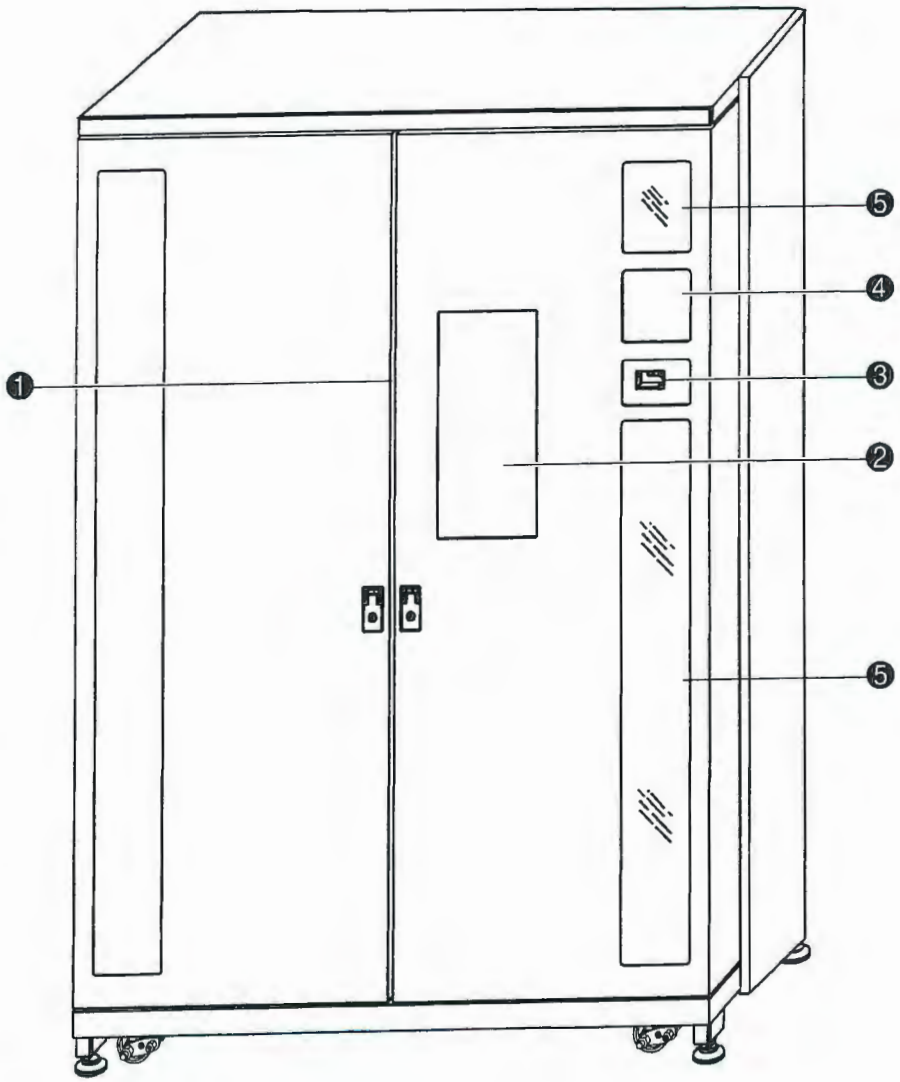


Figure 2: Cabinet front panel (ESL9595)

❶ Dual doors
❷ Load port with magazines
❸ Power switch
❹ Touch screen control panel
❺ Viewing windows

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1129
Doc 3702

17.426
Paula
CPL

Cabinet (Rear Panel)

The rear of the cabinet (see Figure and Figure 4 on page 23) provides easy accessibility to:

- Cooling fans
- Power, control, and data interfaces
- Tape drives

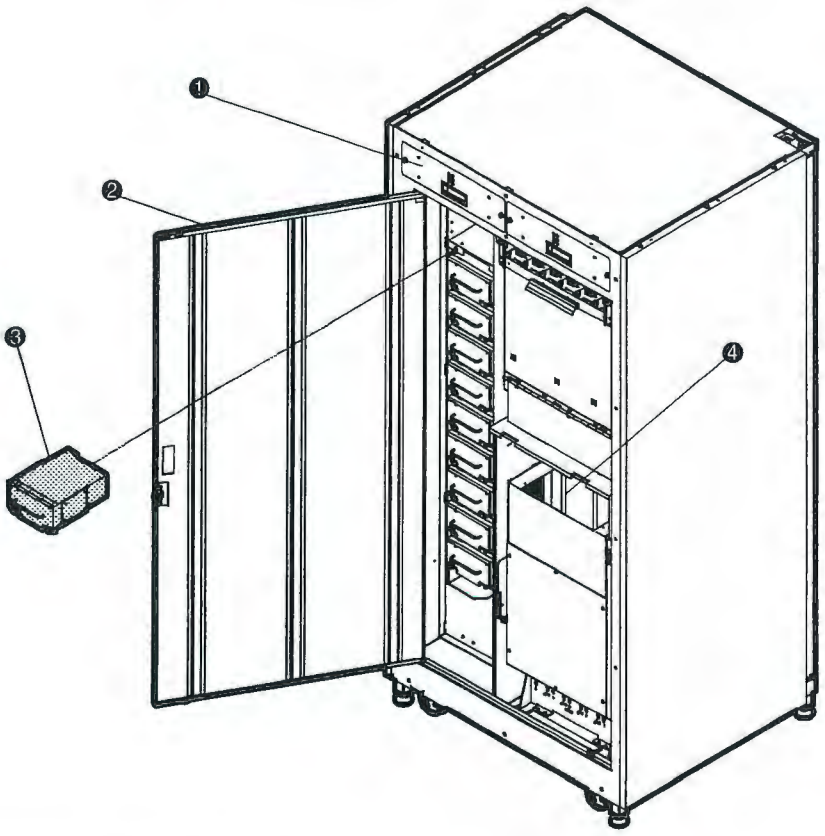


Figure 3: Cabinet rear panel (ESL9322)

1. Hot-pluggable removable fans
2. Easy-access rear panel
3. Hot-pluggable drives in removable canisters
4. Location of optional Fibre Channel upgrade kit

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1130
Doc: 3702

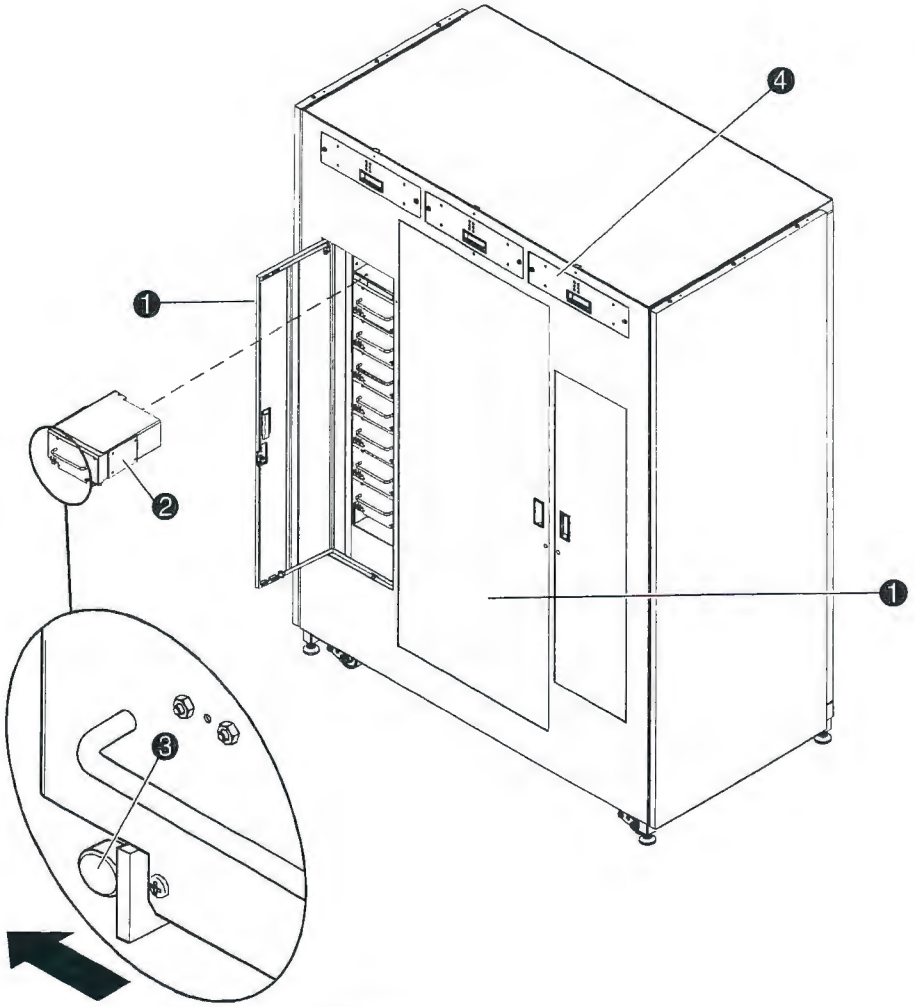


Figure 4: Cabinet rear panel (ESL9595)

❶ Easy-access rear panel

❷ Hot-pluggable drives in removable canisters

❸ Drive quick release thumbscrew on each bottom corner

❹ Hot-pluggable removable fans

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1131
Doc: 3702

Storage Bins (ESL9322)

The ESL9322 stores tape cartridges in the following locations:

- Up to 171 storage bins on the back wall

Note: Some bins are removed if a PTM is installed.

- 111 shelf bins on the inside of the right front door
- 40 shelf bins on the inside of the left front door
- One load port consisting of two 4-cartridge stationary or 6-cartridge removable shelf bins
- Up to 8 tape drives

Figure 5 on page 25 shows the storage bin, load port bin, and tape drive numbering conventions. These conventions are used by the library control panel and diagnostic software programs.

Note: The ESL9322 and ESL9595 tape libraries ship with the maximum number of physical storage slots available. However, access to these slots requires an upgrade key for the library to recognize them. See "Capacity on Demand" on page 135 for additional information.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1132
Nº 3702
Doc:

CPL - AC

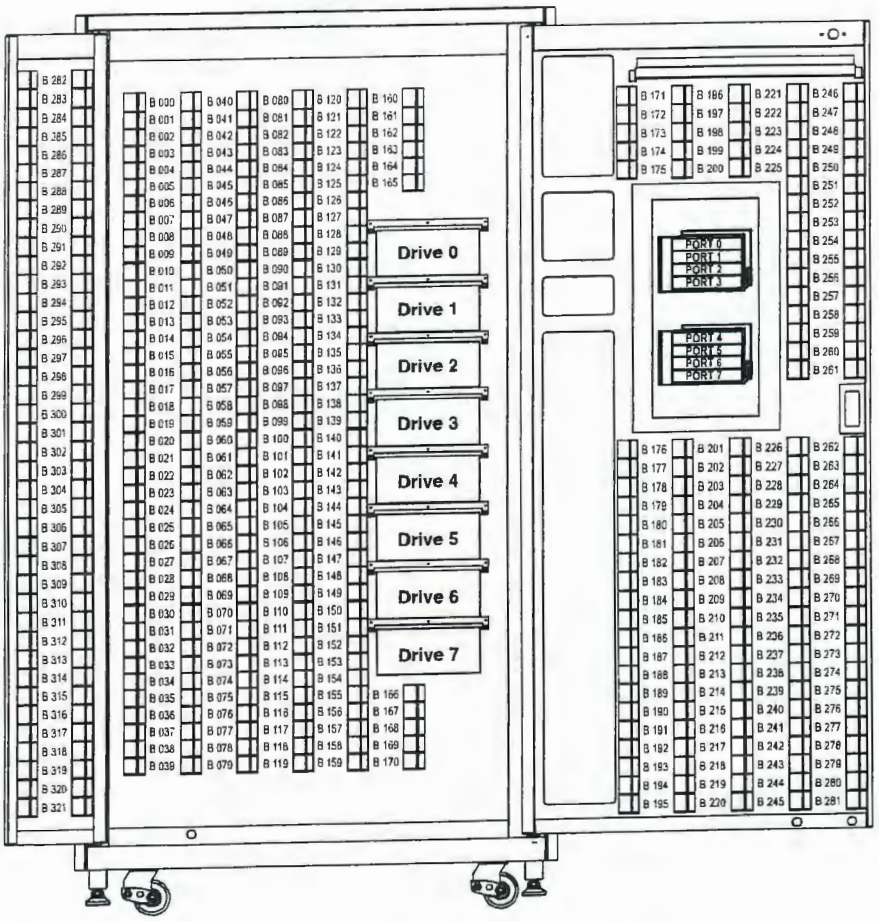


Figure 5: Storage bin numbering conventions (ESL9322)

Note: Storage bin and drive numbering begins with 0. Consequently, the first drive is drive 0, the second drive is drive 1, etc.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1133
Doc: 3702

17.742 Paula CPL - A

Storage Bins (ESL9595)

- The ESL9595 stores tape cartridges in the following locations:
- 288 storage bins on the back wall
- 196 storage bins on the inside of the left door
- 111 storage bins on the inside of the right door
- One load port consisting of two 4-cartridge stationary or 6-cartridge removable shelf bins
- Up to 16 tape drives

Figure 6 shows the storage bin, load port bin, and tape drive numbering conventions. The tape library touch screen control panel and diagnostic software programs use these conventions.

Note: The ESL9322 and ESL9595 tape libraries ship with the maximum number of physical storage slots available. However, access to these slots requires an upgrade key for the library to recognize them. See "Capacity on Demand" on page 135 for additional information.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1134
Doc: 3702

E
17741
Paula

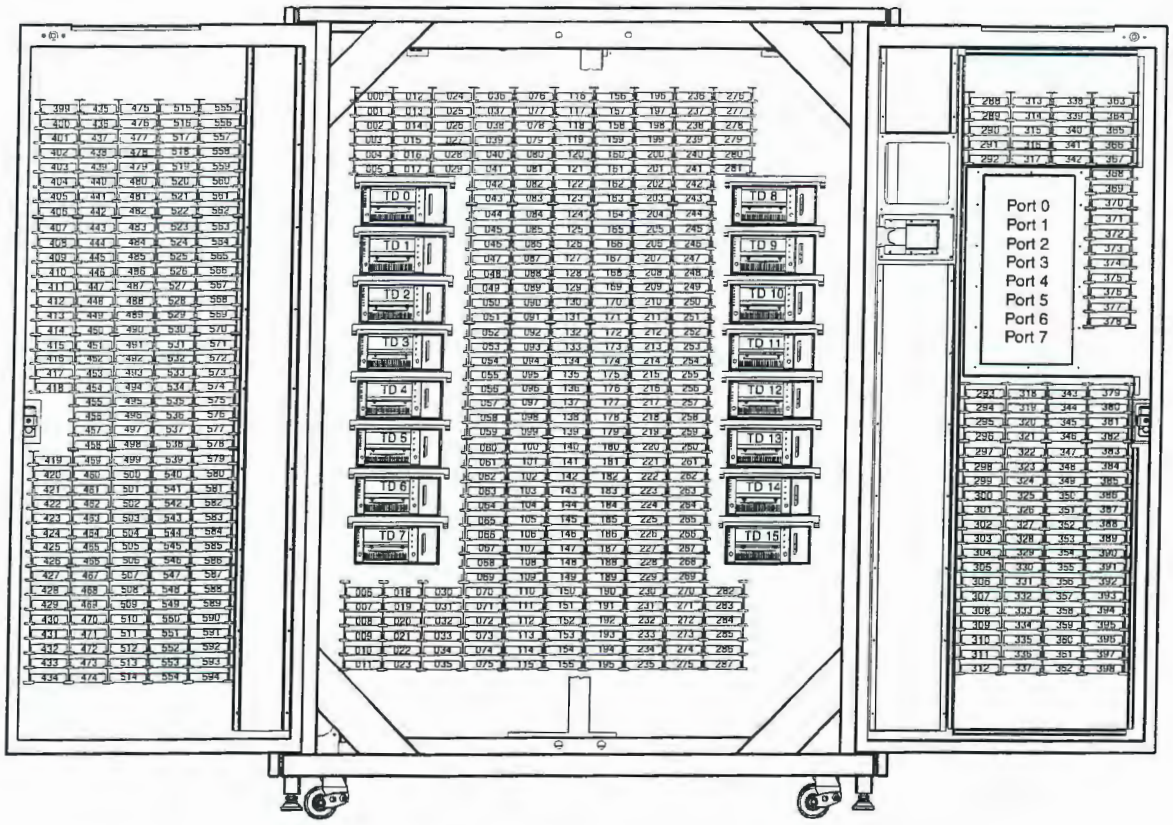


Figure 6: Storage bin numbering conventions (ESL9595)

Note: Storage bin and drive numbering begins with 0. Consequently, the first drive is drive 0, the second drive is drive 1, etc.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1135
Nº 3702
Doc:

Control Panel

The control panel features a menu system for determining library status, configuring the library, and performing certain diagnostic functions (see Figure 7).

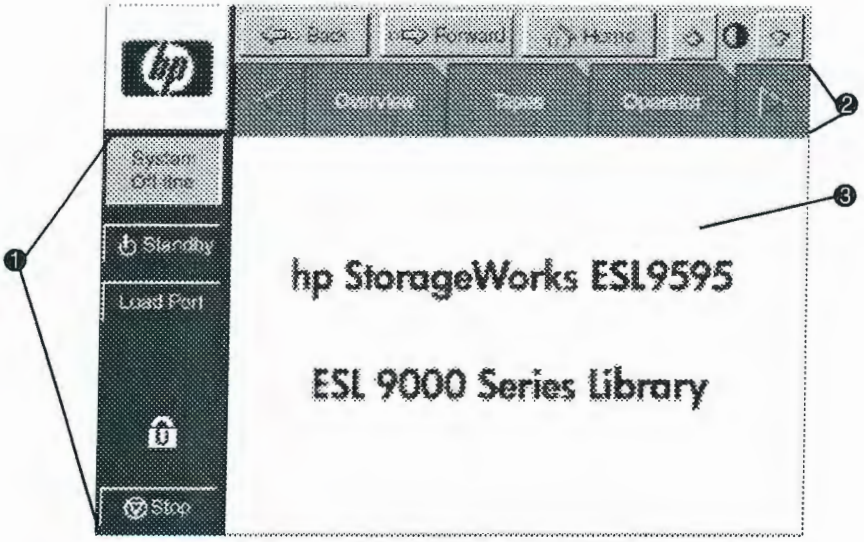


Figure 7: Control panel home screen (ESL9595 shown)

❶ Vertical taskbar ❷ Horizontal taskbar ❸ Main display area

The vertical taskbar (❶ Figure 7) provides various library controls such as system state display (**Off-line** or **On-line**), **Standby** button, **Load Port** button, the security level indicator (lock icon), and the **Stop** button. The **Stop** button immediately removes power from library robotics.

The horizontal taskbar (❷ Figure 7) provides left and right arrow buttons to scroll through the tabs for **Overview**, **Tapes**, **Operator**, **Service**, and **Multi-unit** options.

For more information about the library control panel, see "Using the Control Panel" on page 60.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1136
Doc: 3702

17.739
CPL - Paula

Robotics

Figure 8 shows the library robotics, also referred to as the gripper or GRP on the library control panel.

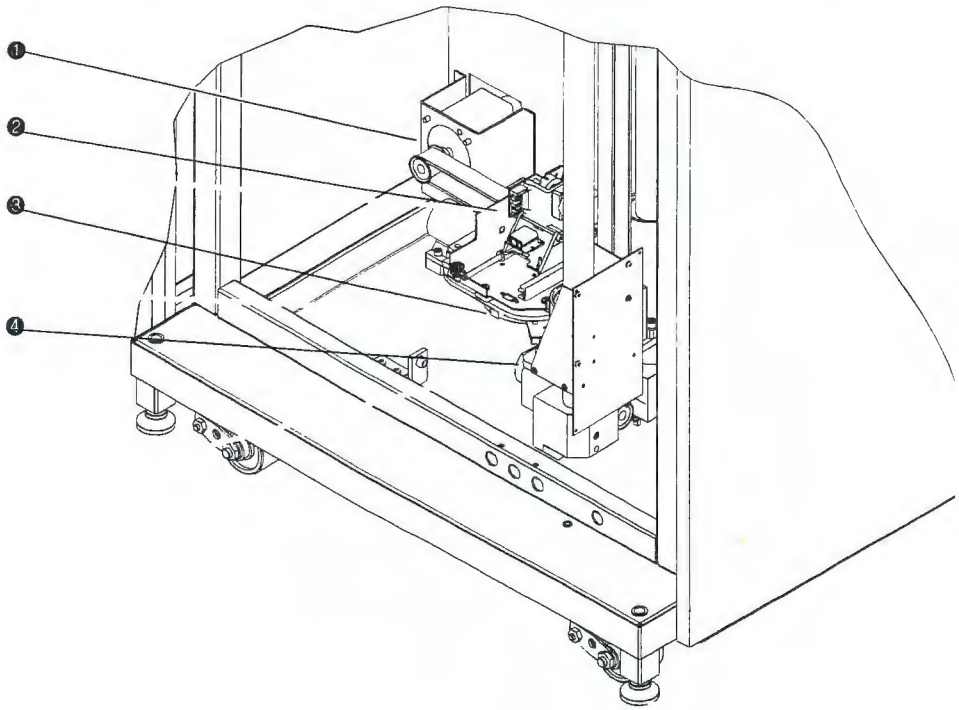


Figure 8: Library robotics

1. Horizontal drive motor
2. Mixed media gripper assembly
3. Extension axis assembly
4. Vertical carriage assembly

The vertical and horizontal actuators move the gripper into position to pick and place tape cartridges. The rotary actuator rotates the gripper 180 degrees, allowing the gripper to pass cartridges between the front storage bins and the back storage bins or tape drives. The extension actuator extends the gripper forward to make contact with the desired cartridge and then retracts the gripper to remove the cartridge from a bin or drive.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1137
3702

The gripper includes a Class II laser bar code scanner that reads up to 12-character, 3-of-9 format bar code labels. The scanner is used to maintain an inventory of the tape cartridges within the library. An inventory occurs automatically each time the library is turned on, or after the bulk load door has been closed. An inventory can also be initiated from the host computer.

Note: Although the library does not require tape cartridges to have bar code labels, properly labeled tape cartridges and full storage bins speed up the inventory process.

Tape Drives

The following sections describe the tape drive technologies supported by the library, including Ultrium and SDLT.

Caution: It is critical to ensure that the media you use matches the format of your tape drive. Cleaning cartridges and formatted data cartridges are unique for each drive technology. Damage may occur if inappropriate media is used in tape drives.

Note: If using mixed media, ensure your software application supports it.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1138
Doc: 3702

ECT
17.737
Cpl Paula
AC

Ultrium Tape Drives

The Ultrium tape drive is a high-performance streaming tape drive that uses Linear Tape-Open (LTO) technology. An Ultrium 230 tape drive is capable of storing up to 100 GB (native) or 200 GB (2:1 compression) of data per cartridge. An Ultrium 460 tape drive is capable of storing up to 200 GB (native) or 400 GB (2:1 compression) of data per cartridge. Access the *HP StorageWorks Ultrium Tape Drive User's Guide* from http://www.hp.com/support for more information about its features and capabilities.

The ESL9322 holds up to 8 Ultrium tape drives. The ESL9595 holds up to 16 Ultrium tape drives.

Note: *ESL9322:* When fewer than 8 Ultrium tape drives are installed, tape drives must occupy consecutive drive bays, beginning with drive bay 0. (See Figure 5 on page 25 for an illustration showing the drive numbering conventions.)

ESL9595: When fewer than 16 Ultrium tape drives are installed, tape drives must occupy consecutive drive bays, beginning with drive bay 0. (See Figure 6 on page 27 for an illustration showing the drive numbering conventions.)

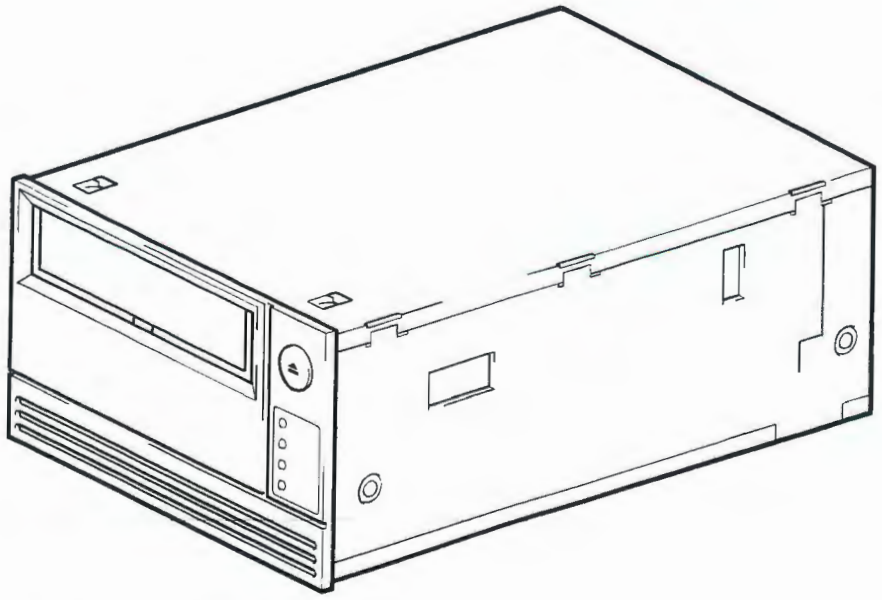


Figure 9: Ultrium tape drive

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1139
Nº 3702
Doc:

17736 Paula

Table 5: Ultrium Tape Drive Capacity and Data Transfer Rate

Drive Model	Data Capacity	Sustained Data Transfer Rate
Ultrium 230	100 GB (native) 200 GB (compressed*)	15 MB/sec (54 GB/hour) 30 MB/sec (108 GB/hour)
Ultrium 460	200 GB (native) 400 GB (compressed*)	30 MB/sec (108 GB/hour) 60 MB/sec (216 GB/hour)

Note: *Compressed capacity assumes a 2:1 compression ratio.

Ultrium Tape Cartridges

Note: In addition to the information provided in this manual, refer to the documentation provided with your media for more information.

Caution: HP Ultrium tape drives require special cleaning cartridges and data cartridges formatted specifically for HP Ultrium. To avoid damage to your tape drive, it is critical to use appropriate cleaning cartridges and properly formatted data cartridges.

Approved media will have the Ultrium format trademark, which indicates that the media has passed Ultrium format compliance testing (see Figure 10).

Figure 10: HP Ultrium format trademark

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1140
3702
Doc:

CPL 17735 Paula

For best results, always use HP branded media. The following tape cartridges are approved for the library's Ultrium tape drives:

- HP Ultrium Data Cartridge
  - — C7972A (400 GB)
  - — C7971A (200 GB)
- HP Ultrium Universal Cleaning Cartridge
  - — C7978A

Note: Ultrium generation 2 cartridges (C7972A) can read and write to Ultrium generation 1 cartridges (C7971A). However, Ultrium generation 1 cartridges can only read and write to other Ultrium generation 1 cartridges.

Caution: Do not bulk erase Ultrium formatted cartridges. This will destroy prerecorded servo information and make the cartridge unusable.

Make it a practice to visually inspect your tape cartridges when loading or removing them from your tape library. Taking a few minutes to check the condition of your cartridges will lower the risk of repeated failures and help ensure uninterrupted backup. See Maintaining Tape Cartridges on page 98 for general precautions when using tape cartridges.

Caution: Always discard damaged tape cartridges. If a defective tape cartridge is loaded into a tape drive, it may in turn damage the drive, potentially requiring drive replacement.

Note: For information on labeling tape cartridges, see Labeling Tape Cartridges on page 47. For information on ordering tape cartridges and bar code labels, refer to the ordering sheet that shipped with your library.

RQS nº 03/2005 - CN - CPMI - CORREIOS
1141
Fls Nº
3702
Doc:

SDLT Tape Drives

The SDLT tape drive is a high-capacity, high-performance streaming tape drive that uses Laser Guided Magnetic Recording (LGMR) technology to maximize the amount of data that can be stored on a tape. An SDLT 320 tape drive is capable of storing up to 160 GB (native) or 320 GB (2:1 compression) of data per cartridge. Access the *HP StorageWorks SDLT Tape Drive Reference Guide* from http://www.hp.com/support for more information about its features and capabilities.

The ESL9322 holds up to 8 SDLT tape drives. The ESL9595 holds up to 16 SDLT tape drives.

Note: *ESL9322:* When fewer than 8 SDLT tape drives are installed, tape drives must occupy consecutive drive bays, beginning with drive bay 0. (See Figure 5 on page 25 for an illustration showing the drive numbering conventions.)

ESL9595: When fewer than 16 SDLT tape drives are installed, tape drives must occupy consecutive drive bays, beginning with drive bay 0. (See Figure 6 on page 27 for an illustration showing the drive numbering conventions.)

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1142
3702
Doc:

E C
17.733
Paula
AC

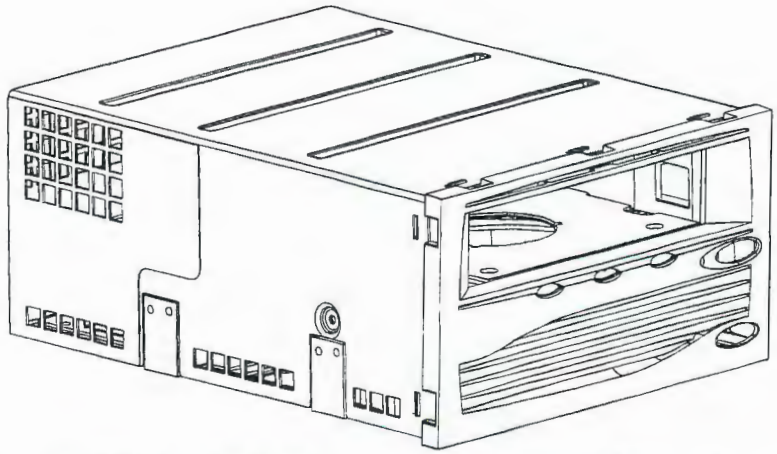


Table 6: SDLT Tape Drive Capacity and Data Transfer Rate

Drive Model	Data Capacity	Sustained Data Transfer Rate
SDLT 110/220	110 GB (native) 220 GB (compressed*)	11 MB/sec (39.6 GB/hour) 22 MB/sec (79.2 GB/hour)
SDLT 160/320	160 GB (native) 320 GB (compressed*)	16 MB/sec (57.6 GB/hour) 32 MB/sec (11.5 GB/hour)

Note: *Compressed capacity assumes a 2:1 compression ratio.

SDLT Tape Cartridges

Note: In addition to the information provided in this manual, refer to the documentation provided with your media for more information.

The following tape cartridges are approved for the library's SDLT tape drives:

- HP SDLT Data Cartridges:
  C7980A (220-320 GB)
- HP SDLT Cleaning Cartridge:
  C7982A

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1143
3702
Doc:

Caution: SDLT tape drives require special cleaning cartridges and data cartridges formatted specifically for SDLT. To avoid damage to your tape drive, it is critical to use appropriate cleaning cartridges, and properly formatted data cartridges. Do not use DLT Tape I, DLT Tape II, DLT Tape III, or DLT Tape IIIXT data cartridges, or DLT cleaning cartridges with SDLT tape drives.

Make it a practice to visually inspect your tape cartridges when loading or removing them from your tape library. Taking a few minutes to check the condition of your cartridges will lower the risk of repeated failures and help ensure uninterrupted backup. See Maintaining Tape Cartridges on page 98 for more information.

Caution: Always discard damaged tape cartridges. If a defective tape cartridge is loaded into a tape drive, it may in turn damage the drive, potentially requiring drive replacement.

Note: For information on labeling tape cartridges, see Labeling Tape Cartridges on page 47. For information on ordering tape cartridges and bar code labels, refer to the ordering sheet that shipped with your library.

Load Port

The load port is a mechanical device in the front panel of the library that lets you insert or export tape cartridges without interrupting library operations. (See Figure 1 on page 20 and Figure 2 on page 21.)

Optional Pass-Through Mechanism (PTM)

An optional PTM enables the transfer of a single tape cartridge between two HP StorageWorks ESL9000 Series tape libraries. The PTM can be used to connect up to five ESL9322 tape libraries or up to four ESL9595 tape libraries, increasing the storage capacity of the entire tape library system.

Note: To order a PTM, contact your HP sales representative.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1144
Nº 3702
Doc:

Optional Network Storage Router

HP StorageWorks Network Storage Routers provide bidirectional connectivity in a Fibre Channel Switched Fabric supporting Fibre Channel and SCSI devices. Internal and external models are available. For more information, visit http://www.hp.com/products/tapestorage, or contact your HP sales representative.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1145
Nº Doc: 3702

17730 Paulo AC

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1146
Nº Doc: 3702

Preparing the Library for Operation

2

This chapter explains how to prepare the HP StorageWorks ESL9000 Series tape library for operation. Sections in this chapter include:

- Opening the Library Doors and Access Panels, page 40
- Connecting SCSI Cables, page 41
- Preparing Tape Cartridges, page 47
- Inserting and Removing Tape Cartridges, page 53
- Turning the Library On and Off, page 57

Note: If you have a slot capacity upgrade for your library, ensure that you order the license key immediately. It may take 24 hours to receive the key.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1147
3702
Doc:

ECT 17728 Paula

Opening the Library Doors and Access Panels

The ESL9322 has one front door and one rear access panel. The ESL9595 has two front doors and three rear access panels.

To unlock and open front doors and rear access panels:

1. Using the key from the accessory kit, unlock the front door latch.
2. Lift the latch above the door lock.
3. Pull on the door latch to open the door, exposing the inside of the library cabinet.
4. Unlock any rear access panel using a 5/32 hex wrench.

Note: When the front doors are open, the robotics are disabled, but the library remains on-line. When the rear access panels are open, the robotics continue to work, but only at half speed.

Caution: Rear access panels must be closed during normal operation for proper cooling and proper operation of the bar code scanner.

To close and lock front doors and rear access panels:

1. Turn the door latch to secure the door to the library frame.
2. Lower the latch over the door lock.
3. Using the key from the accessory kit, lock the latch in place.
4. Close and lock any rear access panel using a 5/32 hex wrench.

RQS nº 03/2005 - CN - CPMI - CORREIOS
1148
Fls Nº 3702
Doc:

Connecting SCSI Cables

This section describes the supported SCSI cable configurations for the tape libraries.

ESL9322 SCSI Cable Configurations

Figure 11 shows the SCSI ports as viewed from the rear of the ESL9322 tape library.

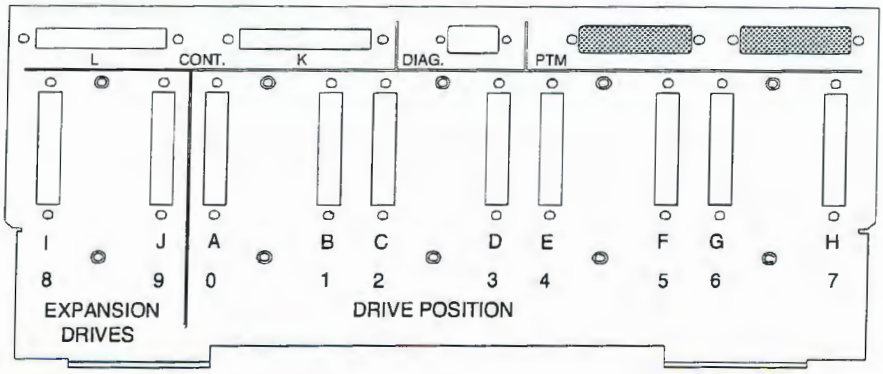


Figure 11: SCSI ports (ESL9322)

Looking from the rear of the ESL9322 tape library, connect the SCSI cables and terminators as shown in Figure 12.

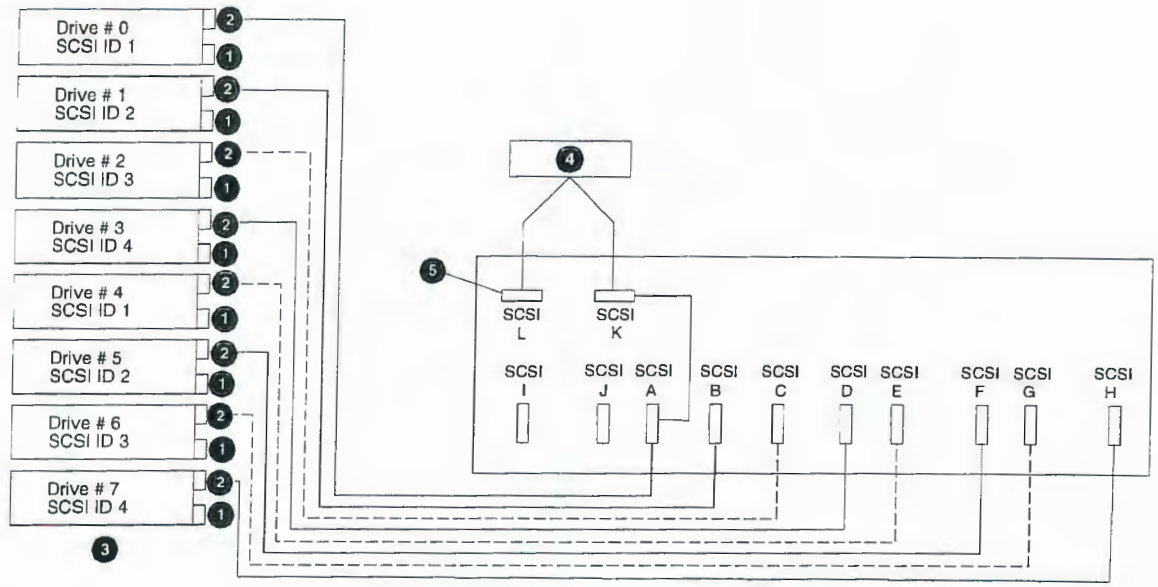
Note: ESL9322 series libraries are equipped with internal SCSI cables and terminators in place for a one drive per SCSI bus configuration. This is the recommended configuration (and the required configuration for Ultrium 460 drives) and ensures optimal performance.

Figure 12 shows the internal SCSI cabling. The connectors are on the SCSI ports that are shown in Figure 11 on page 41.

Note: Drive numbering begins with 0. Consequently, the first drive is drive 0, the second drive is drive 1, etc.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1149
Doc 3702

ECT
17726
Paula
CPL - AC



❶ Terminators (8)
❷ SCSI cables (8)
❸ Drive Column 1
❹ Robotic Controller
❺ Host SCSI Cable

Figure 12: Internal SCSI cabling configuration (ESL9322)

Table 7: SCSI Ports and Device Connections (ESL9322)

SCSI Port Identifier	Device Connection
A	Drive 0
B	Drive 1
C	Drive 2
D	Drive 3
E	Drive 4
F	Drive 5
G	Drive 6
H	Drive 7
I	Not used

RQS nº 03/2005 - CN -
CPMI - CORREIOS
1150
Fls Nº
3702
Doc

ECT 17725 Paula CPL - AC

Table 7: SCSI Ports and Device Connections (ESL9322) (Continued)

SCSI Port Identifier	Device Connection
J	Not used
K	Robot
L	Host

ESL9595 SCSI Cable Configurations

Figure 13 shows the SCSI ports as viewed from the rear of the ESL9595 tape library.

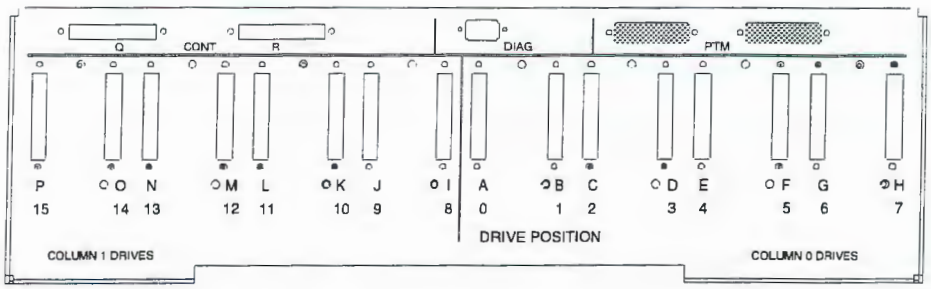


Figure 13: SCSI ports (ESL9595)

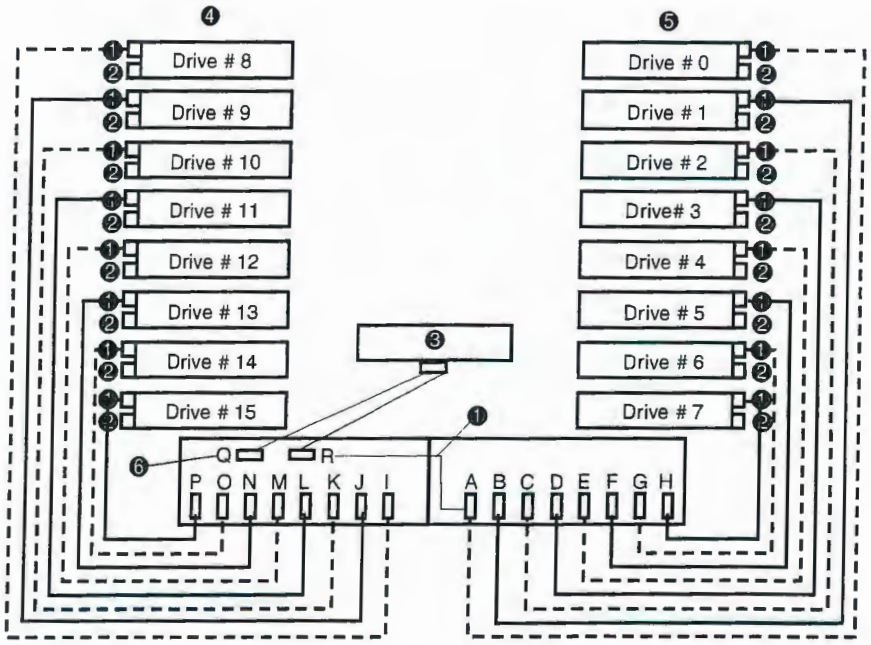
Looking from the rear of the library, connect the SCSI cables and terminators as shown in Figure 14.

Note: ESL9595 series libraries are equipped with internal SCSI cables and terminators in place for a one drive per SCSI bus configuration. This is the recommended configuration (and the required configuration for Ultrium 460 drives) and ensures optimal performance.

Figure 14 shows the internal SCSI cabling. The connectors are on the SCSI ports that are shown in Figure 13 on page 43.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1151
3702

Note: Drive numbering begins with 0. Consequently, the first drive is drive 0, the second drive is drive 1, etc.



❶ SCSI cables (16)
❷ Terminators (16)
❸ Robotic Controller
❹ Drive Column 1
❺ Drive Column 0
❻ Host SCSI Cable

Figure 14: Internal SCSI cabling configuration (ESL9595)

Table 8: SCSI Ports and Device Connections (ESL9595)

SCSI Port Identifier	Device Connection
A	Drive 0
B	Drive 1
C	Drive 2
D	Drive 3
E	Drive 4

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1152
3702
Doc:

E C T
17723
Paulo
CPL - AC

Table 8: SCSI Ports and Device Connections (ESL9595) (Continued)

SCSI Port Identifier	Device Connection
F	Drive 5
G	Drive 6
H	Drive 7
I	Drive 8
J	Drive 9
K	Drive 10
L	Drive 11
M	Drive 12
N	Drive 13
O	Drive 14
P	Drive 15
Q	Host
R	Robot

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1153
Doc: 3702

17723 Paulo CPL - AC

Default SCSI IDs

Table 9 lists the default SCSI IDs for the ESL9000 Series tape library.

Note: The ESL9322 holds a maximum of 8 tape drives, with tape drive 7 being the highest-numbered tape drive. The ESL9595 holds a maximum of 16 tape drives, with tape drive 15 being the highest-numbered tape drive.

Table 9: Default SCSI IDs

Drive #	Default SCSI ID
Tape Library	0
Drive 0	1
Drive 1	2
Drive 2	3
Drive 3	4
Drive 4	1
Drive 5	2
Drive 6	3
Drive 7	4
Drive 8	1
Drive 9	2
Drive 10	3
Drive 11	4
Drive 12	1
Drive 13	2
Drive 14	3
Drive 15	4

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1154
Doc: 3702

17.721 São Paulo CPL

Preparing Tape Cartridges

Caution: Handle tape cartridges with care. Do not drop or mishandle them, or place them near sources of electromagnetic interference. Rough handling can damage the cartridge, making it unusable and potentially hazardous to the tape drives.

Labeling Tape Cartridges

Caution: The misuse and misunderstanding of bar code technology can result in backup and restore failures. To ensure that your bar codes meet HP's quality standards, always purchase them from an approved supplier and never print bar code labels yourself. For more information, refer to the order form provided with the library, as well as the *Bar Code Label Requirements, Compatibility and Usage* white paper available from http://www.hp.com/support.

Note: For information on ordering tape cartridges and bar code labels, refer to the ordering sheet that shipped with your library.

Attaching a bar code label to each tape cartridge enables the library and application software to identify the cartridge quickly, thereby speeding up inventory time. Make it a practice to use bar code labels on your tape cartridges. Your host software may need to keep track of the following information and the associated bar code:

- Date of format or initialization
- Tape's media pool
- Data residing on the tape
- Age of the backup
- Errors encountered while using the tape (to determine if the tape is faulty)

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1155
Doc: 3702

17.720
Paula

SDLT Bar Code Labels

SDLT cartridges have a front slide slot located on the face of the cartridge next to the write-protect switch (❶ Figure 15). Use this slot for inserting the bar code label by sliding it into the slot.

Caution: Do not apply labels onto the top, bottom, sides, or back of the cartridge as this may cause damage to the tape drive, or interfere with reliable operation.

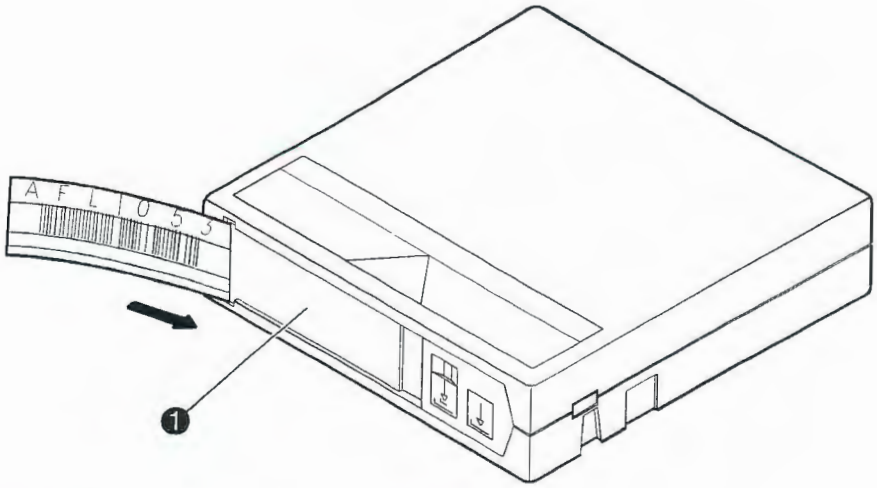


Figure 15: Inserting an SDLT bar code label

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1156
Nº Doc: 3702

Ultrium Bar Code Labels

Ultrium cartridges have a recessed area located on the face of the cartridge next to the write-protect switch. Use this area for attaching the adhesive-backed bar code label (see Figure 17). Do not apply labels onto the cartridge except in this designated area.

Caution: The bar code label should be applied as shown in Figure 19 with the alphanumeric portion facing the hub side of the cartridge. Never apply multiple labels onto a cartridge, because extra labels can cause the cartridge to jam inside a tape drive.

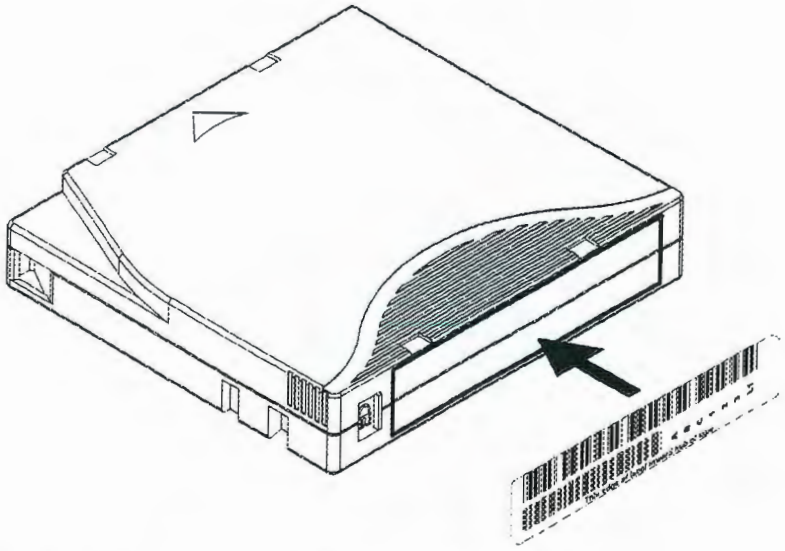


Figure 16: Attaching an Ultrium bar code label

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1157
Doc: 3702

For successful operation of your tape library, place the bar code label *entirely* within the recessed area, ensuring that no part of the label is outside of it (see Figure 17).

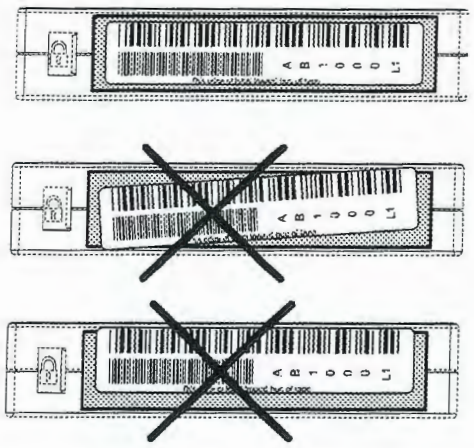


Figure 17: Proper Ultrium bar code label placement

Media Label Identifiers

Be sure to use the proper bar code labels for your drive technology. Table 10 lists the identifier that is found at the end of 7- or 8-character SDLT and Ultrium bar code labels.

Caution: To ensure that your bar codes meet HP's quality standards, always purchase them from an approved supplier and never print bar code labels yourself. For more information, refer to the order form provided with the library, as well as the *Bar Code Label Requirements, Compatibility and Usage* white paper available from http://www.hp.com/support.

Table 10: Media Label Identifiers

Cartridge Type	Density	Label Identifier
SDLT	110/220 GB	S or S1
SDLT	160/320 GB	S or S2
Ultrium 230	100/200 GB	L1
Ultrium 460	200/400GB	L2

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1158
Doc: 3702

Setting the Write-Protect Switch

Each tape cartridge has a sliding write-protect switch. This switch determines whether new data can be written to the tape cartridge (write-enabled) or whether data on the tape cartridge is protected from being erased or overwritten (write-protected).

Write-Protecting SDLT Tape Cartridges

By moving the switch to the left (Figure 18), the tape cartridge is write-protected (orange indicator is visible). By moving the switch to the right (Figure 18), the tape cartridge is write-enabled (orange indicator is not visible).

Moving the write-protect switch to the left while the tape cartridge is in the SDLT tape drive causes the red indicator to immediately light up. If the tape drive is writing data to the tape cartridge, write-protect does not begin until the current write command completes.

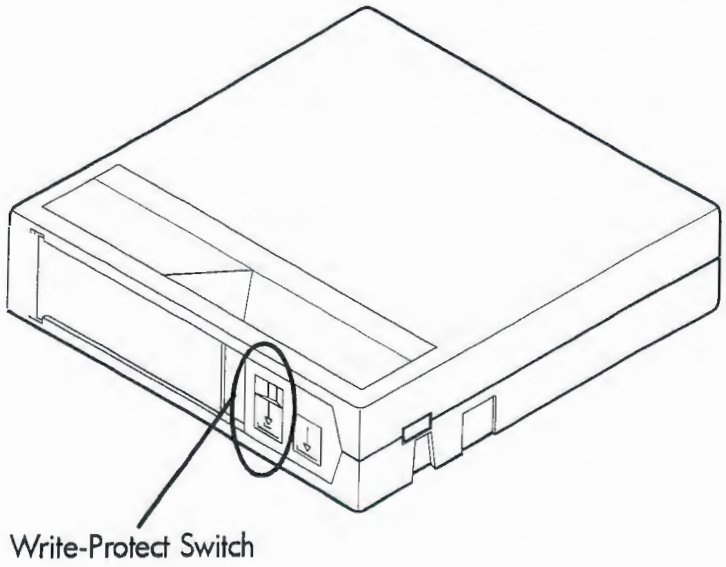


Figure 18: Write-protecting SDLT tape cartridges

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1159
Doc: 3702

17.746 Paula CPL

Write-Protecting Ultrium Tape Cartridges

By moving the switch to the left(❷ Figure 19), the tape cartridge is write-enabled. By moving the switch to the right(❸ Figure 19), the tape cartridge is write-protected.

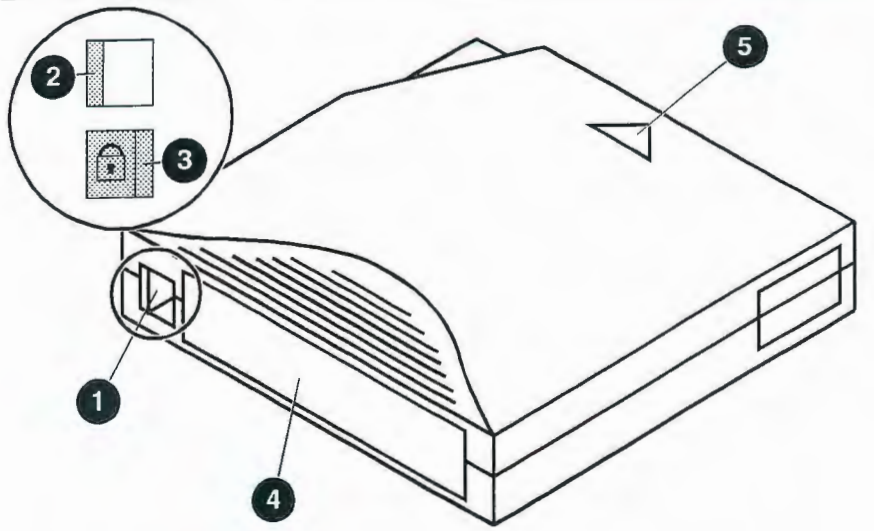


Figure 19: Write-protecting Ultrium tape cartridges

❶ Write protect switch
❷ Write-enabled
❸ Write-protected
❹ Bar code label
❺ Insertion arrow

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1160
3702
Doc

17715
CPL Paula - AC

Inserting and Removing Tape Cartridges

You can insert tape cartridges by:

- Placing them into fixed storage bins within the library cabinet
- Using the load port on the library front panel

Placing Tape Cartridges into Fixed Storage Bins

1. Label the tape cartridge (see Labeling Tape Cartridges on page 47).
2. Set the write-protect switch (see Setting the Write-Protect Switch on page 51).
3. Open the library front door(s) and place a tape cartridge in each fixed storage bin along the back wall of the library and on the inside of the front door(s). Be sure all cartridges are properly oriented. They must be seated in the bins, with the bar codes facing out.

Note: Each cartridge should slide into place with very little force. If a cartridge does not slide into place easily, check the cartridge for correct orientation and structural integrity.

Caution: Handle tape cartridges with care. Do not drop or mishandle them. Rough handling can damage the tape cartridge, making it unusable and potentially hazardous to the tape drives.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1161
Doc 3702

Using the Load Port

This section explains how to insert tape cartridges using the load port mechanism.

Note: To move cartridges to the load port for removal, see "Moving Cartridges" in Chapter 4.

To use the load port:

1. Prepare the tape cartridges to be inserted by affixing a bar code label, and write-protecting or write-enabling each tape cartridge as desired.
2. Press the **Load Port** button on the control panel. The library unlocks the load port.
3. Pull the load port handle toward you. It will move outward about 1 inch (2.54 cm) and enable the load port to be rotated 180 degrees.
4. With the load port door open, place the tape cartridge in an available magazine slot (see Figure 21 on page 56).

WARNING: Opening or closing the load port door presents mechanical hazards. Use both hands to pull or push the load port finger grip, and use the top and bottom surfaces of the load port drum to keep fingers out of load port openings when rotating the load port drum.

5. After loading the magazines, rotate the load port back 180 degrees, and push the load port handle to lock the load port into position.

If **Auto Load** is enabled, the library automatically moves the cartridges to the available storage bins.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1162
3702
Doc:

ECT 17 713 Paula L - A

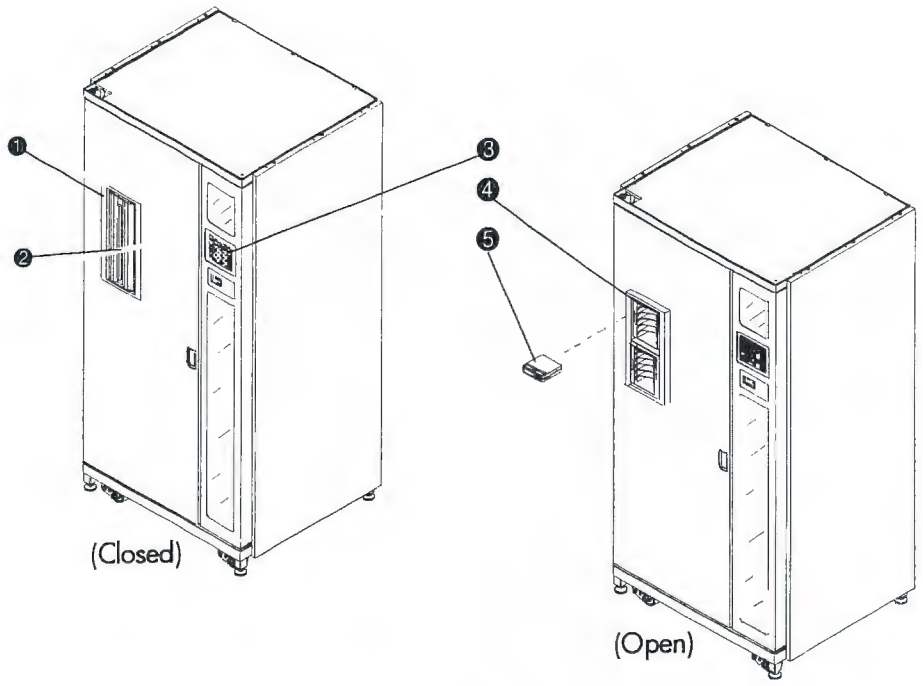


Figure 20: Load port (ESL9322 shown)

❶ Load port
❷ Load port handle
❸ Load port button (control panel)
❹ Magazine
❺ Tape cartridge

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1163
Doc: 3702

Using the Load Pack Magazine

Use the load pack to add and remove tape cartridges.

Adding a Cartridge to a Magazine

The 4-cartridge magazines are stationary and built into the load port. Simply place cartridges into the bins with the bar codes facing out (see Figure 21):

1. Access the load pack magazines by opening the load port (see Using the Load Port on page 54).
2. Insert a tape cartridge into a load pack magazine.
3. Slide the tape cartridge in until you hear it snap into place.

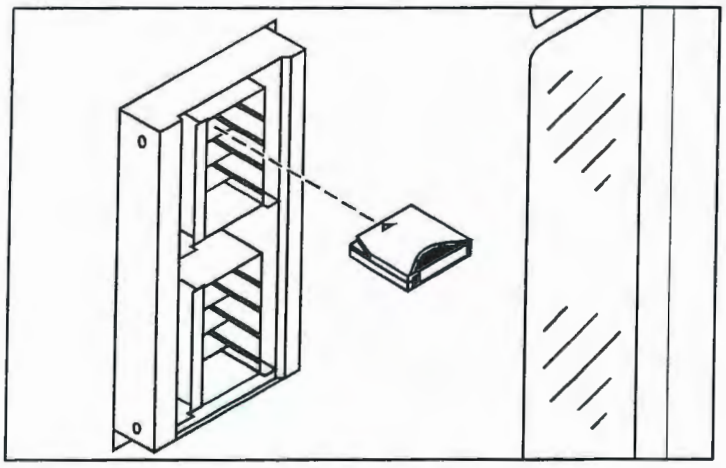


Figure 21: Inserting a tape cartridge into a magazine

Removing a Cartridge from a Magazine

To remove a tape cartridge from a load pack:

1. Push the tape cartridge in until you hear a snap.
2. Eject the tape cartridge.
3. Remove the tape cartridge.
4. Close the load port.

RQS nº 03/2005 - CN - CPMI - CORREIOS
1164
Fls Nº
3702
Doc:

Turning the Library On and Off

Turning the Library On

To turn the library on:

1. Verify that:
   a. All front doors and access panels are closed.
   b. All back panel cable connections are firmly in place.

Note: If there are two AC power distribution assemblies, there will be two main circuit breakers.

---

2. Ensure that CB1 on the AC distribution assembly is turned on. It is located in the base of the cabinet behind the rear access panel. If two AC distribution assemblies are present, turn on CB1 for both assemblies.
3. Turn on the power switch located below the control panel.
4. After several seconds, the control panel becomes active and the **Home** screen appears. The POST routine and inventory routine also run. These routines can take up to nine minutes to complete.

Placing the Library On-line or Off-line

With library turned on, press the **Standby** button on the control panel. Pressing the **Standby** button toggles the library between on-line and off-line states.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1165
Doc 3702

E C T
1710
Paula

Turning the Library Off

To turn the library off:

1. Place the library off-line by pressing the **Standby** button. The library robotics complete any current commands and then stop.
2. Verify that the control panel display shows **System Off-line**.
3. Verify that the gripper is empty by checking the **Overview** screen on the control panel (see Chapter 3). If there is a tape cartridge in the gripper, perform a **Move** command to place the cartridge in an available storage bin.
4. Turn off the power switch located below the control panel.
5. Turn off both circuit breakers on the AC power distribution assembly.

Note: Wait 10 seconds before turning on the power switch again.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
1166
Fls Nº
3702
Doc:

CPL - AC 17.709 Paula

Operating the Control Panel

3

This chapter provides an overview of the control panel and operating procedures. Sections in this chapter include:

- Using the Control Panel, page 60
- Obtaining Library Status, page 66
- Changing the Control Panel Security Levels, page 70

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1167
Doc: 3702

Using the Control Panel

The control panel is activated by touching the screen, and is located at the front of the library. The menus displayed on the control panel let you obtain information about the library, execute library commands, and test library functions. The control panel functions are grouped into the following categories (see Figure 22):

- **Overview** screen—Displays current tape drive, gripper, and load port content and activities.
- **Tapes** screen—Displays tape drive, storage bin, load port, and gripper inventories.
- **Operator** screen—Contains library configuration and control functions (password protected).
- **Service** screen—Contains reporting functions, system tests, and service commands (password protected).
- **Multi-Unit** screen—Contains multi-unit configuration and calibration commands (password protected).
- **License** screen—Lets you enter an upgrade key to access additional bins.

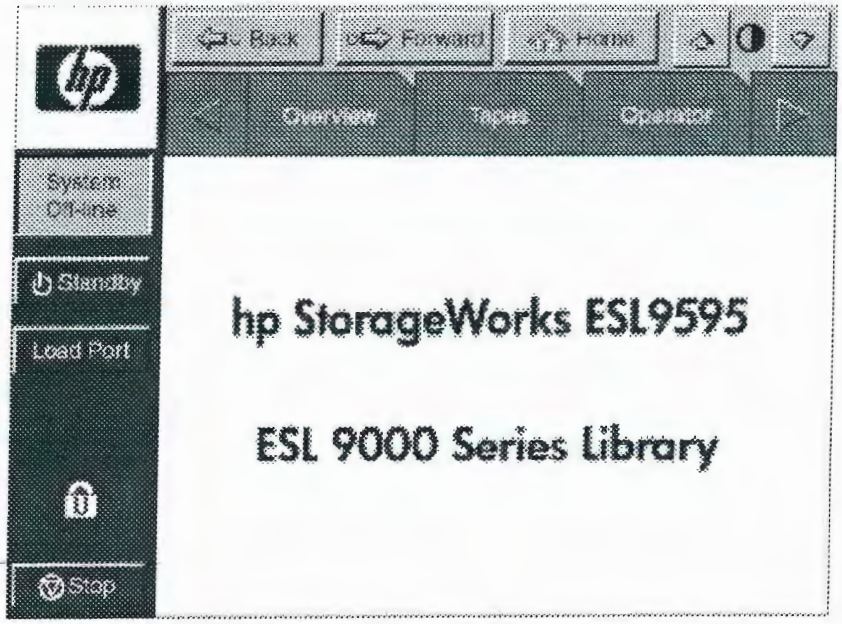


Figure 22: Control panel home screen (ESL9595 shown)

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1168
3702

CPL - AC 1707 Paula

Table 11 lists the control panel menus and their functions.

Table 11: Control Panel Menus

Overview Screen	Tapes Screen	Operator Screen[1]	Service Screen[1]	Multi-Unit Screen[1]	License Screen
Status ■ Tape drives ■ Activity ■ Load port	Inventory ■ Tape drives ■ Storage bins ■ Load port ■ Transport (GRP)	Configure ■ Configure library ■ Configure options ■ Error log Control ■ Move cartridges ■ Inventory tapes ■ Calibrate library ■ Unload drive ■ Unload imp/exp	Reports ■ Statistics ■ Actuator ■ SysTest Library results ■ Auto clean ■ System monitor Miscellaneous ■ SysTest Library ■ Enable/Disable COD ■ Initialize nonvol statistics ■ Initialize nonvol config ■ Change password	Configure/ Calibrate ■ Configure Multi-Unit ■ Calibrate all PTMs	Configure ■ License

[1] The Operator, Service and Multi-Unit screens are password protected.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1169
Doc: 3702

Table 12 describes the control panel navigation features.

Table 12: Control Panel Navigation

Component	Name	Function
Horizontal bar	**Back** button	Moves you backwards screen by screen, through previous menu selections.
	Forward button	Moves you forward screen by screen, through previous menu selections.
	Home button	Redisplays you to the initial control panel screen.
	Contrast buttons	Lets you adjust the contrast of the control panel screen.
Vertical bar	HP logo	Displays service information and **Robotic Firmware** level.
	Status window	Displays the current state of the library and important messages relating to library operation.
	Standby button	Switches the library between on-line and off-line.
	Load Port button	Unlocks the load port so you can open it to access the magazines.
	Security level indicator	Shows the security level (five possible levels) in use at the control panel.
	Stop button	When pressed once, halts all library activity by cutting off power to the library robotics. When pressed a second time, restores power to the library robotics.
Display area	**Overview** screen	Displays the current tape drive, gripper, and load port content and activities.
	Tapes screen	Displays tape drive, storage bin, load port, gripper inventories, and PTM.
	Operator screen	Contains library configuration and control functions. To use this screen, you must have either operator or service-level access privileges.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1170
Doc 3702

Table 12: Control Panel Navigation (Continued)

Component	Name	Function
	Service screen	Contains reporting functions, system tests, and service commands. To use this screen, you must have service-level access privileges.
	Multi-unit screen	Lets you set the library unit, library unit number, number tape libraries, and Calibrate PTM.
	License screen	Lets you enter a software key to access additional bins.

Basic Operation

Touching the screen activates the control panel.

Opening a Screen

To open one of the main screens, touch the appropriate tab at the top of the control panel. The **Overview** and **Tapes** screens are accessible by anyone. The **Operator**, **Service**, and **Multi-Unit** screens require a password.

After the desired screen appears on the control panel, you can view information or press buttons to execute commands and open other screens.

Navigating from Screen to Screen

Three buttons let you move backward and forward through screens you have already opened.

- **Back** button—Moves backward screen by screen through previous selections.
- **Forward** button—Moves forward screen by screen through previous selections.
- **Home** button—Returns to the home screen.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1171
Doc: 3702

Exiting a Screen

To exit any screen, press the **Back** or **Home** button.

If a command is executing, the control panel displays a **Command In Progress** dialogue box with an **Abort** button. Pressing **Abort** cancels the command and stops the ongoing operation. After you press **Abort**, you must still press the **Back** button to exit the screen associated with the aborted command.

Library Controls

Library controls are located along the top and left side of the control panel in the horizontal and vertical bars (see Figure 23 on page 64).

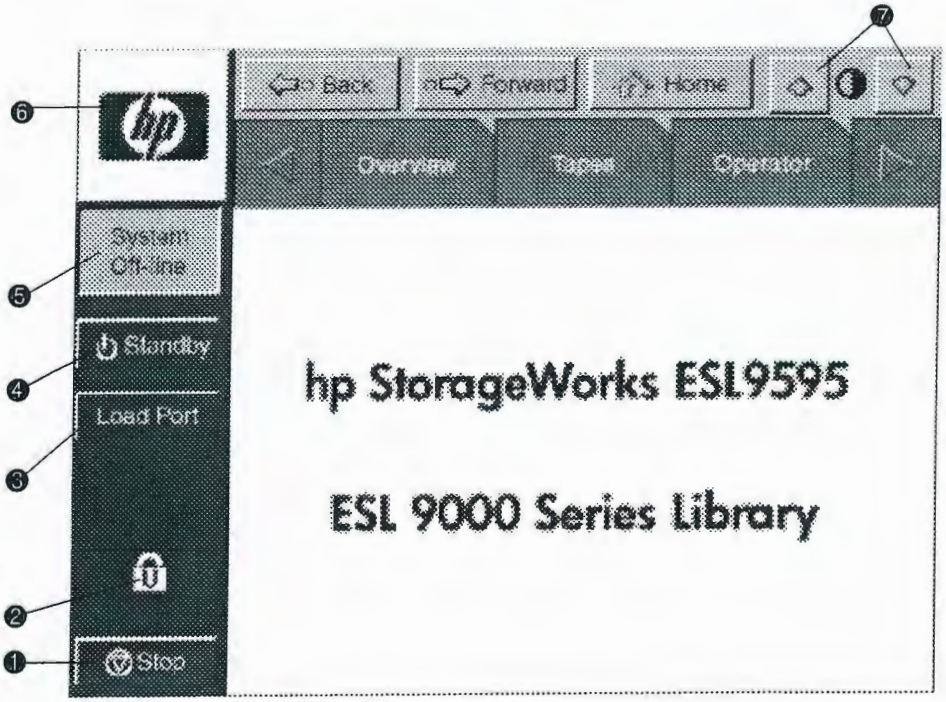


Figure 23: Library controls (ESL9595 shown)

❶ Stop button — Halts library activity immediately by cutting power to the library robotics. Pressing the **Stop** button a second time restores power to the library robotics.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1172
Doc 3702

❷ Lock icon	Shows the current security level at the touch screen GUI. Five security levels are available: **service** (S), **operator** (O), **user** (U), **import only** (I), and **locked** (L). Table 13 on page 65 lists the attributes of each security level.
❸ **Load Port** button	Releases and locks the load port door. If the load port is locked in the closed position, pressing this button releases the load port and then locks the door. If the load port is locked in the open position, pressing this button unlocks the load port, letting you rotate the load port to the closed position where it automatically locks.
❹ **Standby** button	Toggles the library between on-line and off-line states.
❺ **System State** display	Shows the current state of the library (**system on-line**, **system off-line**, **system stopped**, **door open**, and so on).
❻ HP logo	Displays service information and the library firmware level.
❼ Contrast buttons	Adjusts the contrast of the control panel.

Table 13 lists the security levels for the library.

Table 13: Security Levels, Highest to Lowest

Level	Password Protected	Overview Screen Access	Tapes Screen Access	Operator Screen Access	Service Screen Access	Load Port Access	Stop and Standby Access
Service	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Operator	Yes	Yes	Yes	Yes	No	Yes	Yes
User	Yes	Yes	Yes	No	No	Yes	Yes
Multi-unit	Yes	No	No	No	No	No	No
Import only	Yes	Yes	Yes	No	No	Yes	No
Locked	No	Yes	Yes	No	No	No	No

Note: The default passwords are: **Operator** screen -- **1234**, **Service** screen -- **5678**, **User** screen -- **2222**, **Multi-unit** screen --**1234**, and **Import only** screen -- **1111**.

For more information on password and security levels see "Changing the Control Panel Security Levels" on page 70.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1173
3702
Doc:

Obtaining Library Status

The **Overview** and **Tapes** screens on the control panel provide library status. The **Overview** screen displays a snapshot of the tape drive, robot activity, and load port inventory (see Figure 24). The **Tapes** screen displays the inventory of all elements in the library (see Figure 25 on page 68).

To display the **Overview** or **Tapes** screen, press the appropriate option on the control panel. Note that these functions operate in **On-line** or **Off-line** modes.

Overview Screen

The **Overview** screen provides the following information:

- Drive status
- Activity
- Load port content and status

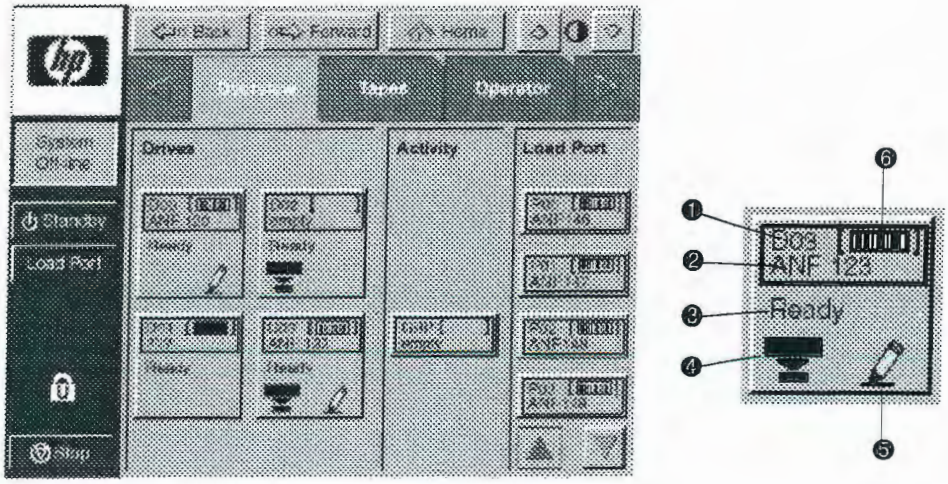


Figure 24: Overview screen

❶ Element number
❷ Bar code number
❸ Element status
❹ Compressed-enabled
❺ Write-enabled
❻ Cartridge present

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls- Nº 1174
Nº 3702
Doc:

Drive Status

The **Drives** area reports whether or not:

- A tape drive has a cartridge
- The cartridge is write-enabled or write-protected
- Compression is enabled

It also provides status for:

- Bar code labels
- Drive states
- Drive types
- Media types
- Drive serial numbers
- Drive firmware level
- Controller firmware level
- SCSI IDs
- Drive cleaning

For a more detailed view of drive status, press on the desired drive to display the **Tape Drive Status** box (see Figure 25 on page 68). Use the arrow buttons at the bottom of the box to scroll to other drives, if desired. To return to the **Overview** screen, press the screen anywhere in the **Tape Drive Status** box, or press the **Back** button (see Figure 25 on page 68).

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1175
Doc: 3702

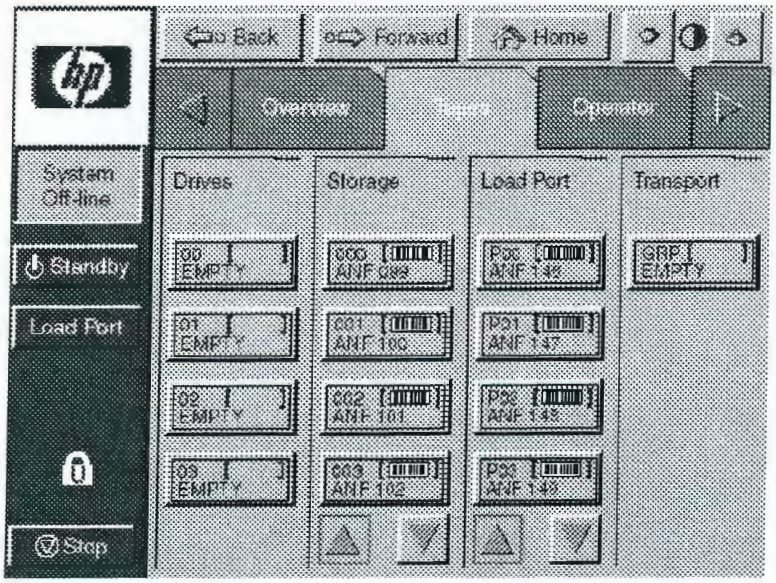


Figure 25: Tape drive status box

Activity Status

The **Activity** area shows the source element, the transport medium, and the destination element involved in the activity. It also shows the current location of the tape cartridge and the progress of the activity.

Load Port Status

The **Load Port** area identifies tape cartridges currently stored in either magazine in the load port. Use the arrow button to view contents not currently displayed.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1176
Nº Doc: 3702

Tapes Screen

The **Tapes** screen identifies the tape cartridges residing in the following elements (see Figure 3-5):

- **Drives**
- **Storage** (fixed storage bins)
- **Load Port**
- **Transport** (gripper), and PTM

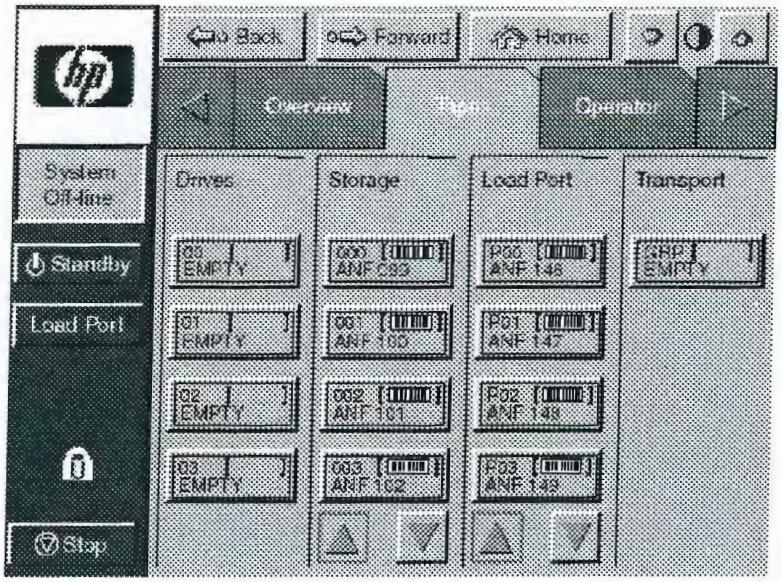


Figure 26: Tapes screen

Viewing Storage and Load Port Elements

The **Drives**, **Storage**, and **Load Port** categories might contain too many elements to display at once. To scroll through these elements, use the arrow buttons at the bottom of each category.

You can also expand the **Drives**, **Storage**, or **Load Port** list by touching a specific category. To return to the start of the **Tapes** screen, press the **Back** button.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1177
3702

Changing the Control Panel Security Levels

ESL 9000 Series library control panels have five levels of security:

- **Operator (O)**—Provides access to the **Operator** set of screens and all functions on the system bar.
- **Service (S)**—Provides access to both the **Operator** and **Service** set of screens and all functions on the system bar.
- **User (U)**—Provides access to screens that are not password protected (**Overview** and **Tapes** screens) and all functions on the status bar.
- **Import Only (I)**—Provides access to **Overview** and **Tapes** screens and the **Load Port** button on the system bar (no **Stop** or **Standby**).
- **Locked (L)**—Provides access to **Overview** and **Tapes** screens only.

The security level indicator (lock icon) at the lower left corner of the control panel indicates the current security level (**O**, **S**, **U**, **I**, or **L**).

Securing the Control Panel

When the **User** security level is set, access is restricted to the **Operator** and **Service** screens. Because these screens control library configuration, testing, and initializing functions, the **User** security level is the appropriate default condition for routine library operation.

For more information about changing to a higher security level to access the **Operator** or **Service** screens, see "Opening the Operator Screen" in Chapter 4.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1178
3702

Changing Security Levels

To change security levels:

1. Press the **Lock** icon. The **Password** screen is displayed (see Figure 27).

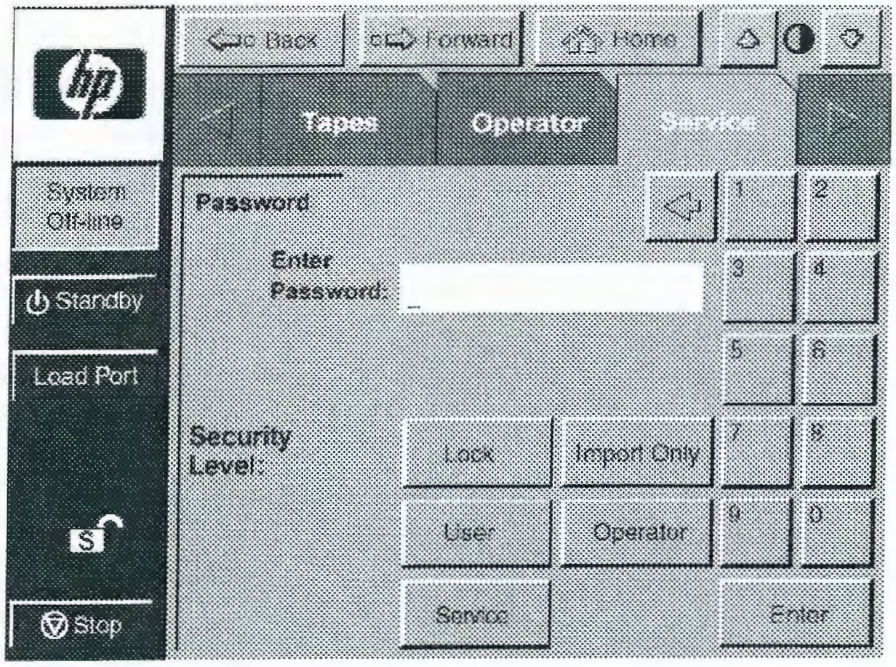


Figure 27: Change password screen

2. Press the **Security Level** button for the desired level of security (**Operator**, **Service**, **User**, **Import Only**, or **Locked**).
3. Enter a password if necessary. A password is required to enter a higher security level than the current level.
4. Press the **Enter** button. A new screen verifies that the new security level has been set successfully.
5. Press **OK**. The lock icon displays the new security level (**O**, **S**, **U**, **I**, or **L**).

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1179
3702
Doc:

17696

Note: This procedure is especially useful to change from the **Operator** or **Service** levels to the **User** level after executing an **Operator** or **Service** level command.

If the control panel is accessed from the **Operator** (**O**) or **Service** (**S**) level, and no activity has occurred for 15 minutes, it will return to the initial screen (Figure 22 on page 60), and to the default security level.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1180
3702

17.695

Operator Commands

4

This chapter describes the commands found on the **Operator** screen of the library control panel. Sections in this chapter include:

- Opening the Operator Screen, page 74
- Configuring the Library, page 76
- Configuring Library Options, page 79
- Calibrating the Library, page 83
- Performing an Inventory, page 84
- Moving Cartridges, page 85
- Unloading a Drive, page 87
- Unloading the Load Port, page 88

Note: The library must be off-line to perform any of the functions listed above. To change the library status, press the **Standby** button on the control panel.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1181
3702

Opening the Operator Screen

To open the Operator screen:

1. Press the **Operator** tab. The control panel displays the password screen (see Figure 28).

Note: To change passwords, see "Changing Security Levels" on page 71.

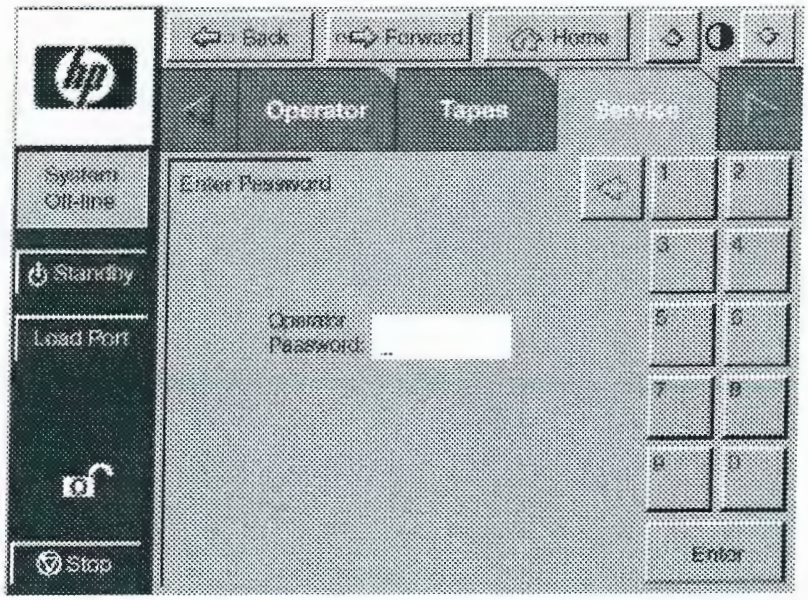


Figure 28: Operator password screen

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1182
Nº 3702
Doc:

2. To gain access to the **Operator** screen, enter the correct operator or service password and press **Enter** (see Figure 29 on page 75). The default operator password is 1234.

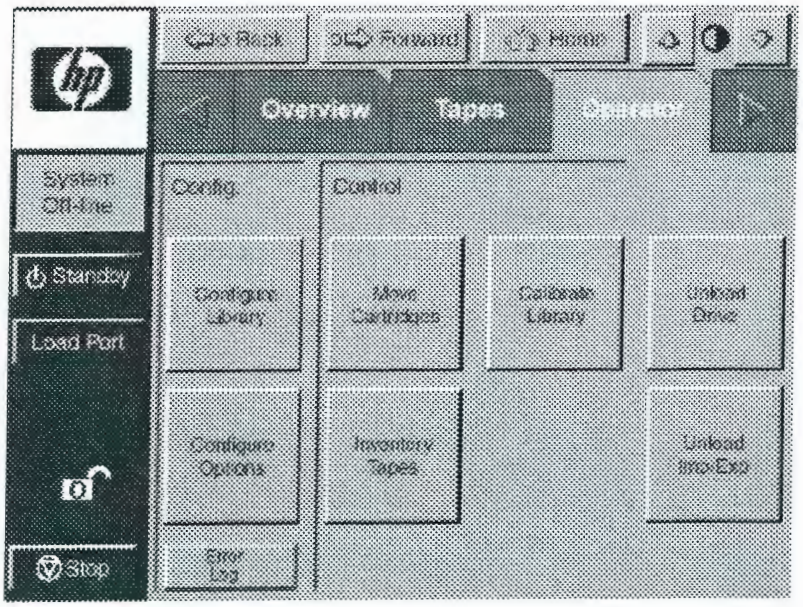


Figure 29: Operator screen

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1183
3702
Doc:

Configuring the Library

The **Configure Library** command lets you assign the following:

- Library model number
- Number of storage bins
- Number of drives
- Library SCSI ID
- Tape drive SCSI ID
- PTM configuration

Note: The serial number and IEEE ID fields are set automatically through the library firmware.

To configure any of these attributes:

1. In the **Operator** screen, press the **Configure Library** button. The control panel displays the **Configure: Library** screen (see Figure 30).

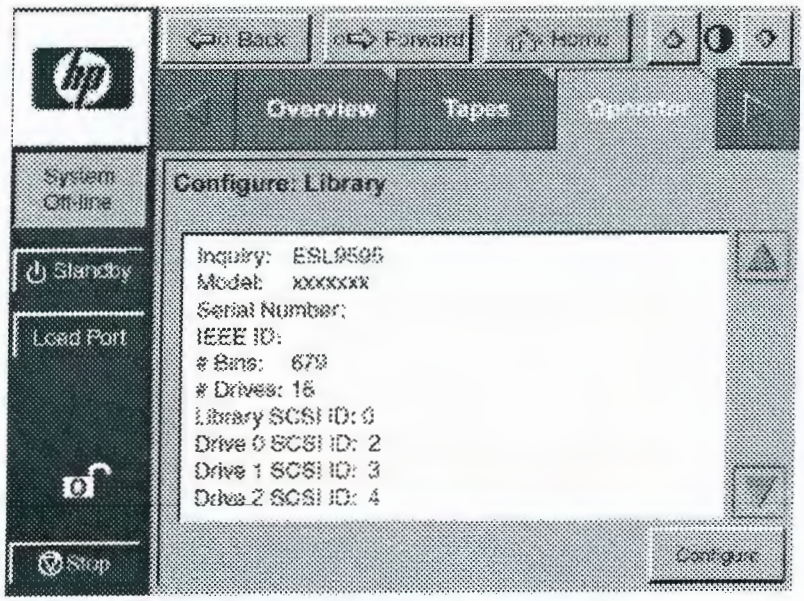


Figure 30: Configure: library screen (ESL9595 shown)

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1184
3702

2. Press the **Configure** button. The control panel displays the **Configure: Library Settings** screen (see Figure 31). Make sure that the library is off-line.

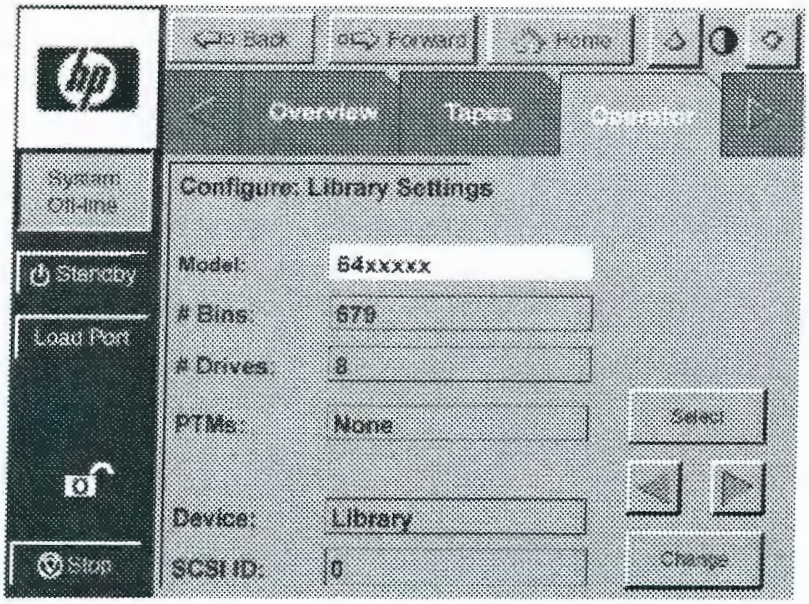


Figure 31: Configure: library settings screen (ESL9595 shown)

3. Press the **Select** button until you highlight the setting you want to change.
4. Using the arrow buttons, scroll through the available values for the setting.
5. Press the **Change** button to accept the new value.
6. Repeat step 3 through step 5 to make other changes.
7. Press the **Back** button to return to the **Configure: Library** screen.

The options you selected are now part of the library configuration.

Note: Not all model numbers are available from the GUI. If you are unable to find a particular model number, refer to the configuration menu in the ESL LibDiag serial diagnostics tool, which must be used to set the model number. Access LibDiag from http://www.hp.com/support.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1185
3702
Doc

Caution: The model number is set at the factory and should be changed only at the direction of an authorized service representative.

SCSI ID Assignment Guidelines

When selecting SCSI ID numbers, each SCSI device on the same bus must have a unique number from 0 to 15. SCSI devices include the library robotics, the host bus adapter, and the library tape drives.

If you set up the library with multiple SCSI buses, you can assign the same number to two or more devices, provided each device is on a different SCSI bus.

Note: Power must be cycled for the new SCSI ID number to become effective.

PTM Configuration

To configure the optional PTM, refer to the *HP StorageWorks ESL9000 Series Pass-Through Mechanism Installation Guide* that shipped with the PTM.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1186
Doc 3702

17.689

Configuring Library Options

The **Configure Options** command lets you set the following:

- **Power-On State**—Determines whether the library is on-line or in standby mode when powered up (default is **On-Line**).
- **Auto Clean**—Allows the library to perform drive cleaning tasks automatically as needed (default is **Disable**).

Note: Cleaning should be done using your backup application software. Backup application software must be compatible with the library auto clean feature to avoid robot command conflicts. HP does not support preventive autocleaning operation.

- **Retries**—Causes the library to retry a failed command automatically before issuing an error message (default is **Enable**).
- **Barcode Labels**—Turns bar code scanning on or off during inventory. This option should be disabled when the library contains cartridges that are not labeled (default is **Enable**).
- **Auto Inventory**—Causes the library to perform an inventory whenever the library is powered up (default is **Enable**).

Note: Before changing the **Auto Load** configuration option, check the recommendations of your software application. It may need to manage tape importing and exporting to maintain an accurate inventory.

- **Auto Load**—Causes the library to automatically move cartridges in the load port to empty storage bins as soon as the load port door closes (default is **Disable**).
- **Temp. Detection**—Enables or disables the over-temperature detection warning and shutdown features of the library (default is **Enable**).
- **Power-On Security**—Determines the library security level when powered up (default is **User**).

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1187
Doc: 3702

Note: Before changing the **Auto Drive Unload** configuration option, check the recommendations of your software application.

- **Auto Drive Unload**—Causes the drive to unload a tape when a **Move Medium** command is received (default in **Enable**).
- **Barcode Retries**—Lets you set a number of attempts to read a bar code label before giving up (default is **8**).
- **Set StorageWorks Defaults**—Returns all configure options to factory default states.

Configuring a Library Option

To configure a library option:

1. From the **Operator** screen, press the **Configure Options** button. The control panel displays the **Configure: Options** screen (see Figure 32).

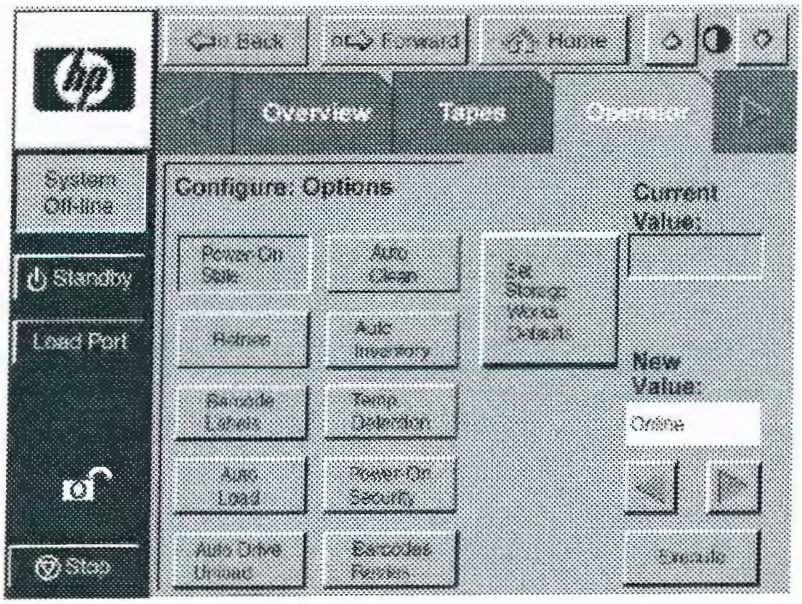


Figure 32: Configure: options screen

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1188
3702
Doc:

17.687

2. Press the button for the desired option.
3. Using the arrow buttons, scroll through available values for the selected option.
4. When the **New Value** box displays the desired value, press the **Execute** button to apply the new value. The **Current Value** box displays the new value.
5. Repeat step 2 through step 4 to change other configuration options.
6. When you have finished making changes to library options, press the **Back** button until you return to the initial **Operator** screen.

To return the library to the default values press the **Set StorageWorks Defaults** button.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1189
3702
Doc:

Viewing the Error Log

The library error log records library errors and the time they occurred (see Appendix C for a listing of the error codes and descriptions). Because the library has no system clock, the time stamps indicate uptime since the last power cycle.

Note: At the time an error occurs, the control panel will indicate the error, along with a description of the error. After the error has been cleared, it can still be viewed from the error log.

To view the error log:

1. From the **Operator** screen, press the **Error Log** button.
2. Using the arrow buttons, scroll through the available information.
3. To exit the error log, press the **Back** button to return to the initial **Operator** screen.

Note: The error log provides SCSI sense data values and is a valuable diagnostics tool for your authorized service provider.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1190
3702
Doc:

Calibrating the Library

The **Calibrate Library** command lets you calibrate the storage bins, the tape drives, the load port, or the entire library. Calibrate the library during initial installation and after any maintenance procedure.

To calibrate library elements:

1. From the **Operator** page, press the **Calibrate Library** button. The control panel displays the **Calibrate Library** screen (see Figure 33).
2. Press the button for the calibration option you want.

Note: Pressing the Calibrate All button causes the drives, bins, and the load port to be calibrated. This operation takes approximately 20 minutes.

The control panel displays a **Command In Progress** screen while the calibration process is in progress.

3. When the calibration process is complete, repeat step 2 to perform another calibration, if desired.

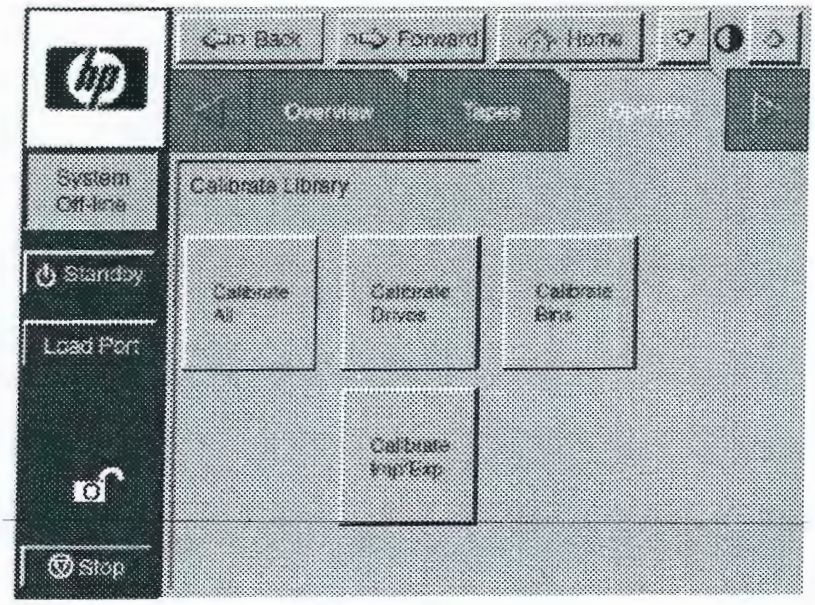


Figure 33: Calibrate library screen

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1191
3702

Performing an Inventory

The **Inventory Tapes** command reads the bar code labels of the cartridges in the tape drives, fixed storage bins, and the load port bins. All elements that contain cartridges without labels are marked as full with no label.

To perform an inventory:

1. Press the **Inventory Tapes** button in the **Operator** screen. The control panel displays a **Command In Progress** screen.
2. Press the **Abort** button to stop continuous running of the inventory process. Otherwise, the process will continue until all storage elements have been inventoried.

Note: The inventory process is also stopped if an error is detected or if the rear door is opened. In this case, the control panel displays an error message.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1192
Doc: 3702

Moving Cartridges

The **Move Cartridge** command lets you move any tape cartridge in the library to the destination you specify. This destination can be a storage bin, a tape drive, the load port, the gripper, or the PTM.

Note: To move a cartridge from a tape drive when auto-drive unload is disabled, issue an **Unload Drive** command. (See "Unloading a Drive" on page 87.)

To move a cartridge:

1. From the **Operator** screen, press the **Move Cartridge** button. The control panel displays the **Control: Move Cartridge** screen, with the **Source** input field active (see Figure 34).

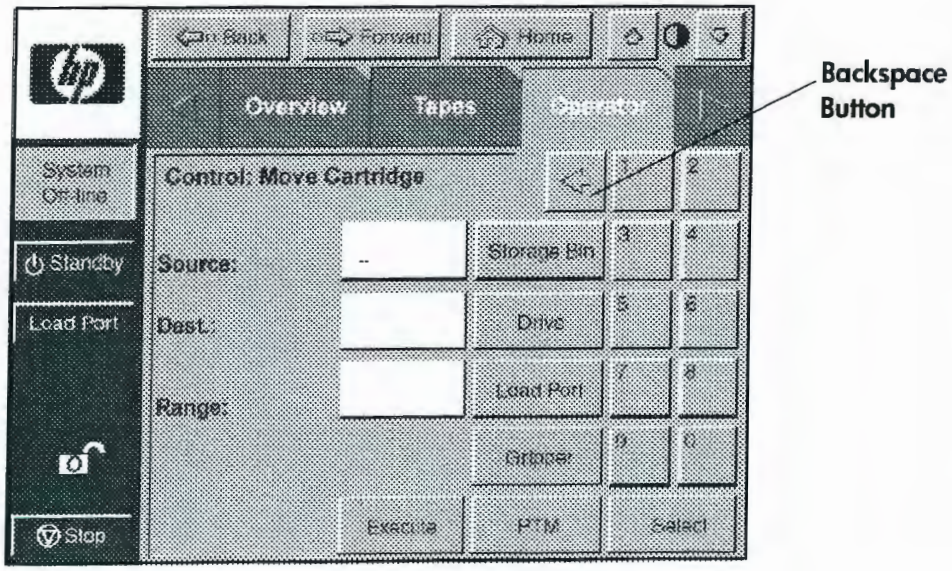


Figure 34: Control: move cartridge screen

Note: Use the backspace button to erase a partial entry character by character (❶ Figure 34).

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1193
Doc: 3702

2. Identify the source element of the cartridge:
   a. Press the appropriate source element button (**Storage Bin**, **Drive**, **Load Port**, **Gripper**, or **PTM**). When you press an element type, the **Range** box (below the **Dest.** box) displays the range of addresses.
   b. Using the keypad, enter the address of the source element and then press the **Select** button. The **Source** information is displayed in the **Source** box and the **Dest.** box becomes active.
3. Identify the destination for the cartridge:
   a. Press the appropriate destination element button (**Storage Bin**, **Drive**, **Load Port**, **Gripper**, or **PTM**).
   b. Using the keypad, enter the address of the destination element and then press the **Execute** button. The **Dest.** box displays the destination information and the move is initiated.

The control panel displays a **Command In Progress** dialog box with an **Abort** button. The **Move Cartridge** command continues until completed unless you press the **Abort** button to stop the operation.

RQS nº 03/2005 - CN - CPMI - CORREIOS
1194
Fls Nº
3702
Doc:

Unloading a Drive

The **Unload Drive** command prepares a tape cartridge to be removed from a drive by rewinding and ejecting the cartridge. After unloading the drive, remove the tape cartridge using the **Move Cartridge** command.

To unload a drive:

1. From the **Operator** screen, press the **Unload Drive** button. The control panel displays the **Control: Unload Drive** screen (see Figure 35).

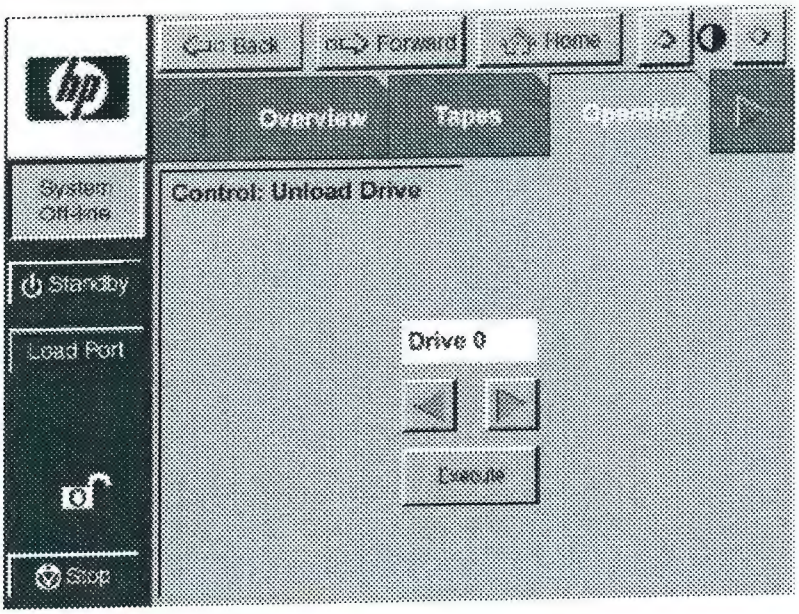


Figure 35: Control: unload drive screen

2. Use the arrow buttons to highlight the desired drive and then press **Execute**.

   The control panel displays a **Command In Progress** dialog box. The **Unload Drive** command continues until completed unless you press the **Abort** button to stop the operation.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1195
Doc: 3702

Unloading the Load Port

The **Unload Imp/Exp** command moves a tape cartridge from the load port to an available storage bin. This option must be invoked after inserting a tape into the load port whenever the library **Auto Load** feature is disabled. See "Configuring Library Options"on page 79.

Note: You can also use the **Move Cartridge** command to unload the load port. This command is especially useful if the destination of the move is important. For more information about the **Move Cartridge** command, see "Moving Cartridges" on page 85.

To unload the load port:

1. From the **Operator** screen, press the **Unload Imp/Exp** button. The control panel displays a **Command In Progress** dialog box.
2. If it becomes necessary to stop the **Unload** command, press the **Abort** button.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1196
Doc. 3702

5

Maintenance and Troubleshooting

This chapter provides troubleshooting and maintenance information for the HP StorageWorks ESL9000 Series tape library. Sections in this chapter include:

- Troubleshooting Common Problems, page 90
- Maintaining Tape Cartridges, page 98
- Cleaning Tape Drives, page 100
- Using HP StorageWorks Library and Tape Tools, page 102

Troubleshooting Common Problems

This section describes problems you might encounter during the setup and operation of the HP StorageWorks ESL9000 Series tape library. Corrective information is provided to help you resolve the problems.

Several of these problems produce error messages on the control panel called sense data values. Sense data value messages consist of a number and a description of the error. For a complete list of sense data values, see Appendix C, "Sense Data Values."

The troubleshooting information in this section includes the following topics:

- Start Up Problems
- Control Panel Problems
- Robotics Problems
- Operating Problems
- Tape Drive Problems

Start Up Problems

Table 14 lists corrective actions for problems that might occur during start-up. If the problems persist, contact your authorized service provider.

Table 14: Start Up Problems

Problem	Corrective Action
The library does not power on.	■ Make sure the power cord is connected to a grounded electrical outlet. ■ Make sure that the power distribution assembly (left rear corner of cabinet) circuit breaker is on. ■ Make sure that all power supplies are switched on. ■ Make sure that the power switch behind the slide panel just below the control panel is on.
The library or tape drives do not respond on the SCSI bus.	Make sure each SCSI device on the same SCSI bus has a unique address and the last device is properly terminated

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1198
3702
Doc:

Table 14: Start Up Problems (Continued)

Problem	Corrective Action
During initialization, the library reports "Not Ready."	■ Determine the failure type by checking any previous error codes returned to the host computer. ■ Correct the cause of the error.
One or more tape drives fail to spin up during start-up.	■ With the tape drive powered off, check all power connections. ■ Make sure the correct number of drives is specified in the library's configuration. ■ Make sure the hot-swap switch is set correctly on the drives that did not spin up.
The library starts up in standby mode.	Press the **Standby** button to verify that the library switches to on-line mode. You can use the control panel to select either on-line or standby mode at powerup.

Control Panel Problems

Table 15 lists corrective actions for control panel problems. If the problems persist, contact your authorized service provider.

Table 15: Control Panel Problems

Problem	Corrective Action
The control panel is blank.	■ Make sure the power cord is connected to a grounded electrical outlet. ■ Make sure that the power distribution assembly (left rear corner of cabinet) circuit breaker is on. ■ Make sure that all power supplies are switched on. ■ Make sure that the power switch behind the slide panel just below the control panel is on. ■ Touch the GUI control panel to bring it out of sleep mode.
The control panel does not respond to touch.	Contact your authorized service provider.
An error message is displayed.	■ Write down the details of the error message, including the SK, ASC, and ASCQ numeric values. ■ Press **OK** to clear the message. ■ See Appendix C, "Sense Data Values," for instructions about resolving the error.

RQS nº 03/2005 - CN - CPMI - CORREIOS
1199
Fls Nº
3702
Doc:

Robotics Problems

Table 16 lists corrective actions for robotics problems.

Table 16: Robotics Problems

Problem	Corrective Action
The robot does not move at powerup.	■ Make sure that all internal packing materials (shipping brackets, foam pads, and tie wraps) have been removed. ■ Check the **Stop** and **Standby** buttons to ensure the library is on-line, and the **Stop** button is disabled.
The gripper partially grips a tape cartridge.	Issue a **Move Cartridge** command to move the cartridge from the gripper to an empty storage bin.
The bar code reader on the gripper fails.	■ Verify that nothing obstructs the reader. ■ Check for damaged or dirty bar code labels. ■ Restart the library.
The robot times out or fails during an operation.	■ Check that the tape cartridge involved in the operation is properly positioned in the bin or drive, and ready to be picked. ■ Check that the robot is not obstructed in any way. ■ Retry the operation.

RQS nº 03/2005 - CN - CPMI - CORREIOS
1200
Fls Nº
3702
Doc:

Table 16: Robotics Problems (Continued)

Problem	Corrective Action
The robot drops a cartridge.	■ Open the front door. ■ Retrieve the cartridge, check it for damage, orient it properly, and place the cartridge in an empty storage bin. (Do not try to place the cartridge in the gripper.) ■ Visually inspect the gripper and extension axis. ■ Perform an inventory following the instructions in Chapter 4, "Operator Commands", so that the library records the position of the manually placed cartridge. ■ Recalibrate the library.
A cartridge is in the gripper at start-up, or when a **Move** command is requested, or after a **Place** command is executed.	■ Use a **Move** command to move the cartridge from the gripper to an empty slot. ■ Open the front door. ■ Manually remove the cartridge from the gripper and place it in an empty bin. ■ Perform an inventory following the instructions in Chapter 4, "Operator Commands", so that the library records the position of the manually placed cartridge. ■ Recalibrate the library.
The gripper does not have a cartridge after completing a pick command.	■ Make sure there is a cartridge in the source location. ■ Retry the command ■ Recalibrate the library.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1201
Doc: 3702

Operating Problems

Table 17 lists corrective actions for problems that might occur during library operation. If the problem persists, contact your authorized service provider.

Table 17: Operating Problems

Problem	Corrective Action
The host computer cannot communicate with the library, or one or more of the drives.	■ Make sure that the library is on-line. ■ This might be a SCSI bus time-out or a premature disconnect problem. ■ Check cable connections, cable length, SCSI addresses, and termination. ■ If the library is communicating via Fibre Channel, then check for: — Addressing issues — Mapping issues — Zoning — Fibre Channel cable damage — Proper installation and configuration of HBAs — Up-to-date firmware and drivers ■ Restart the host and the library.
A tape cartridge is reported as not present.	**Note:** This message indicates that the gripper could not sense a tape cartridge in a particular storage bin, even though the inventory reports that it is present. ■ Check to see if the designated cartridge is present. If it is, make sure it is properly seated. (For a tape drive, make sure the cartridge is completely unloaded.) ■ Retry the command.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1202
3702
Doc:

Table 17: Operating Problems (Continued)

Problem	Corrective Action
A Move command failed.	■ Check the source and destination. The source should hold the cartridge to be moved, and the destination should be empty. ■ Make sure the gripper is empty and all actuators are free of obstruction. ■ Make sure the library is on-line and the **Stop** button is released. ■ Retry the command.
A flash memory error is reported.	Contact your HP service representative.
A maximum temperature exceeded warning appears.	■ Ensure that the rear access panels are closed. ■ If the ambient temperature is too warm, then lower the room temperature (see "Environmental Specifications" on page 106). ■ Make sure the three fan units are operational; the **Normal** LEDs should be lit. ■ Check temperatures and fan speed using the control panel **System Monitor** functions. ■ Make sure that the air filter is clean. ■ Ensure that there are no obstructions to the air flow at the fan inlet or exhaust. ■ Turn off the library and allow it to cool down. Lower the room temperature, if possible, and increase ventilation around the library. **Note:** If the operating temperature is too high, the library will automatically shut down until the temperature drops.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1203
3702
Doc:

Tape Drive Problems

Table 18 lists corrective actions for tape drive problems. If the problem persists, contact your authorized service provider.

Table 18: Tape Drive Problems

Problem	Corrective Action
The library does not recognize the tape drive.	■ Make sure all SCSI cabling is properly connected. ■ Verify correct SCSI termination. ■ Make sure the SCSI ID is correct. ■ Make sure firmware is up to date.
The tape drive does not power up.	■ With the tape drive powered off, check all power connections. ■ Make sure the correct number of drives is specified in the library's configuration. ■ Make sure that the drive's hot-swap switch is set correctly.
The amber LED is on.	Try to unload the tape cartridge, and then reinitialize the tape drive by turning the drive power off, and then back on. The green LED should flash. If reinitializing is successful, the LEDs light steadily again and then go off.
Fatal or nonfatal errors occur. The cause cannot be determined.	■ Make sure all SCSI cabling is properly connected, and that there are no bent pins. ■ Make sure the SCSI ID is correct. ■ Examine the media last used in the drive for damage. ■ Check the software error logs for drive or media errors.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1204
Doc: 3702

Tape Drive Interface LED Problems

Table 19 lists the corrective actions for tape drive interface LED problems. If the problem persists, contact your authorized service provider.

Table 19: Tape Drive Interface LED Problems

Red Led	Green Led	Condition	Action Required
ON	ON	Reserved condition.	Contact your authorized service provider.
ON	Flashing	Reserved condition.	Contact your authorized service provider.
ON	OFF	Drive power fail.	Toggle the hot-plug tape drive switch to clear the condition. If this is unsuccessful, contact your authorized service provider.
OFF	ON	GOOD	None required
OFF	Flashing	SCSI bus incompatible components.	This indicates an LVD/HVD incompatibility. Make sure all components are LVD.
OFF	OFF	No power to tape drive interface.	Make sure the hot-plug tape drive switch is on. Reseat the tape drive. Make sure the library is powered on and the correct number of tape drives is configured.
Flashing	ON	Drive unhealthy	Make sure the drive leader is in place and then reseat the tape drive. If problem persists, contact your authorized service provider.
Flashing	Flashing	Drive inserted, in the process of becoming ready.	This is normal after the library or tape drive power is turned on for a short period of time. If the problem persists, contact your authorized service provider.
Flashing	OFF	Microbridge incompatibility.	Contact your authorized service provider.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1205
Doc 3702

Maintaining Tape Cartridges

Note: In addition to the information provided in this manual, access the *HP StorageWorks SDLT Tape Drive Reference Guide*, and the *HP StorageWorks Ultrium Tape Drive User's Guide* from http://www.hp.com/support for more information.

For longer life of recorded or unrecorded tape cartridges:

- Do not carry cartridges loosely in a container that exposes them to unnecessary physical shock. Dropping or bumping cartridges may dislodge and damage internal components.
- Store tape cartridges vertically in their protective cases until needed. Store tape cartridges in a clean environment that duplicates the conditions of the room in which they will be used.
- Use tape cartridges in temperatures between 50°F to 104°F (10°C and 40°C).
- If a tape cartridge has been exposed to extreme heat or cold, stabilize the tape cartridge at room temperature for the same amount of time it was exposed for up to 24 hours.
- Keep cartridges out of direct sunlight and do not place tape cartridges near electromagnetic interference sources, such as terminals, motors, and video or X-ray equipment. Doing so may cause data on the tape cartridge to be altered or erased.
- Do not touch the tape medium or open the tape door unnecessarily. Dust and skin oils can contaminate the tape, impact performance, and cause damage.
- Store tape cartridges in a dust-free environment where the relative humidity is between 20 percent and 80 percent. For longer tape cartridge life, store the tape cartridge at 40 percent to 60 percent relative humidity.
- Use only HP qualified bar code labels. Apply them only in the designated areas of the tape cartridge, and do not apply more than one label at a time.
- Follow guidelines provided by the tape cartridge manufacturer.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1206
Doc: 3702

17.669

If a tape cartridge is dropped or damage is suspected, gently shake the tape cartridge:

- If it rattles, it is damaged. Restore the data on the tape cartridge by some means other than by using the tape drive, and discard the damaged tape cartridge.
- If it doesn't rattle, check the tape leader inside the cartridge. To do this, open the door on the rear of the tape cartridge by releasing the door lock. The tape leader should be visible at the top-left of the tape cartridge.

Caution: Do not touch the tape leader or the tape medium. Dust or skin oils can contaminate the tape, impact performance, and cause damage.

RQS nº 03/2005 - CN - CPMI - CORREIOS
1207
Fls Nº
Doc 3702

Cleaning Tape Drives

Use the guidelines in the following sections to clean your tape drives.

Cleaning SDLT Tape Drives

Be aware of the following:

- Under normal conditions, the cleaning cartridge is effective for about 20 cleanings.
- SDLT tape drives typically do not need regular cleaning, as their design allows for minimal head contamination.
- Use the cleaning tape only if the cleaning **Alert** light is on.
- Use the cleaning tape more than once if a tape has severely contaminated the drive heads. If the problem persists after two cleanings, and the cleaning tape has not expired, contact your authorized service provider.

Note: Do not use a DLT cleaning tape (almond in color) in an SDLT drive. SDLT cleaning tapes are gray and use a 7- or 8-character bar code label, CLNxxxS or CLNxxxS1.

To clean the tape heads:

1. Move a cleaning cartridge into the drive. The tape drive automatically loads the cartridge and cleans the heads.

   During the cleaning cycle the drive's green **Ready** LED flashes. At the end of the cleaning cycle, the drive ejects the cartridge.
2. Remove the cleaning cartridge from the drive.

CPMI - CORREIOS
1208
Fls Nº
3702
Doc:

Cleaning Ultrium Tape Drives

Be aware of the following:

- Ultrium tape drives have been developed to have a minimal cleaning requirement.

Note: Only use HP-approved Ultrium cleaning cartridges.

- An HP Ultrium Universal Cleaning Cartridge can be used up to 50 times. If you are using an older HP Ultrium cleaning cartridge, check the documentation that came with your media.

Caution: Only use HP Ultrium Universal Cleaning Cartridges in the Ultrium 460 tape drive.

- If the cleaning cartridge is ejected immediately, then it has expired or is not an Ultrium cleaning cartridge. Discard it and use a new one.

To clean the tape heads:

1. Move a cleaning cartridge into the drive. The tape drive automatically loads the cartridge and cleans the heads.

   During the cleaning cycle, the orange **Use Cleaning Cartridge** LED is on and the drive's green **Ready** LED flashes. At the end of the cleaning cycle, the drive ejects the cartridge. The cleaning cycle can take up to five minutes.
2. Move the cleaning cartridge back to the proper storage bin.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1209
Nº 3702
Doc:

Using HP StorageWorks Library and Tape Tools

To provide continued service to our customers, HP provides the HP StorageWorks (L&TT) software application. L&TT is a diagnostic tool that is designed to aid in the installation and maintenance of both HP tape devices and tape libraries. L&TT includes several features designed to be used by both HP storage customers and trained service personnel. The key features include:

- Diagnostic tools for tape drive and tape automation devices that are designed for simple troubleshooting.
- Multiple options for retrieving and updating both the latest firmware and the most current version of L&TT.

Periodic firmware image updates are released on the Internet. For optimal performance, HP recommends that you update your system periodically with the latest device firmware.

L&TT is available for download at no cost from the HP website at:
http://www.hp.com/support/tapetools

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1210
Doc: 3702

Specifications

This appendix lists characteristics and specifications of the HP StorageWorks ESL9000 Series tape library. These characteristics and specifications are categorized as follows:

- Physical Characteristics, page 104
- Performance Characteristics, page 106
- Environmental Specifications, page 106
- Safety and Regulatory Specifications, page 107

Note: For tape drive specifications, see the appropriate tape drive product manual.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1211
Doc: 3702

Physical Characteristics

Table 20 lists dimensions and other physical characteristics of the ESL9322 tape library.

Table 20: Physical Characteristics (ESL9322)

Description	Specifications ESL9322
Width	40 in (101.6 cm)
Depth	29 in (74 cm)
Height	75 in (191 cm)
Weight	1072 lb (487 kg) 8-drive configuration without cartridges Crated: 1307 lb (593 kg)
Maximum tape drives	8
Maximum tape cartridges	322
Drive type	SDLT 110/220 and 160/320 Ultrium 230 and Ultrium 460
Host-to-library interface software	SCSI-2 medium changer command set
Power cord	2 standard, US, IEC 320 C19 female connector rated at 125 VAC (NEMA 5-20P connector included
Host-to-tape drive interface software	■ For SDLT and Ultrium 230: SCSI-2 ■ For Ultrium 460: SCSI-3
Library diagnostics	RS-232C service port for connecting to a field service computer.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1212
Nº 3702
Doc:

17.663

Table 21 lists dimensions and other physical characteristics of the ESL9595 tape library.

Table 21: Physical Characteristics (ESL9595)

Description	Specifications ESL9595
Width	60 in (152 cm)
Depth	29 in (74 cm)
Height	75 in (191 cm)
Weight	1444 lb (655 kg) 16-drive configuration without cartridges Crated: 1822 lb (827 kg)
Maximum tape drives	16
Maximum tape cartridges	595
Drive type	SDLT 110/220 and 160/320 Ultrium 230 and Ultrium 460
Host-to-library interface software	SCSI-2 medium changer command set
Power cord	2 standard, US, IEC 320 C19 female connector rated at 125 VAC (NEMA 5-20P connector included
Host-to-tape drive interface software	■ For SDLT and Ultrium 230: SCSI-2 ■ For Ultrium 460: SCSI-3
Library diagnostics	RS-232C service port for connecting to a field service computer.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1213
3702
Doc:

17.662

Performance Characteristics

Table 22 lists the performance characteristics of the library.

Table 22: Performance Characteristics

Description	Specification
Average swap time	22 seconds, consisting of two Move Medium commands
Inventory (fully loaded with cartridges)	Less than 5 minutes

Environmental Specifications

Table 23 lists the power-environmental and mechanical-environmental specifications of the library.

Table 23: Environmental Specifications

Description		Specification
Electrical inputs	Voltage	90 VAC to 264 VAC
	Frequency	47 Hz to 63 Hz
	Power consumption	VA max 1600 W, 1200W
	Electrical connection to power	IEC 320 C19 female connector inside rear door
Operating temperature	Dry bulb	59° to 90° F (15° to 32° C)
	Wet bulb	77° F (25° C) max
	Thermal transition	18° F (11° C) per hour
Shipping and storage temperature	Dry bulb	-40° to 151° F (-40° to 66° C)
	Wet bulb	115° F (46° C) max
	Thermal transition	54° F (30° C) per hour
Relative humidity	Operating	20% to 80% non-condensing
	Shipping and storage	5% to 95% non-condensing

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1214
Nº 3702
Doc:

Table 23: Environmental Specifications (Continued)

Description	Specification	
Altitude	Operating Shipping and storage	Sea level to 10,000 ft (3,048 m) Sea level to 12,000 ft (3,657 m)
Heat dissipation	Operating	5500 BTU/hr (1400 KCal/hr or 1600 W) for ESL9595 4125 BTU/hr (1050 KCal/hr or 1200 W) for ESL9322
Acoustical noise (sound power level)	Operating Idle	8.10 Bel 7.63 Bel
Acoustical noise (pressure @ bystander)	Operating	63 dB

Safety and Regulatory Specifications

The library carries the following Regulatory Agency product safety certifications.

Table 24: Regulatory and Product Safety Certifications

Description	Specification
UL Listed Mark	UL 1950 (standard for safety of information technology equipment)
NEMKO GS Mark (Germany)	EN60950, IEC950 (standard for safety of information technology equipment, third edition)
CE Marking (European Union)	Low Voltage Directive, 73/23/EEC, European Union
CUL Mark (Canadian UL)	CAN/CSA 22.2 No. 950 (standard for safety of information technology equipment)
Regulatory Series ID Number	ED1002, Class A

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1215
Doc 3702

17.660

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1216
3702
Doc:

17659
V -

Regulatory Compliance Notices

B

This appendix includes the following information:

- Federal Communications Commission Notice, page 110
- Canadian Notice (Avis Canadien), page 112
- European Union Notice, page 112
- BSMI Class A Notice, page 113
- Japanese Notice, page 113
- Laser Device, page 113
- Laser Regulation Labels, page 115

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1217
Doc: 3702

Federal Communications Commission Notice

Part 15 of the Federal Communications Commission (FCC) Rules and Regulations has established Radio Frequency (RF) emission limits to provide an interference-free radio frequency spectrum. Many electronic devices, including computers, generate RF energy incidental to their intended function and are, therefore, covered by these rules. These rules place computers and related peripheral devices into two classes, A and B, depending upon their intended installation. Class A devices are those that may reasonably be expected to be installed in a business or commercial environment. Class B devices are those that may reasonably be expected to be installed in a residential environment (that is, personal computers). The FCC requires devices in both classes to bear a label indicating the interference potential of the device as well as additional operating instructions for the user.

The rating label on the device shows which class (A or B) the equipment falls into. Class B devices have an FCC logo or FCC ID on the label. Class A devices do not have an FCC logo or FCC ID on the label. Once the class of the device is determined, refer to the following corresponding statement.

Class A Equipment

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, 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 personal expense.

Class B Equipment

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1218
3702
Doc:

equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio or television technician for help.

Modifications

The FCC requires the user to be notified that any changes or modifications made to this device that are not expressly approved by Hewlett-Packard Company may void the user's authority to operate the equipment.

Cables

Connections to this device must be made with shielded cables with metallic RFI/EMI connector hoods in order to maintain compliance with FCC Rules and Regulations.

Declaration of Conformity for products marked with the FCC logo - United States only

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

For questions regarding this FCC declaration, contact:

Hewlett-Packard Company
Regulatory Engineer, MS E-200
825 14th Street S.W.
Loveland, CO 80537

Or, call

(970) 898-1738

To identify this product, refer to the Part, Series, or Model number found on the product.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1219
3702
Doc:

Canadian Notice (Avis Canadien)

Class A Equipment

This Class A digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulations.

Cet appareil numérique de la classe A respecte toutes les exigences du Règlement sur le matériel brouilleur du Canada.

Class B Equipment

This Class B digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulations.

Cet appareil numérique de la classe B respecte toutes les exigences du Règlement sur le matériel brouilleur du Canada.

European Union Notice

CE

Products bearing the CE marking comply with the EMC Directive (89/336/EEC) and the Low Voltage Directive (73/23/EEC) issued by the Commission of the European Community and if this product has telecommunication functionality, the R&TTE Directive (1999/5/EC).

Compliance with these directives implies conformity to the following European Norms (in parentheses are the equivalent international standards and regulations):

- EN 55022 (CISPR 22) - Electromagnetic Interference
- EN55024 (IEC61000-4-2, 3, 4, 5, 6, 8, 11) - Electromagnetic Immunity
- EN61000-3-2 (IEC61000-3-2) - Power Line Harmonics
- EN61000-3-3 (IEC61000-3-3) - Power Line Flicker
- EN 60950 (IEC 60950) - Product Safety

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1220
Nº Doc 3702

BSMI Class A Notice

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。

Japanese Notice

ご使用になっている装置にVCCIマークが付いていましたら、次の説明文をお読み下さい。

この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラスB情報技術装置です。この装置は、家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。
取扱説明書に従って正しい取り扱いをして下さい。

VCCIマークが付いていない場合には、次の点にご注意下さい。

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。

Laser Device

All HP systems equipped with a laser device comply with safety standards, including International Electrotechnical Commission (IEC) 825. With specific regard to the laser, the equipment complies with laser product performance standards set by government agencies as a Class 1 laser product. The product does not emit hazardous light; the beam is totally enclosed during all modes of customer operation and maintenance.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1221
Nº Doc: 3702

Laser Safety Warnings

WARNING: To reduce the risk of exposure to hazardous radiation:

Do not try to open the laser device enclosure. There are no user-serviceable components inside.

Do not operate controls, make adjustments, or perform procedures to the laser device other than those specified herein.

Allow only HP authorized service technicians to repair the laser device.

Compliance with CDRH Regulations

The Center for Devices and Radiological Health (CDRH) of the U.S. Food and Drug Administration implemented regulations for laser products on August 2, 1976. These regulations apply to laser products manufactured from August 1, 1976. Compliance is mandatory for products marketed in the United States.

Compliance with International Regulations

All HP systems equipped with laser devices comply with appropriate safety standards, including IEC825.

Laser Specifications

Table 25: Laser Specifications

Feature	Description
Laser type	Semiconductor GaAlAs
Wave length	780 nm +/- 35 nm
Divergence angle	53.5 degrees +/- 0.5 degrees
Output power	Less than 0.2 mW or 10,869 W m-2 sr-1
Polarization	Circular 0.25
Numerical aperture	0.45 inches +/- 0.04 inches

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1222
Doc: 3702

Laser Regulation Labels

Product Conformation Label

The product conformation label is on the rear panel of the library (see Figure 36).

PRODUCT CONFORMS TO USA DHHS 21CFR SUBCHAPTER "J"

Figure 36: Product conformation label

Laser Caution Label

The laser light caution label is near the laser (see Figure 37).

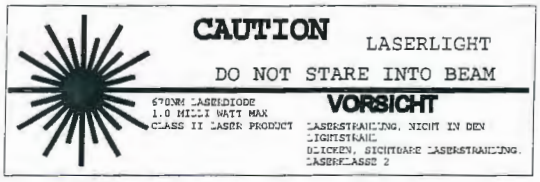


Figure 37: Laser light caution label

Exposure Caution Label

The exposure caution label is on the laser (see Figure 38).

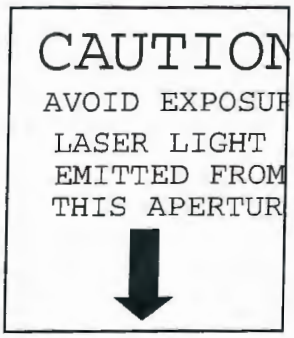


Figure 38: Exposure caution label

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1223
3702
Doc:

17.652

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1224
Doc: 3702

Sense Data Values

This appendix lists sense data values and descriptions. These values appear in library error codes, as well as in the library error log.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1225
3702

Sense Data Values

Table 26 lists message information that can be sent from the library to a host computer

- Sense key
- ASC
- Additional Sense Code Qualifier (ASCQ)
- Message name, description, and (potential) recovery action
- Valid interfaces
  - — SCSI (host computer)
  - — DIAG (diagnostic port/computer)
  - — Both = SCSI and DIAG port

The message name and description might contain abbreviations as follows:

- (A/D) Analog-to-Digital
- (DEV) Device
- (DIAG) Diagnostics
- (LU) Logical Unit
- (NVRAM) Nonvolatile RAM
- (REQ'D) Required

Table 26: Sense Data Values (Hexadecimal)

Sense Key	ASC	ASCQ	Message Name/Description
-none-	30	03	CLEANING CARTRIDGE INSTALLED Indicates that the element contains a cleaning cartridge that is not used-up. This is returned with the element status data, which has no sense key.
-none-	80	01	DRIVE REQUIRES CLEANING Tape drive indicates that drive needs cleaning. Clean the tape drive. This is returned with element status data, which has no sense key.
00	00	00	NO ADDITIONAL SENSE INFORMATION No recovery necessary.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1226
Doc: 3702

Table 26: Sense Data Values (Hexadecimal) (Continued)

Sense Key	ASC	ASCQ	Message Name/Description
02	04	00	LU IS NOT READY, CAUSE NOT REPORTABLE Check library power. Retry command.
02	04	01	LOGICAL UNIT IN PROCESS OF BECOMING READY Wait for library to complete initialization.
02	04	02	LOGICAL UNIT INIT REQUIRED Element status or calibration unknown. Run an inventory command.
02	04	03	LU IS NOT READY, MANUAL INTERVENTION REQ'D Initialization failed. Determine failure type by checking any previous error code in the error log. Correct the cause of the failure and toggle **Standby** button.
02	5A	01	OPERATOR MEDIUM REMOVAL REQUEST Indicates that the element contains a cleaning cartridge that is used-up and the library is unable to export the cleaning cartridge. Manually unload the tape, and replace it with a new cleaning cartridge. The load port door is open, so import/export elements can not be accessed. Close the load port door.
02	80	00	DOOR IS OPENED INVENTORY MAY HAVE BEEN CORRUPTED Close door and retry command. If the library is on-line, it executes its initialization procedure. If not done automatically, run an inventory command.
02	80	07	SYSTEM IS STOPPED (BUTTON IS CURRENTLY PUSHED) The **Stop** button on the control panel was pressed. Press the **Stop** button again to reactivate the robotics.
02	80	09	LOGICAL UNIT IS TURNED OFF-LINE The library is ready to communicate with the diagnostic PC. Press the **Standby** button on the control panel to place the library on-line.
04	80	00	GRIPPER AXIS INTERNAL FAIL Upgrade firmware to latest revision. Call your authorized service provider.
04	80	0A	NVRAM CHECKSUM FAILURE Nonvolatile RAM contents are corrupted. Run the INITIALIZE NON-VOLATILE CONFIG command and then a CALIBRATE ALL command. Call your authorized service provider.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1227
3702
Doc:

Table 26: Sense Data Values (Hexadecimal) (Continued)

Sense Key	ASC	ASCQ	Message Name/Description
04	80	0F	LOW POWER ERROR Check power connections, and check for failed power supplies.
04	80	11	MOTOR POWER FAILURE Indicates motor power turned off for a reason not otherwise reported. Toggle of the **Stop** button should clear. If the motor power failure occurs after the action of closing the door, or when the door is not latched, then upgrade firmware to latest revision. Check door switches. Check for one or more faulty Power Supply Modules.
04	80	23	BARCODE DECODER COMMUNICATION FAILURE Unable to initialize decoder.Check cable connections around Y-axis interconnect.
04	81	00	GRIPPER AXIS INTERNAL FAIL Gripper axis code internal failure. Contact your HP service representative.
04	81	54	GRIPPER TPU REGISTER FAILURE Replace robotic controller board.
04	81	55	GRIPPER TPU RAM FAILURE Replace robotic controller board.
04	82	00	ROTARY AXIS INERNAL FAIL Upgrade firmware to latest revision. Call your authorized service provider.
04	82	01	ROTARY TIMEOUT The rotary axis did not reach the desired position within the time limit. Retry the command. If the failure recurs, contact your authorized service provider.
04	82	08	ROTARY HOME NOT FOUND The home flag was not found. Run a CALIBRATE ALL command.
04	82	10	ROTARY INVALID START The rotary axis has not been homed yet. Issue a CALIBRATE ALL command. Call your authorized service provider. Upgrade firmware to latest revision.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1228
Nº Doc: 3702

Table 26: Sense Data Values (Hexadecimal) (Continued)

Sense Key	ASC	ASCQ	Message Name/Description
04	82	20	ROTARY TEST FAILURE Call your authorized service provider.
04	82	23	ROTARY POSITION OVERFLOW The position step counter overflowed. Issue a CALIBRATE ALL command.
04	83	00	EXTENSION INTERNAL FAILURE Upgrade firmware to latest revision. Extension axis code internal failure. Call your authorized service provider.
04	83	01	EXTENSION TIMEOUT Retry the command. If failure recurs, then run extension self-test.
04	83	02	EXTENSION CURRENT FEEDBACK FAILURE Determine if something is obstructing the extension axis motion. Determine the cause of the obstruction by repeating the command that failed. If a tape is colliding with a bin or drive, then issue a CALIBRATE ALL command. Visually inspect extension axis and belt, look for debris, excessive wear of damage.
04	83	03	EXTENSION MECHANICAL POSITION ERROR Determine if something is obstructing the extension axis motion. Determine the cause of the obstruction by repeating the command that failed. If a tape is colliding with a bin or drive, then recalibrating the system may clear the condition. Visually inspect extension axis and belt, look for debris, excessive wear of damage.
04	83	08	EXTENSION HOME NOT FOUND Check extension home sensor and flag. Visually inspect extension axis and belt, look for debris, excessive wear of damage.
04	83	20	EXTENSION TEST FAILURE The value of the extension encoder did not change during the self-test. Visually inspect extension axis and belt, look for debris, excessive wear of damage.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1229
3702

17.646

Table 26: Sense Data Values (Hexadecimal) (Continued)

Sense Key	ASC	ASCQ	Message Name/Description
04	83	22	EXTENSION ENCODER FAILURE The value of the extension encoder did not change during the self-test. Visually inspect extension axis and belt, look for debris, excessive wear of damage.
04	83	40	EXTENSION FORCE NOT REACHED During calibration or pushing in a drive, the extension never reached its intended force. If error is occurring during a place to a drive, ensure drive is securely installed.
04	83	41	EXTENSION FORCE OBJECT MISSING During calibration or pushing in a drive, the extension never made contact with any object. Verify the electronic model number and configuration matches physical configuration of library. This error will be returned if a bin is not installed, which is expected by the model number configured. If error is occurring during a drive calibration, ensure drive is securely installed.
04	83	50	EXTENSION SENSOR FAIL The Cartridge In Gripper (CIG) sensor was occluded unexpectedly during calibration, inventory or pick/place. Retry the command.
04	84	00	VERTICAL INTERNAL FAILURE Vertical axis code internal failure. Upgrade firmware to latest revision. Call your authorized service provider.
04	84	03	VERTICAL MECHANICAL POSITION ERROR Vertical axis did not reach desired position. Retry command. Determine if something is obstructing the vertical axis motion. Determine the cause of the obstruction by repeating the command that failed. If a tape is colliding with a bin or drive, then a CALIBRATE ALL command may clear the condition.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1230
Doc: 3702

Table 26: Sense Data Values (Hexadecimal) (Continued)

Sense Key	ASC	ASCQ	Message Name/Description
04	84	08	VERTICAL HOME NOT FOUND Vertical axis did not reach the home position. Visually inspect vertical axis and belt, look for debris, excessive wear, or damage.
04	84	20	VERTICAL TEST FAILURE The value of the vertical encoder did not change during the self-test. Visually inspect vertical axis and belt, look for debris, excessive wear, or damage.
04	84	22	VERTICAL ENCODER FAILURE The value of the vertical encoder did not change during the self-test. Visually inspect vertical axis and belt, look for debris, excessive wear, or damage.
04	84	23	VERTICAL POSITION OVERFLOW The position step counter overflowed. Issue a CALIBRATE ALL command.
04	84	30	VERTICAL MAPPING FAILURE Scanner was unable to detect vertical target during calibration. Determine which target (drive, bin, load port) is not mapping. Inspect target for scratches, bends, wear, etc. Invoke CALIBRATE ALL command from control panel.
04	85	00	HORIZONTAL INTERNAL FAILURE Horizontal axis code internal failure. Upgrade firmware to latest revision. Call your authorized service provider.
04	85	03	HORIZONTAL MECHANICAL POSITION ERROR Horizontal axis did not reach desired position. Retry command. Determine if anything is obstructing the horizontal motion. If a tape is colliding with a bin or drive, then run a CALIBRATE ALL command. Visually inspect vertical axis and belt, look for debris, excessive wear, or damage.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1231
3702
Doc:

Table 26: Sense Data Values (Hexadecimal) (Continued)

Sense Key	ASC	ASCQ	Message Name/Description
04	85	08	HORIZONTAL HOME NOT FOUND Horizontal axis did not reach the home position. Issue CALIBRATE ALL and retry operation. Check vertical sensors and flag.
04	85	20	HORIZONTAL TEST FAILURE The value of the horizontal encoder did not change during the self-test. Visually inspect vertical axis and belt, look for debris, excessive wear, or damage. Issue CALIBRATE ALL and retry operation.
04	85	22	HORIZONTAL ENCODER FAILURE The value of the horizontal encoder did not change during the self-test. Visually inspect vertical axis and belt, look for debris, excessive wear, or damage.
04	85	23	HORIZONTAL POSITION OVERFLOW The position step counter overflowed. Issue a CALIBRATE ALL command.
04	85	30	HORIZONTAL MAPPING FAILURE Scanner was unable to detect horizontal target during calibration. Determine which target (drive, bin, load port) is not mapping. Inspect target for scratches, bends, wear, etc. Invoke CALIBRATE ALL from control panel.
04	88	01	MAXIMUM TEMPERATURE EXCEEDED Library turns off and remains off until the temperature returns to an acceptable level 59 to 90°F (15 to 32°C). Check fans, look for airflow obstructions, and make sure ambient room temperature is sufficiently cool.
04	8B	00	PASSTHRU INTERNAL FAILURE Upgrade firmware to latest revision. Call your authorized service provider.
04	8B	02	PASSTHRU CURRENT FEEDBACK FAILURE The pass-through axis is obstructed. Check for obstructions (cables, etc.). Disconnect unit from power and then manually move the axis to ensure it moves freely between cabinets, with no binding or undue friction.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1232
Doc 3702

17.643
4°C

Table 26: Sense Data Values (Hexadecimal) (Continued)

Sense Key	ASC	ASCQ	Message Name/Description
04	8B	03	PASSTHRU MECHANICAL POSITION ERROR Check for obstructions (cables, etc.). Disconnect unit from power then manually move the axis to ensure it moves freely between cabinets, with no binding or undue friction. Retry command.
04	8B	08	PASSTHRU HOME NOT FOUND Check for obstructions (cables, etc.). Disconnect unit from power then manually move the axis to ensure it moves freely between cabinets, with no binding or undue friction.
04	8B	20	PASSTHRU TEST FAILURE Check for obstructions (cables, etc.). Disconnect unit from power then manually move the axis to ensure it moves freely between cabinets, with no binding or undue friction.
04	8B	22	PASSTHRU ENCODER FAILURE The value of the pass-through encoder did not change during the self-test. Check the motor encoder connection. Check for obstructions (cables, etc.). Disconnect unit from power then manually move the axis to ensure it moves freely between cabinets, with no binding or undue friction.
04	8B	51	PTM ELECTRONICS NOT PRESENT The library backplane needs to be upgraded. Call your authorized service provider.
04	8C	06	LOAD PORT DOOR OPEN Load port door unlocked but failed to open
04	8D	24	HANDLE HARDWARE Stepper was unable to reach destination (open or close). Retry command. If the failure recurs, run drive handle Self-test.
04	8E	01	FLASH MEMORY UNABLE TO IDENTIFY Flash is soldered onto the board. Contact your HP service representative.
04	8E	02	FLASH MEMORY UNABLE TO ERASE Flash is soldered onto the board. Contact your HP service representative.
04	8E	03	FLASH MEMORY UNABLE TO PROGRAM Flash is soldered onto the board. Contact your HP service representative.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1233
Nº 3702
Doc:

Table 26: Sense Data Values (Hexadecimal) (Continued)

Sense Key	ASC	ASCQ	Message Name/Description
04	F3	02	DRIVE COMMUNICATION TIMEOUT The library is unable to communicate with a drive. Reseat drive module.
04	F3	11	DRIVE HANDLE NOT OK The tape drive is reporting that the handle cannot open. (This might indicate that a cartridge is present that has not been unloaded.)
05	1A	00	PARAMETER LIST LENGTH ERROR Make sure the software supports the library and has the latest patches and updates.
05	20	00	INVALID COMMAND OPERATION CODE Make sure the backup software supports the library, and has the latest patches.
05	21	01	INVALID ELEMENT ADDRESS Make sure the backup software supports the library, and has the latest patches.
05	24	00	INVALID FIELD IN COMMAND DATA BLOCK Make sure the backup software supports the library, and has the latest patches.
05	25	00	LOGICAL UNIT IS NOT SUPPORTED Check that the library is configured correctly in the software.
05	26	00	INVALID FIELD IN PARAMETER LIST Make sure the backup software supports the library, and has the latest patches.
05	26	02	PARAMETER VALUE INVALID Make sure the backup software supports the library, and has the latest patches. If using the diagnostic utility, check parameters used in last command, and try again.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1234
3702
Doc:

Table 26: Sense Data Values (Hexadecimal) (Continued)

Sense Key	ASC	ASCQ	Message Name/Description
05	30	03	CLEANING CARTRIDGE INSTALLED One of the following conditions exist: ■ A cleaning cartridge cannot be removed from a drive because it is being used in a cleaning operation. ■ A cartridge cannot be placed into the drive because the drive is being cleaned. ■ A cartridge cannot be placed into an empty storage element because it is reserved for a cleaning cartridge that is currently in use in a drive cleaning operation.
05	39	00	SAVING PARAMETERS NOT SUPPORTED Make sure the backup software supports the library, and has the latest patches.
05	3A	00	MEDIUM NOT PRESENT The inventory indicated that a cartridge was in this bin but no cartridge was sensed by the gripper when it attempted to pick it. Retry the command. Check for proper seating of the cartridge. If cartridge is truly not present, run inventory command. It might also indicate that the tape is not ready to be picked from the drive because the tape is not fully unloaded. If the problem persists on an DLT drive, check the function of the tape drive handle assembly. Manually unload the tape.
05	3B	0D	MEDIUM DESTINATION ELEMENT FULL According to inventory, already contains a cartridge. If the destination is truly empty, issue an inventory command and retry the MOVE command. If the destination was full, retry the operation using an empty element as the destination.
05	3B	0E	MEDIUM SOURCE ELEMENT EMPTY According to inventory, source does not contain a cartridge. If the source is truly full, issue an inventory command and retry the MOVE command. If the source was truly empty, then retry the operation using a full element as the source.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1235
3702
Doc:

Table 26: Sense Data Values (Hexadecimal) (Continued)

Sense Key	ASC	ASCQ	Message Name/Description
05	4E	00	OVERLAPPED COMMANDS ATTEMPTED Due to a second command being sent from the same host before a previous command has completed, the previous command has been aborted. This can also occur when executing off-line commands via the control panel and DIAG port simultaneously. Do not run backup software and diagnostic software at the same time.
05	53	02	MEDIUM REMOVAL PREVENTED PREVENT MEDIUM REMOVAL command was executed and command was received to export cartridge. Attempt to move cartridge from software. If unsuccessful, close software and try again from the GUI control panel. If still unsuccessful, disconnect from host, power-cycle, and retry the operation from the GUI control panel.
05	80	01	TRANSFER FULL - COMMAND CANNOT BE EXECUTED Gripper has cartridge in it. Move cartridge to empty storage bin using MOVE command. Retry command.
05	80	22	ELEMENT CONTENTS UNKNOWN The contents of an element address are unknown. Issue an inventory command.
05	82	11	ROTARY INVALID COMMAND Rotary axis was commanded to a position out of its legal range. This is an internal code failure.
05	83	11	EXTENSION INVALID COMMAND Extension axis was commanded to a position out of the libraries mechanical limits. Upgrade firmware to latest revision. Recalibrate the library. If occurred when system was online, call your authorized service provider.
05	84	11	VERTICAL INVALID COMMAND Vertical axis commanded to position out of library mechanical limits. Calibrate the library. Upgrade firmware to latest revision. If occurred when system was online, call your authorized service provider.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1236
Nº 3702
Doc:

Table 26: Sense Data Values (Hexadecimal) (Continued)

Sense Key	ASC	ASCQ	Message Name/Description
05	85	11	HORIZONTAL INVALID COMMAND Horizontal axis commanded to position out of library mechanical limits. Calibrate the library. Upgrade firmware to latest revision. If occurred when system was online, call your authorized service provider.
05	8A	02	UNCALIBRATED POSITION Library requires calibration. Run a CALIBRATE ALL command.
05	8B	11	PASSTHRU INVALID COMMAND Pass-through axis was commanded to a position out of the libraries mechanical limits. Run a CALIBRATE ALL command.
05	F0	01	RESERVATION CONFLICT Internal firmware error. Report this occurrence and previous command (if known) to your HP service representative. Upgrade firmware to the latest revision.
05	F1	00	COMMAND UNSPECIFIED Internal firmware error. Report this occurrence and previous command (if known) to your HP service representative. Upgrade firmware to the latest revision.
05	F1	01	COMMAND HEAP OVERFLOW Internal firmware error. Report this occurrence and previous command (if known) to your HP service representative. Upgrade firmware to the latest revision.
05	F1	02	UNRECOGNIZED COMMAND Internal firmware error. Report this occurrence and previous command (if known) to your HP service representative. Upgrade firmware to the latest revision.
05	F1	03	COMMAND REGISTER ERROR Internal firmware error. Report this occurrence and previous command (if known) to your HP service representative. Upgrade firmware to the latest revision.
05	F3	00	COMMUNICATION INTERNAL FAILURE Internal drive communication port code or hardware failure. Reseat drive module.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1237
Nº 3702
Doc:

Table 26: Sense Data Values (Hexadecimal) (Continued)

Sense Key	ASC	ASCQ	Message Name/Description
06	28	01	IMPORT OR EXPORT ELEMENT ACCESSED Information message. Load port door has been closed.
06	29	00	POWER-ON, OR BUS DEVICE RESET OCCURRED Informational message. If power on occurs, the host user should assume the inventory might have been corrupted, and should run a CALIBRATE ALL command.
06	29	01	POWER-ON OCCURRED Informational message
06	29	02	SCSI BUS RESET OCCURRED Informational message
06	29	03	BUS DEVICE RESET OCCURRED Informational message
06	29	04	INTERNAL DEVICE RESET OCCURRED Informational message
06	2A	01	MODE PARAMETERS CHANGED Mode parameters might have changed due to another host issuing a MODE SELECT command.
06	54	00	SCSI TO HOST SYSTEM INTERFACE FAILURE Possible SCSI bus time-out or premature disconnect. Check cable connections and cable length.
06	80	00	DOOR WAS OPENED INVENTORY MAY HAVE BEEN CORRUPTED Close door. If not done automatically, run an inventory command.
06	80	07	SYSTEM STOP BUTTON WAS PRESSED (MAY CURRENTLY BE PRESSED) The **Stop** button on the control panel was pressed. Press the **Stop** button. Retry command.
06	80	08	LOGICAL UNIT TURNED ON-LINE The library is ready to communicate with the host computer. Press the **Standby** button on the control panel to take the library off-line.
06	80	09	LOGICAL UNIT STANDBY BUTTON WAS PRESSED Retry command.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1238
Nº 3702
Doc.

Table 26: Sense Data Values (Hexadecimal) (Continued)

Sense Key	ASC	ASCQ	Message Name/Description
06	80	0E	DATA TRANSFER CHANGED A drive has been inserted into the library.
06	88	00	WARNING SAFE TEMPERATURE EXCEEDED This is only a warning that the temperature in the library exceeds the normal operational temperature 96.8°F (36°C). Check fans, look for airflow obstructions, and make sure ambient room temperature is sufficiently cool.
0B	00	00	SCSI ABORT Command aborted because host sent SCSI Abort Message.
0B	08	00	LOGICAL UNIT COMMUNICATION FAILURE Check cables. Ensure library is turned on. Retry command.
0B	08	01	LIBRARY COMMUNICATION TIME-OUT ER_LU_COM_TO Retry command.
0B	30	00	INCOMPATIBLE MEDIA An attempt was made to move media to a destination element that is incapable of receiving it. Make sure that you are using media that is compatible with your drive and library.
0B	43	00	SCSI MESSAGE ERROR Make sure the backup software supports the library, and has the latest patches.
0B	45	00	SELECT OR RE-SELECT FAILURE Library timed out trying to reselect host. Make sure host is powered up and on-line.
0B	47	00	SCSI PARITY ERROR SCSI Parity Error detected. Check SCSI cable connections, cable length, and termination.
0B	48	00	INITIATOR DETECTED ERROR Initiator Detected Error Message was received from the host.
0B	80	01	TRANSFER FULL - AT END OF PLACE Gripper has cartridge in it at end of a place operation (Move Medium with a target other than the Transfer). Move cartridge to empty storage bin using MOVE command.

RQS nº 03/2005 - CN - CPMI - CORREIOS
1239
Fls Nº
3702
Doc:

17.636

Table 26: Sense Data Values (Hexadecimal) (Continued)

Sense Key	ASC	ASCQ	Message Name/Description
0B	80	06	TRANSFER EMPTY - COMMAND ABORTED Gripper does not contain cartridge at end of pick portion of MOVE command. Check location of cartridge used in operation. Retry operation.
0B	80	0B	COMMAND ABORTED BY USER Informational message. No action is necessary.
0B	80	0D	CARTRIDGE IS ONLY PARTIALLY GRIPPED (ONLY SEEN IN THE FRONT SENSOR) Issue a MOVE command to move the cartridge from the transfer element to an empty storage element.
0B	80	10	LOAD RETRY FAILED Library was unable to successfully load the drive, even after retries. Check drive alignment. Reseat the drive. If the problem continues, drive might need servicing.
0B	81	01	GRIPPER TIMEOUT Gripper did not reach desired position.
0B	81	04	GRIPPER OPEN FAILURE Gripper did not reach open position. If this failure occurs after closing the door, or when the door is not latched, then upgrade to the latest revision of firmware.
0B	81	05	GRIPPER CLOSE FAILURE Gripper did not reach close position. If this failure occurs after closing the door, or when the door is not latched, then upgrade firmware to latest revision.
0B	81	51	UNABLE TO PICK CARTRIDGE Cartridge was sensed in front gripper sensor, but was unable to seat cartridge in the rear gripper sensor. Check that gripper sensors are working and/or that tape was ejected far enough.
0B	82	04	ROTARY FRONT FAILED The rotary move to the front position failed. Retry the command.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1240
3702
Nº - Doc:

Table 26: Sense Data Values (Hexadecimal) (Continued)

Sense Key	ASC	ASCQ	Message Name/Description
0B	82	05	ROTARY BACK FAILURE The rotary move to the back position failed. Retry the command. If the failure recurs, issue a SELF-TEST command. Replace the robotics controller.
0B	83	01	EXTENSION TIMEOUT Extension axis did not reach desired position. Retry command.
0B	83	10	EXTENSION INVALID ACTUATOR START POSITION Extension axis position is unknown. Issue a CALIBRATE ALL command. Upgrade firmware to latest revision. Call your authorized service provider.
0B	84	01	VERTICAL TIMEOUT Vertical axis did not reach desired position within the time limits. Retry command.
0B	84	10	VERTICAL INVALID ACTUATOR START POSITION Position of vertical axis is unknown. Issue a CALIBRATE ALL command. Upgrade firmware to latest revision. Call your authorized service provider.
0B	85	01	HORIZONTAL TIMEOUT Horizontal axis did not reach desired position within the time limits. Retry command.
0B	85	10	HORIZONTAL INVALID ACTUATOR START POSITION Position of horizontal axis is unknown. Issue a CALIBRATE ALL command. Upgrade firmware to latest revision. Call your authorized service provider.
0B	8B	01	PASSTHRU TIMEOUT Pass-through axis did not reach desired position. Retry command.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1241
Doc: 3702

Table 26: Sense Data Values (Hexadecimal) (Continued)

Sense Key	ASC	ASCQ	Message Name/Description
0B	8B	10	PASSTHRU INVALID ACTUATOR START POSITION Pass-through axis position is unknown. Issue a CALIBRATE ALL command. Upgrade firmware to latest revision. Call your authorized service provider.
0B	8B	60	PTM FULL The PTM contains a cartridge. Issue a command to retrieve the cartridge from the PTM and place it in either a bin or a tape drive.
0B	8C	01	LOAD PORT TIMEOUT The load port door was unlocked, but did not leave its current position before time-out (30 seconds). This might be due to the door being stuck, or in the case of a close operation, the operator not moving the door.
0B	8C	09	LOAD PACK DETENT FAILURE The load pack bin detention spring is unable to hold or release the cartridge. This is detected during a place if the tape does not stay seated in the pack or during a pick if the tape does not eject from the pack.
0B	8D	01	DRIVE HANDLE TIMEOUT Drive handle did not reach commanded position within time limits. Retry the command.
0B	8F	00	LIBRARY UNIT COMMAND TIMED OUT Verify that communications to the library still exists by issuing another command. Check cabling.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1242
Nº 3702 Doc.

17.633

Capacity on Demand

The HP StorageWorks ESL9322 and ESL9595 tape libraries ship with the maximum number of physical storage slots available. However access to these slots requires an upgrade key for the library to recognize them.

ESL9322:

- 222 slots (standard)
- Upgrade to 322 slots

ESL9595:

- 400 slots (standard)
- Upgrade to 500 slots
- Upgrade to 595 slots

Note: To purchase a slot upgrade kit, contact your HP authorized reseller or sales representative.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1243
3702
Doc:

Upgrading Your Capacity

After you obtain your upgrade key, you can upgrade the capacity of your library:

1. Make sure all jobs running on the library have been stopped, and then place the library into **Standby** mode.
2. Ensure that you have the upgrade key.
3. Touch the **License** tab on the control panel.

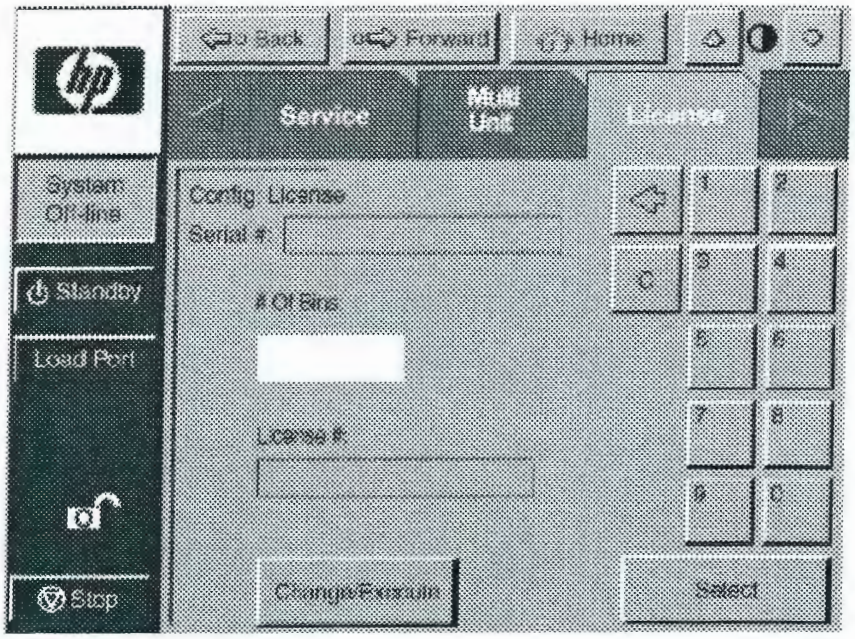


Figure 39: License screen (ESL9595 shown)

4. Enter the number of bins you are upgrading to and then press **Select**.
5. Enter the license number provided to you by HP.
6. Press **Change/Execute**.

The library automatically updates the configuration to the number of bins provided by the license key.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1244
Doc 3702

17.631

If you receive an error message:

1. Verify that the license number you entered is correct and enter it again.
2. Contact your HP sales representative.

Note: Application software may need to be closed and restarted and the library reconfigured to work properly with the newly enabled bins.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1245
3702
Doc:

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1246
Nº 3702
Doc:

index

A

additional sense code qualifier 118
ASC 118
ASCQ 118
authorized reseller, HP 14

B

bar code 30, 40, 47, 48, 49, 50, 52, 54, 56
buttons
  Abort 64, 84, 86, 87, 88
  Back 62, 64, 69, 77, 81
  Backspace 85
  Calibrate All 83
  Calibrate Library 83
  Change 77
  Configure 77
  Configure Library 76
  Configure Options 80
  Contrast 62
  Execute 81, 86
  Forward 62, 63
  Gripper 86
  Home 62, 64
  Import Only 71
  Inventory Tapes 84
  Load Port 54, 62, 70, 86
  Locked 71
  Move Cartridge 85
  Operator 71
  PTM 86
  Select 71, 77, 86
  Service 71
  Set StorageWorks Default 81
  Standby 57, 58, 62, 70, 91, 92, 119, 130
  Stop 62, 64, 70, 92, 95, 119
  Storage Bin 86
  Tape Drive 86
  Unload Drive 87
  Unload Imp/Exp 88
  User 71

C

cabinet 19
  front view 20
  rear view 22
calibration 83
capacity upgrade 135, 136
characteristics
  performance 106
  physical 104
commands
  CALIBRATE LIBRARY 83
  CONFIGURE LIBRARY 76
  CONFIGURE OPTIONS 79
  INVENTORY TAPES 84
  MODE SELECT 130
  MOVE 127
  MOVE CARTRIDGE 85, 86, 87
  MOVE MEDIUM 80, 128, 131, 132
  PREVENT MEDIUM REMOVAL 128
  REZERO UNIT 120, 123, 133, 134
  SELF-TEST 133
  UNLOAD 88
  UNLOAD DRIVE 85, 87
  UNLOAD IMP/EXP 88

common problems and solutions 90
configuration 76
  library options 79
  library settings 77
  SCSI ID assignment 78
control panel 28, 60
  features 62
  functions 60, 61
  initial screen 60
  problems 91
  securing 70
  security levels 70
  using 60
conventions
  document 10
  equipment symbols 11
  text symbols 10

D

data values 118
document
  conventions 10

E

environmental specifications 106
equipment symbols 11
European Union Notice 112
exposure caution label 115

F

features and benefits 18
front panel 19
front view 20

G

getting help 13
gripper 19
  components
    extension axis assembly 29
    gripper assembly 29
    horizontal drive motor 29
    vertical carriage assembly 29

H

help, obtaining 13
HP
  authorized reseller 14
  storage website 13
  technical support 13

I

inventory 84

L

laser caution label 115
LEDs
  Normal 95
library
  components 19
    cabinet 19
    control panel 28
    front panel 19
    rear cabinet 22
    robotics 29
    tape cartridges 35
  configurations 18
  controls 64
  drive types 17
  elements 83
    calibrate 83
  messages 118
  model numbers 17
  models 16
  options 79
    configuring 80
  settings 77
  status 66
    activity status 68
    drive status 67
    load port status 68
    overview screen 66
    storage and load port elements 69

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1248
Doc: 3702

tapes screen 69
load pack 56
installation and removal 56
load port 36, 55
button 55
location
ESL9322 20
ESL9595 21
magazine 55
opening 54
operating 55
tape cartridge 55
unloading 88

M

manageability 18
mixed media 30
model numbers 17
models 16
MOVE 58
moving cartridges 85, 88
multi-unit operation 28

O

operating problems 94
operator screen 74
opening 74
optional PTM 36

P

pass-through mechanism 18
performance characteristics 106
performing an inventory 84
physical characteristics 104
power switch
location
ESL9322 20
ESL9595 21
preserving tape cartridges 100
PTM 18

R

rack stability, warning 12
rear view 22
recovery action 118
regulatory 107, 109
robotics 29
problems 92

S

screen
calibrate library 83
configure 76
exiting 64
initial 60
library settings 77
move cartridges 85
multi-unit 60
navigating 63
opening 63
operator 60, 74, 75
options 80
overview 60
password 74
service 60
tapes 60
unload drives 87
SCSI
breakouts 43
SCSI ID assignment 78
security levels 65
changing 70, 71
sense data 117
sense key 118
serviceability 18
slot upgrade 135, 136
specifications
environmental 106
performance 106
physical 104
regulatory 107
safety 107

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1249
3702
Doc:

start-up problems 90
storage and load port elements 69
symbols in text 10
symbols on equipment 11

T

tape cartridge locations
  ESL9322 24
  ESL9595 26
tape cartridges
  inserting 72
  installation and removal 56
  installing 56
  mixed media 30
  moving 85
tape drive cleaning 36
tape drives 30, 32
  LTO Ultrium 31
  mixed media 30
  SDLT 31
  unloading 87
tapes screen 69
technical support, HP 13
text symbols 10
troubleshooting
  control panel problems 91
  operating problems 94
  robotics problems 92
  sense data values 117
  start-up problems 90

U

unload a drive 87
unload the load port 88

V

valid interfaces 118
  both 118
  DIAG 118
  SCSI 118

W

warning
  defined 10
  laser safety 114
  load port door 54
  rack stability 12
  symbols on equipment 11
websites
  HP storage 13
  HP technical support 13
  library & tape tools 102

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1250
3702
Doc:

ANEXO UNIDADE DE BACKUP ROBOTIZADO
PARTE B

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

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1251
Doc: 3702

CPL - AC
17.633

Managing MC/ServiceGuard

HEWLETT® PACKARD

B3936-90024

January 1998

© Copyright 1998 Hewlett-Packard Company

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1252
Doc 3702

Legal Notices

The information contained in this document is subject to change without notice.

Hewlett-Packard makes no warranty of any kind with regard to this manual, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Hewlett-Packard shall not be liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.

Copyright © 1995, 1997, 1998 Hewlett-Packard Company.

This document contains information which is protected by copyright. All rights are reserved. Reproduction, adaptation, or translation without prior written permission is prohibited, except as allowed under the copyright laws.

Corporate Offices:

Hewlett-Packard Co.
3000 Hanover St.
Palo Alto, CA 94304

Use, duplication or disclosure by the U.S. Government Department of Defense is subject to restrictions as set forth in paragraph (b)(3)(ii) of the Rights in Technical Data and Software clause in FAR 52.227-7013.

Rights for non-DOD U.S. Government Departments and Agencies are as set forth in FAR 52.227-19(c)(1,2).

Use of this manual and flexible disc(s), compact disc(s), or tape cartridge(s) supplied for this pack is restricted to this product only. Additional copies of the programs may be made for security and back-up purposes only. Resale of the programs in their present form or with alterations, is expressly prohibited.

A copy of the specific warranty terms applicable to your Hewlett-Packard product and replacement parts can be obtained from your local Sales and Service Office.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1253
Nº 3702
Doc

Contents

1. **MC/ServiceGuard at a Glance**

What is MC/ServiceGuard? 16
Failover 17
Using this Guide 20
For More Information 22

2. **Understanding MC/ServiceGuard Hardware Configurations**

Redundancy of Cluster Components 24
Redundant Network Components 26
Redundant Ethernet Configuration 26
Providing Redundant FDDI Connections 28
Using Dual Attach FDDI Stations 28
Fibre Channel Switched Configurations 29
Using a Serial (RS232) Heartbeat Line 30
Redundant Disk Storage 32
Supported Disk Interfaces 32
Data Protection 33
Monitoring of Disks Through Event Monitoring Service 34
Replacement of Failed Disk Mechanisms 34
Sample Disk Configurations 34
Root Disk Limitations on Shared Buses 36
Larger Clusters 39
Active/Standby Model 39
Point to Point Connections to Storage Devices 40

3. **Understanding MC/ServiceGuard Software Components**

MC/ServiceGuard Architecture 44
How the Cluster Manager Works 45

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1254
Nº Doc: 3702

Contents

Configuration of the Cluster 45
Manual Startup of Entire Cluster 45
Heartbeat Messages 46
Automatic Cluster Restart 47
Dynamic Cluster Re-formation 47
Cluster Quorum for Re-formation 48
Use of the Cluster Lock 48
Single Cluster Lock 49
Dual Cluster Lock 49
No Cluster Lock 49
Backing Up Cluster Lock Information 50

How the Package Manager Works 51
Deciding When and Where to Run and Halt Packages 51
Starting the Package and Running Application Services 51
Service Monitor 52
Using the Event Monitoring Service 53
Using the EMS HA Monitors 53
Stopping the Package 54

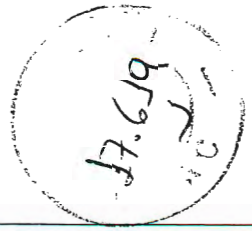
How the Network Manager Works 55
Stationary and Relocatable IP Addresses 55
Adding and Deleting Relocatable IP Addresses 56
Monitoring LAN Interfaces and Detecting Failure 56

Responses to Failures 62
Transfer of Control (TOC) When a Node Fails 62
Responses to Hardware Failures 62
Responses to Package and Service Failures 63

4. Planning and Documenting an HA Cluster

General Planning 67
Planning for Expansion 67

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1255
Nº 3702
Doc:



Contents

Hardware Planning 69
SPU Information 70
Network Information 70
Setting SCSI Addresses for the Largest Expected Cluster Size 72
Disk I/O Information 73
Hardware Configuration Worksheet 75

Power Supply Planning 76
Power Supply Configuration Worksheet 77

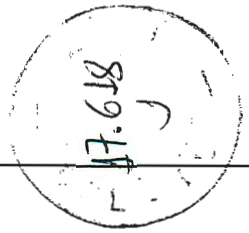
Volume Group and Physical Volume Planning 78
Volume Group and Physical Volume Worksheet 78
Volume Group and PV Links Worksheet 80

Cluster Configuration Planning 81
Choosing the Cluster Lock Volume Group 81
Planning for Expansion 82
Cluster Manager Parameters 83
Cluster Configuration Worksheet 87

Package Configuration Planning 88
Logical Volume and Filesystem Planning 88
Monitoring Registered Package Resources 89
Choosing Switching and Failover Behavior 90
Planning for Expansion 92
Package Configuration File Parameters 93
Package Control Script Variables 97
Package Configuration Worksheet 100

5. Building an HA Cluster Configuration

Preparing Your Systems 103
Editing Security Files 103
Ensuring Consistency of Kernel Configuration 104
Enabling the Network Time Protocol 104



Contents

Preparing for Changes in Cluster Size 104

Installing MC/ServiceGuard 106

Creating the Logical Volume Infrastructure 107
Creating Mirrors of Root Logical Volumes 107
Creating Volume Groups for Mirrored Individual Data Disks. 109
Creating Volume Groups on Disk Arrays Using PV Links. 111
Deactivating the Volume Group. 113
Distributing the Volume Group to Other Nodes 114
Creating Additional Volume Groups 116

Configuring the Cluster 117
Using SAM to Configure the Cluster 117
Using MC/ServiceGuard Commands to Configure the Cluster 118
Adding or Removing Nodes While the Cluster is Running. 121

Verifying the Cluster Configuration 122

Distributing the Binary Configuration File 124
Distributing the Configuration File with SAM 124
Distributing the Configuration File with HP-UX Commands 124
Storing Volume Group and Cluster Lock Configuration Data 125
Checking Cluster Operation. 126

Preventing Automatic Activation of Volume Groups 127

Setting up Autostart Features. 128

Changing the System Message 129

Deleting the Cluster Configuration. 130

6. Configuring Packages and Their Services

Creating the Package Configuration. 132
Using SAM to Configure a Package. 132
Using MC/ServiceGuard Commands to Create a Package. 133

Contents

Writing the Package Control Script 138
Using SAM to Write the Package Control Script 138
Using Commands to Write the Package Control Script 138
Customizing the Package Control Script 139
Adding Customer Defined Functions to the Package Control Script 142
Adding or Removing Packages on a Running Cluster 143

Verify and Distribute the Configuration 144
Distributing the Configuration File And Control Script with SAM . 144
Copying Package Control Scripts with HP-UX commands 144
Distributing the Binary Cluster Configuration File with HP-UX Commands 144
Verifying Cluster and Package Configuration 145

7. Cluster and Package Maintenance

Managing the Cluster and Nodes 148
Starting the Cluster When all Nodes are Down 148
Adding Previously Configured Nodes to a Running Cluster 149
Removing Nodes from Operation in a Running Cluster 150
Halting the Entire Cluster 151
Reconfiguring a Halted Cluster 152
Automatically Restarting the Cluster 153

Reconfiguring a Running Cluster 154
Using SAM to Add Nodes to the Configuration While the Cluster is Running 155
Using MC/ServiceGuard Commands to Add Nodes to the Configuration While the Cluster is Running 155
Using SAM to Delete Nodes from the Configuration While the Cluster is Running 156
Using MC/ServiceGuard Commands to Delete Nodes from the Configuration While the Cluster is Running 156

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1258
Nº - Doc: 3702

Contents

Using SAM to Change the Volume Group Configuration While the Cluster is Running 157
Using MC/ServiceGuard Commands to Change the Volume Group Configuration While the Cluster is Running 158
Managing Packages and Services 159
Starting a Package 159
Halting a Package 160
Moving a Package 160
Reconfiguring on a Halted Cluster 161
Reconfiguring a Package on a Running Cluster 162
Adding a Package to a Running Cluster 162
Deleting a Package from a Running Cluster 163
Changing the PACKAGE_SWITCHING_ENABLED Flag 163
Allowable Package States During Reconfiguration 164
Responding to Cluster Events 166
Single-Node Operation 167
Removing MC/ServiceGuard from a System 168

8. Troubleshooting Your Cluster

Testing Cluster Operation 170
Start the Cluster using SAM 170
Testing the Package Manager 170
Testing the Cluster Manager 171
Testing the Network Manager 172
Monitoring Hardware 173
Using Event Monitoring Service 173
Using HP Predictive Monitoring 173
Replacing Disks 175
Replacing a Faulty Array Mechanism 175

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1259
Nº 3702
Doc:

Contents

Replacing a Faulty Mechanism in an HA Enclosure 175
Replacing a Lock Disk 176
Online Hardware Maintenance with In-line SCSI Terminator. 176

Troubleshooting Approaches. 179
Reviewing Cluster and Package States. 179
Reviewing Package IP Addresses 187
Reviewing the System Log File 187
Reviewing Configuration Files 188
Reviewing the Package Control Script 188
Using the `cmquerycl` and `cmcheckconf` Commands. 189
Using the `cmscancl` Command 189
Using the `cmviewconf` Command 190
Reviewing the LAN Configuration 190

Solving Problems 192
Cluster Re-formations 192
System Administration Errors 193
Package Movement Errors. 195
Node and Network Failures. 195

A. MC/ServiceGuard Commands

B. Enterprise Cluster Master Toolkit

C. Designing Highly Available Cluster Applications

Automating Application Operation 208
Insulate Users from Outages. 208
Define Application Startup and Shutdown. 209

Controlling the Speed of Application Failover. 210
Replicate Non-Data File Systems 210
Use Raw Volumes. 211

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1260
Nº 3702 Doc:

Contents

Evaluate the Use of JFS 211
Minimize Data Loss 211
Use Restartable Transactions 212
Use Checkpoints 213
Design for Multiple Servers 214
Design for Replicated Data Sites 214

Designing Applications to Run on Multiple Systems 215
Avoid Node Specific Information 215
Avoid Using SPU IDs or MAC Addresses 217
Assign Unique Names to Applications 217
Use uname(2) With Care 218
Bind to a Fixed Port 219
Bind to Relocatable IP Addresses 219
Give Each Application its Own Volume Group 220
Use Multiple Destinations for SNA Applications 221
Avoid File Locking 221

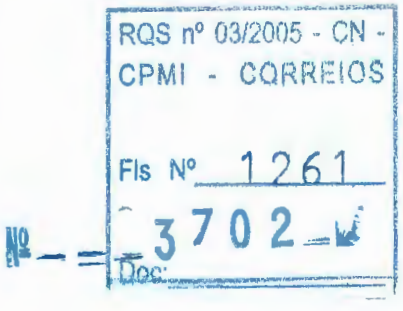
Restoring Client Connections 222

Handling Application Failures 224
Create Applications to be Failure Tolerant 224
Be Able to Monitor Applications 224

Minimizing Planned Downtime 226
Reducing Time Needed for Application Upgrades and Patches 226
Providing Online Application Reconfiguration 227
Documenting Maintenance Operations 228

D. Integrating HA Applications with MC/ServiceGuard

Checklist for Integrating HA Applications 230
Defining Baseline Application Behavior on a Single System 230
Integrating HA Applications in Multiple Systems 231
Testing the Cluster 231



Contents

E. Rolling Software Upgrades

Steps for Rolling Upgrades 234
Performing a Cold Install During Rolling Upgrade 234
Using SAM to Perform a Rolling Upgrade 235
Keeping Kernels Consistent 235

Example of Rolling Upgrade 236
Step 1. 236
Step 2. 237
Step 3. 237
Step 4. 238
Step 5. 238

Limitations of Rolling Upgrades. 240

F. Using OTS/9000 on the LAN

G. Blank Planning Worksheets

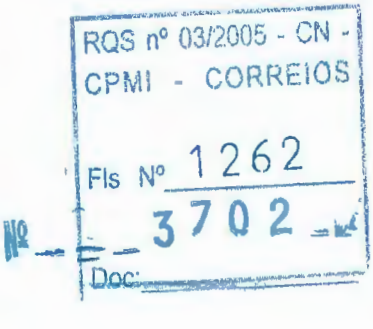
Blank Hardware Worksheet 244

Blank Power Supply Worksheet 245

Blank Volume Group and Physical Volume Worksheet 246

Cluster Configuration Worksheet. 247

Package Configuration Worksheet 248



Contents

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1263
Doc 3702

Printing History

Printing Date	Part Number	Edition
January 1995	B3936-90001	First
June 1995	B3936-90003	Second
December 1995	B3936-90005	Third
August 1997	B3936-90019	Fourth
January 1998	B3936-90024	Fifth

The last printing date and part number indicate the current edition, which applies to the A.11.01 version of MC/ServiceGuard.

The printing date changes when a new edition is printed. (Minor corrections and updates which are incorporated at reprint do not cause the date to change.) The part number is revised when extensive technical changes are incorporated.

New editions of this manual will incorporate all material updated since the previous edition.

HP Printing Division:

Enterprise Systems Division
Hewlett-Packard Co.
19111 Pruneridge Ave.
Cupertino, CA 95014

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1264
Nº 3702

17.610

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1265
Nº 3702
Doc:

CPL 17.609

1 MC/ServiceGuard at a Glance

This chapter introduces MC/ServiceGuard on HP-UX and shows where to find different kinds of information in this book. The following topics are presented:

- What is MC/ServiceGuard?
- Using this Guide
- For More Information

If you are ready to start setting up MC/ServiceGuard clusters, skip ahead to the chapter "Planning and Documenting an HA Cluster." Specific steps for setup are given in the chapter "Building an HA Cluster Configuration."

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1266
Nº 3702 Doc:

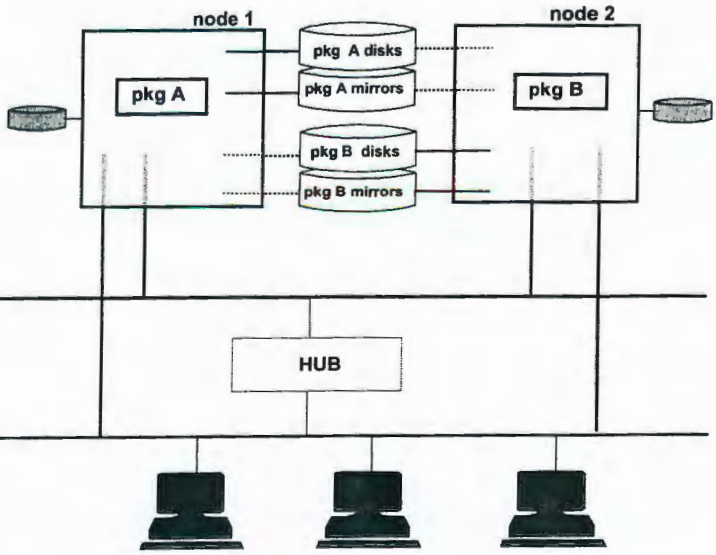
What is MC/ServiceGuard?

MC/ServiceGuard allows you to create high availability clusters of HP 9000 Series 800 computers. A **high availability** computer system allows application services to continue in spite of a hardware or software failure. Highly available systems protect users from software failures as well as from failure of a system processing unit (SPU), disk, or local area network (LAN) component. In the event that one component fails, the redundant component takes over. MC/ServiceGuard and other high availability subsystems coordinate the transfer between components.

An MC/ServiceGuard **cluster** is a networked grouping of HP 9000 series 800 servers (host systems known as **nodes**) having sufficient redundancy of software and hardware that a **single point of failure** will not significantly disrupt service. Application services (individual HP-UX processes) are grouped together in **packages**; in the event of a single service, node, network, or other resource failure, MC/ServiceGuard can automatically transfer control of the package to another node within the cluster, allowing services to remain available with minimal interruption.

Figure 1-1 shows a typical MC/ServiceGuard cluster with two nodes.

Figure 1-1 Typical Cluster Configuration



ROS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1267
Doc: 3702

17.607

In the figure, node 1 (one of two SPU's) is running package A, and node 2 is running package B. Each package has a separate group of disks associated with it, containing data needed by the package's applications, and a mirror copy of the data. Note that both nodes are physically connected to both groups of mirrored disks. However, only one node at a time may access the data for a given group of disks. In the figure, node 1 is shown with exclusive access to the top two disks (solid line), and node 2 is shown as connected without access to the top disks (dotted line). Similarly, node 2 is shown with exclusive access to the bottom two disks (solid line), and node 1 is shown as connected without access to the bottom disks (dotted line).

Mirror copies of data provide redundancy in case of disk failures. In addition, a total of four data buses are shown for the disks that are connected to node 1 and node 2. This configuration provides the maximum redundancy and also gives optimal I/O performance, since each package is using different buses.

Note that the network hardware is cabled to provide redundant LAN interfaces on each node. MC/ServiceGuard uses TCP/IP network services for reliable communication among nodes in the cluster, including the transmission of **heartbeat messages**, signals from each functioning node which are central to the operation of the cluster. TCP/IP services also are used for other types of inter-node communication. (The heartbeat is explained in more detail in the chapter "Understanding MC/ServiceGuard Software.")

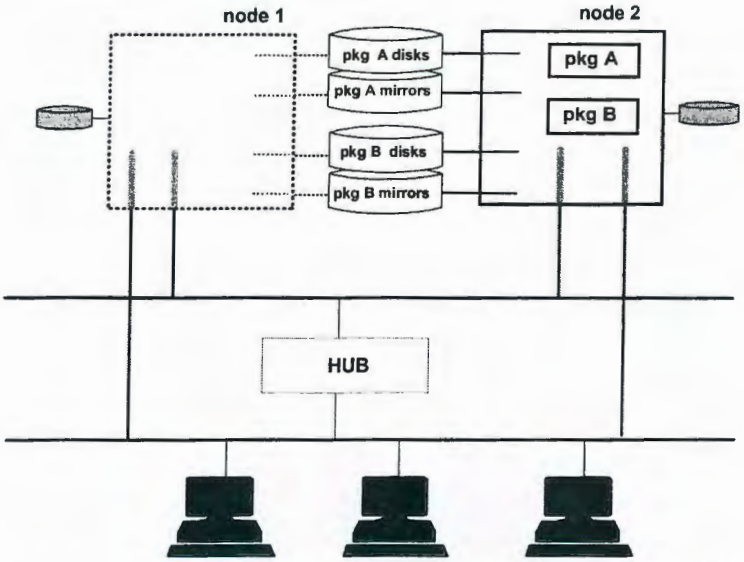
Failover

Under normal conditions, a fully operating MC/ServiceGuard cluster simply monitors the health of the cluster's components while the packages are running on individual nodes. Any host system running in the MC/ServiceGuard cluster is called an **active node**. When you create the package, you specify a **primary node** and one or more **adoptive nodes**. When a node or its network communications fails, MC/ServiceGuard can transfer control of the package to the next available adoptive node. This situation is shown in Figure 1-2.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1268
3702
Doc:

17.606

Figure 1-2 **Typical Cluster After Failover**



After this transfer, the package remains on the adoptive node as long the adoptive node continues running, even if the primary node comes back online. In situations where the adoptive node continues running successfully, you may manually transfer control of the package back to the primary node at the appropriate time. In certain circumstances, in the event of an adoptive node failure, a package that is running on an adoptive node will switch back automatically to its primary node (assuming the primary node is running again as a cluster member).

Figure 1-2 does not show the power connections to the cluster, but these are important as well. In order to remove all single points of failure from the cluster, you should provide as many separate power circuits as needed to prevent a single point of failure of your nodes, disks and disk mirrors. Each power circuit should be protected by an uninterruptible power source. For more details, refer to the section on "Power Supply Planning" in the "Planning" chapter.

MC/ServiceGuard is designed to work in conjunction with other HP high availability products, such as MirrorDisk/UX, which provides disk redundancy to eliminate single points of failure in the disk subsystem; Event Monitoring Service (EMS), which lets you monitor and detect failures that are not directly handled by MC/ServiceGuard; disk arrays, which use various RAID levels for data protection; and HP's UPS

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1269
3702
Doc:

1270
AC

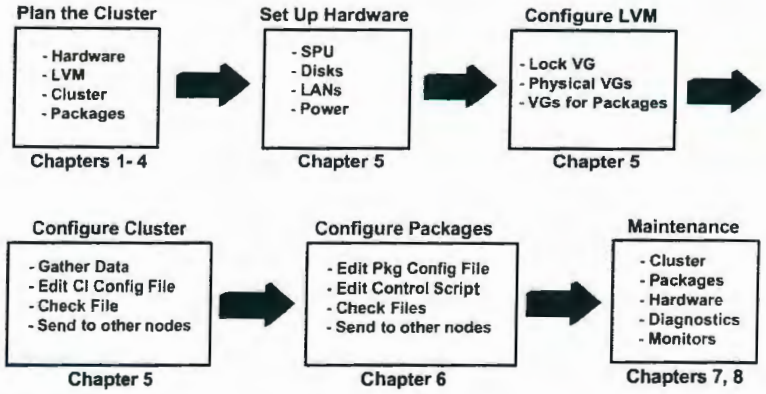
(uninterruptible power supply), PowerTrust, which eliminates failures related to power outage. These products are highly recommended along with MC/ServiceGuard to provide the greatest degree of availability.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
1270
Fls Nº
3702
Doc:

Using this Guide

This manual presents the tasks you need to perform in order to create a functioning HA cluster using MC/ServiceGuard. These tasks are shown in Figure 1-3.

Figure 1-3 Tasks in Configuring an MC/ServiceGuard Cluster



The tasks in Figure 1-3 are covered in step-by-step detail in chapters 4 through 7. It is strongly recommended that you gather all the data that is needed for configuration *before you start*. Refer to Chapter 4, "Planning and Documenting an HA Cluster," for tips on gathering data.

If you are ready to set up an MC/ServiceGuard cluster, skip ahead to the "Planning" chapter. Specific guidelines on cluster creation are found in the chapters "Building a Cluster Configuration" and "Configuring Packages and their Services."

The following is a quick glance at the remaining chapters of this book:

- Chapter 2, "Understanding MC/ServiceGuard Hardware Configurations," describes the hardware configurations used by MC/ServiceGuard and provides a general view of how they work together.
- Chapter 3, "Understanding MC/ServiceGuard Software Components," describes the software components of MC/ServiceGuard and shows how they function within the HP-UX operating system.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1271
3702
Doc:

17.603

- Chapter 4, "Planning and Documenting an HA Cluster," steps through the planning process and provides a set of worksheets for organizing information about the cluster.
- Chapter 5, "Building an HA Cluster Configuration," describes the creation of the cluster configuration.
- Chapter 6, "Configuring Packages and Their Services," describes the creation of high availability packages and the control scripts associated with them.
- Chapter 7, "Cluster and Package Maintenance," presents the basic cluster administration tasks.
- Chapter 8, "Troubleshooting Your Cluster," explains cluster testing and troubleshooting strategies.
- Appendix A, "MC/ServiceGuard Commands," lists the MC/ServiceGuard commands and reprints summary information from each man page.
- Appendix B, "Enterprise Cluster Master Toolkit," presents a set of package configuration files and control scripts for a group of Internet servers and third-party database products.
- Appendix C, "Designing Highly Available Cluster Applications," describes how to create or port applications for HA operation.
- Appendix D, "Integrating HA Applications with MC/ServiceGuard," summarizes the steps you follow to integrate an existing application into the MC/ServiceGuard environment.
- Appendix E, "Rolling Software Upgrades," describes the process of upgrading your MC/ServiceGuard software or the HP-UX operating system to a new release while the cluster is running.
- Appendix F, "Using OTS/9000 on the LAN," explains how to configure your MC/ServiceGuard cluster to use OTS/9000 on your LAN.
- Appendix G, "Blank Planning Worksheets," contains a set of empty worksheets for preparing an MC/ServiceGuard configuration.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1272
3702
Doc:

17.602
CPL - AC

For More Information

The following documents contain additional useful information:

- *Clusters for High Availability: a Primer of HP-UX Solutions*. HP Press, 1995 (ISBN 0-13-494758-4)
- *Configuring OPS Clusters with MC/LockManager, third edition* (B5158-90018)
- *Using EMS HA Monitors* (B5735-90001)
- *Managing Systems and Workgroups* (B2355-90157)
- *Managing Highly Available NFS* (B5125-90001)

Use the following URL to access HP's high availability web page:

- http://www.hp.com/go/ha

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1273
3702
Doc:

17.601

2 Understanding MC/ServiceGuard Hardware Configurations

This chapter gives a broad overview of how the MC/ServiceGuard hardware components work. The following topics are presented:

- Redundancy of Cluster Components
- Redundant Network Components
- Redundant Disk Storage
- Larger Clusters

RQS nº 03/2005 - CN - CPMI - CORREIOS
1274
Fls Nº
3702
Doc:

Redundancy of Cluster Components

In order to provide a high level of availability, a typical cluster uses redundant system components, for example two or more SPUs and two or more independent disks. This redundancy eliminates single points of failure. In general, the more redundancy, the greater your access to applications, data, and supportive services in the event of a failure. In addition to hardware redundancy, you must have the software support which enables and controls the transfer of your applications to another SPU or network after a failure. MC/ServiceGuard provides this support as follows:

- In the case of LAN failure, MC/ServiceGuard switches to a standby LAN or moves affected packages to a standby node.
- In the case of SPU failure, your application is transferred from a failed SPU to a functioning SPU automatically and in a minimal amount of time.
- For failure of other monitored resources, such as disk interfaces, a package can be moved to another node.
- For software failures, an application can be restarted on the same node or another node with minimum disruption.

MC/ServiceGuard also gives you the advantage of easily transferring control of your application to another SPU in order to bring the original SPU down for system administration, maintenance, or version upgrades.

The current maximum number of nodes supported in an MC/ServiceGuard cluster is 8. Fast/Wide SCSI disks or disk arrays can be connected to a maximum of 4 nodes at a time on a shared (multi-initiator) bus. Disk arrays using fibre channel and those that do not use a shared bus — such as the EMC Symmetrix — can be simultaneously connected to all 8 nodes.

The guidelines for package failover depend on the type of disk technology in the cluster. For example, a package that accesses data on a Fast/Wide SCSI disk or disk array can failover to a maximum of 4 nodes. A package that accesses data from a disk in a cluster using Fibre Channel or EMC Symmetrix disk technology can be configured to failover to 8 nodes.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1275
Doc 3702

Note that a package that does *not* access data from a disk on a shared bus can be configured to failover to however many nodes are configured in the cluster (regardless of disk technology). For instance, if a package only runs local executables, it can be configured to failover to all nodes in the cluster that have local copies of those executables, regardless of the type of disk connectivity.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1276
3702
Doc:

Redundant Network Components

To eliminate single points of failure for networking, each subnet accessed by a cluster node is required to have redundant network interfaces. Redundant cables are also needed to protect against cable failures. Each interface card is connected to a different cable, and the cables themselves are connected by a connector such as a hub or a bridge. In the case of FDDI networks, each interface card is connected via a cable to a different concentrator. This arrangement of physical cables connected to each other via a bridge or concentrator or switch is known as a **bridged net**.

IP addresses can be associated with interfaces on a bridged net. An interface that has an IP address associated with it is known as a **primary interface**, and an interface that does not have an IP address associated with it is known as a **standby interface**. Standby interfaces are those which are available for switching by MC/ServiceGuard if a failure occurs on the primary. When MC/ServiceGuard detects a primary interface failure, it will switch the IP addresses and any associated connections from the failed interface card to a healthy standby interface card.

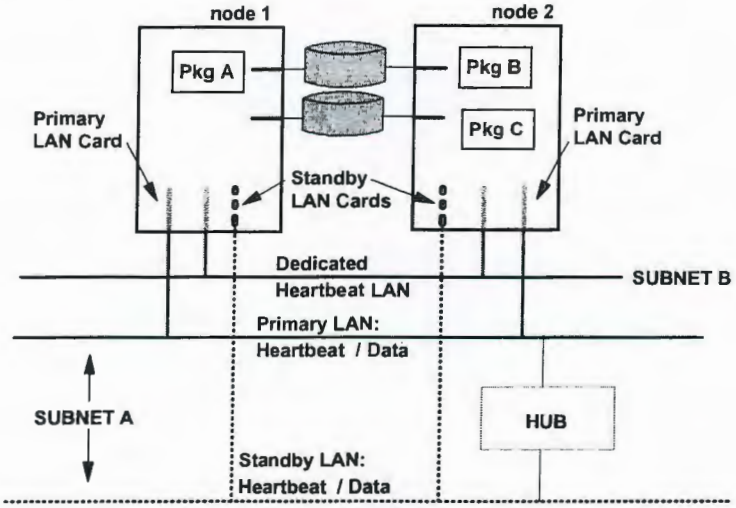
A selection of network configurations is described further inthe following sections. For a complete list of supported networks, refer to the *MC/ServiceGuard Release Notes* for your version of the product.

Redundant Ethernet Configuration

The use of redundant network components is shown in Figure 2-1, which is an Ethernet configuration. Token ring is configured in a similar fashion.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1277
3702
Doc:

Figure 2-1 **Redundant LANs**



In the figure, a two-node MC/ServiceGuard cluster has one bridged net configured with both a primary and a standby LAN card for the data/heartbeat subnet (Subnet A). Another LAN card provides an optional dedicated heartbeat LAN. Note that the primary and standby LAN segments are connected by a hub to provide a redundant data/heartbeat subnet. Each node has its own IP address for this subnet. In case of a failure of a primary LAN card for the data/heartbeat subnet, MC/ServiceGuard will perform a local switch to the standby LAN card on the same node.

Redundant heartbeat is provided by the primary LAN and the dedicated LAN which are both carrying the heartbeat. In Figure 2-1, local switching is not needed for the dedicated heartbeat LAN, since there is already a redundant path via the other subnet. In case of data congestion on the primary LAN, the dedicated heartbeat LAN will prevent a false diagnosis of heartbeat failure. Each node has its own IP address for dedicated heartbeat LAN.

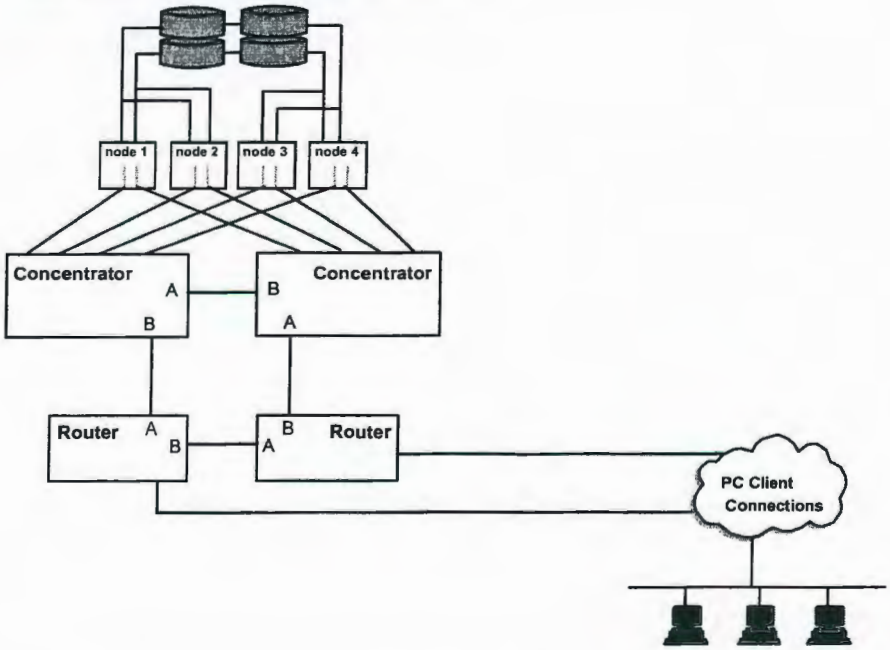
NOTE You should verify that network traffic is not too high on the heartbeat/ data LAN. If traffic is too high, this LAN might not perform adequately in transmitting heartbeats if the dedicated heartbeat LAN fails.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1278
Nº 3702
Doc:

Providing Redundant FDDI Connections

FDDI is a high speed fiber optic interconnect medium. If you are using FDDI, you can create a redundant configuration by using a star topology to connect all the nodes to two concentrators, which are also connected to two routers, which communicate with the world outside the cluster. In this case, you use two FDDI cards in each node. The configuration is shown in Figure 2-2. Note that the concentrators are connected together using dual cables cross-connected Port A to Port B. The routers must be configured to send all packets to both concentrators.

Figure 2-2 **Redundant FDDI Configuration**



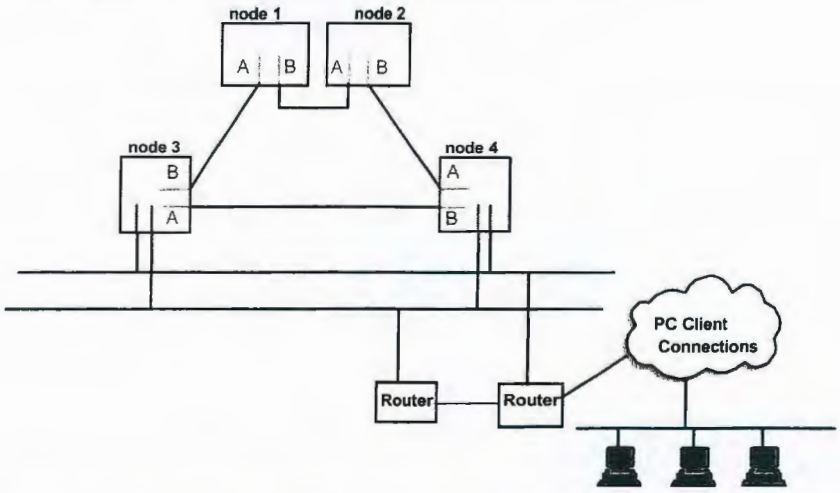
Using Dual Attach FDDI Stations

Another way of obtaining redundant FDDI connections is to configure dual attach stations on each node to create an FDDI ring, shown in Figure 2-3. An advantage of this configuration is that only one slot is used in the system card cage. In Figure 2-3, note that nodes 3 and 4 also use Ethernet to provide connectivity outside the cluster.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
1279
Fls Nº 3702
Doc:

17.595

Figure 2-3 **Configuration with Dual Attach FDDI Stations**



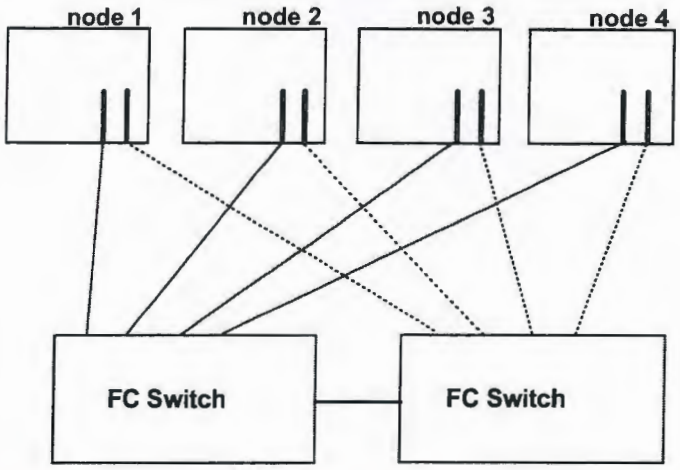
The use of dual attach cards gives protection against failures in both cables and connectors, but does not protect against card failures. LAN card failure would result in a package switching to another node.

Fibre Channel Switched Configurations

Another type of high speed fiber optic interconnect is provided with Fibre Channel, which is normally used with larger clusters (4 to 8 nodes). MC/ServiceGuard clusters configured on enterprise parallel server (EPS) systems can use Fibre Channel switches to provide redundant network paths among nodes. A four node example with two switches is shown in Figure 2-4. For a two-switch topology, all primary paths must go into one switch while all standbys must go to the second switch.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1280
3702
Doc:

Figure 2-4 **FibreChannel Interconnect in a Four-Node Cluster**



In the figure, the solid lines refer to the primary network path among the nodes and the dotted lines refer to the standby path. If there is a failure in one of the primary lines, a local switch takes place on the node that has a failed primary line, and the standby is used instead.

Using a Serial (RS232) Heartbeat Line

MC/ServiceGuard supports a two-node configuration using serial (RS232) communication for heartbeats only. You select this as an alternate heartbeat interface to provide redundant heartbeat. If you configure serial (RS232) as a heartbeat line, MC/ServiceGuard will send the heartbeat continuously on both the LAN configured for heartbeat and a monitored serial (RS232) line.

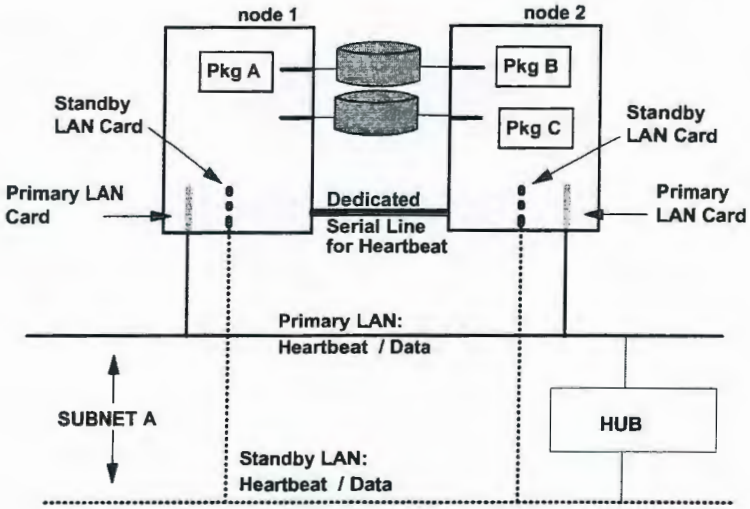
Even if you have a serial (RS232) line configured for redundant heartbeat, one LAN is still required to carry a heartbeat signal. The serial line heartbeat protects against network saturation but not against network failure, since MC/ServiceGuard requires TCP/IP to communicate between cluster members. If both network cards fail on one node, then having a serial line heartbeat keeps the cluster up long enough to detect the LAN controller card status and to fail the node with bad network connections while the healthy node stays up and runs all the packages.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1281
3702

NOTE The use of a serial (RS232) heartbeat line is supported only in a two-node cluster configuration.

A serial (RS232) heartbeat line is shown in Figure 2-5.

Figure 2-5 Serial (RS232) Heartbeat Line



RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1282
Doc 3702

Redundant Disk Storage

Each node in a cluster has its own root disk, but each node is also physically connected to several other disks in such a way that more than one node can obtain access to the data and programs associated with a package it is configured for. This access is provided by the Logical Volume Manager. A disk volume group can be activated by no more than one node at a time, but when the package is moved, the volume group can be activated by the adoptive node. All of the disks in the volume group owned by a package must be connected to the original node and to all possible adoptive nodes for that package. Disk storage is made redundant by using RAID or software mirroring.

Supported Disk Interfaces

The following interfaces are supported by MC/ServiceGuard for disks that are connected to two or more nodes (shared data disks):

- Single-ended SCSI.
- Fast/Wide SCSI.
- HP FiberLink.
- FibreChannel.

Not all SCSI disks are supported. See the *HP 9000 Servers Configuration Guide* (available through your HP representative) for a list of currently supported disks.

External shared Fast/Wide SCSI buses must be equipped with in-line terminators for disks on a shared bus. Refer to the "Troubleshooting" chapter for additional information.

When planning and assigning SCSI bus priority, remember that one node can dominate a bus shared by multiple nodes, depending on what SCSI addresses are assigned to the controller for each node on the shared bus. All SCSI addresses, including the addresses of all interface cards, must be unique for all devices on a shared bus. See the manual *Configuring HP-UX for Peripherals* for information on SCSI bus addressing and priority.

RQS - CN - CPMI - CORREIOS
Fls Nº 1283
Doc: 3702

Data Protection

It is required that you provide data protection for your highly available system, using one of two methods:

- Disk Mirroring
- Disk Arrays using RAID Levels and PV Links

Disk Mirroring

Disk mirroring is one method for providing data protection. The logical volumes used for MC/ServiceGuard packages should be mirrored. MC/ServiceGuard does not provide protection for data on your disks; this is provided by HP's MirrorDisk/UX product, which operates in conjunction with Logical Volume Manager. When you configure logical volumes using MirrorDisk/UX, the members of each mirrored set contain exactly the same data. If one disk should fail, MirrorDisk/UX will automatically keep the data available by accessing the other mirror. Three-way mirroring may be used to allow for online backups or even to provide an additional level of high availability.

To protect against SCSI bus failures, each copy of the data must be accessed by a separate SCSI bus; that is, you cannot have all copies of the data on disk drives connected to the same bus.

While it is valuable to mirror your root disks, it is critical for high availability that you mirror your data disks. In the event of damage to a root disk of one SPU, the other SPUs in the cluster will take over control of the applications. However, if a data disk is damaged, and not mirrored, any application which depends on that disk will not be available until the problem with the disk is repaired. Even then, it may not be possible to recover the data on that disk.

Disk Arrays using RAID Levels and PV Links

An alternate method of achieving protection for your data is to use a disk array using RAID Level 1 or RAID Level 5. The array provides data redundancy for the disks. This protection needs to be combined with the use of redundant SCSI interfaces between each node and the array. The use of redundant interfaces, configured with LVM's PV Links feature protects against single points of failure in the I/O channel, and RAID 1 or 5 configuration provides redundancy for the storage media. (PV links are also known as alternate links in LVM.)

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1284
3702
Doc:

Monitoring of Disks Through Event Monitoring Service

You can configure disk monitoring to detect a failed mechanism by using the disk monitor capabilities of the EMS HA Monitors, available as a separate product (B5735AA). Monitoring can be set up to trigger a package failover or to report disk failure events to a target application such as ClusterView. Refer to the manual *Using EMS HA Monitors* (HP part number B5735-90001) for additional information.

Replacement of Failed Disk Mechanisms

Mirroring provides data protection, but after a disk failure, the failed disk must be replaced. With conventional disks, this is done by bringing down the cluster and replacing the mechanism. With disk arrays and with special HA disk enclosures, it is possible to replace a disk while the cluster stays up and the application remains online. The process is described under "Replacing Disks" in the chapter "Troubleshooting Your Cluster."

Sample Disk Configurations

Figure 2-6 shows a two node cluster. Each node has one root disk which is mirrored and one package for which it is the primary node. Resources have been allocated to each node so that each node may adopt the package from the other node. Each package has one disk volume group assigned to it and the logical volumes in that volume group are mirrored. Please note that Package A's disk and the mirror of Package B's disk are on one interface while Package B's disk and the mirror of Package A's disk are on a separate bus. This arrangement eliminates single points of failure and makes either the disk or its mirror available in the event one of the buses fails.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1285
3702
Doc:

Figure 2-6 **Mirrored Disks Connected for High Availability**

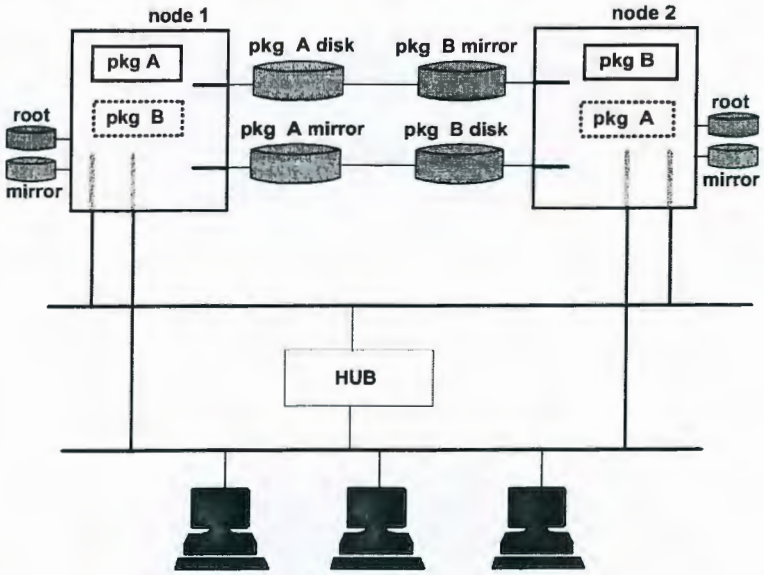
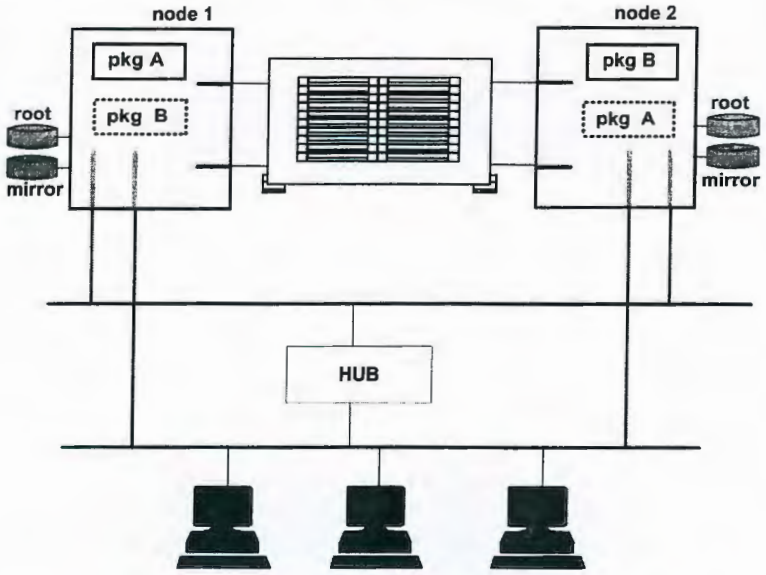


Figure 2-7 shows a similar cluster with a disk array connected to each node on two I/O channels. In this configuration, Logical Volume Manager's PV links are used to define the separate pathways to the data from one node.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1286
Doc: 3702

Figure 2-7 **Cluster with High Availability Disk Array**



Details on logical volume configuration for MC/ServiceGuard, including PV Links, are given in the chapter "Building an HA Cluster Configuration."

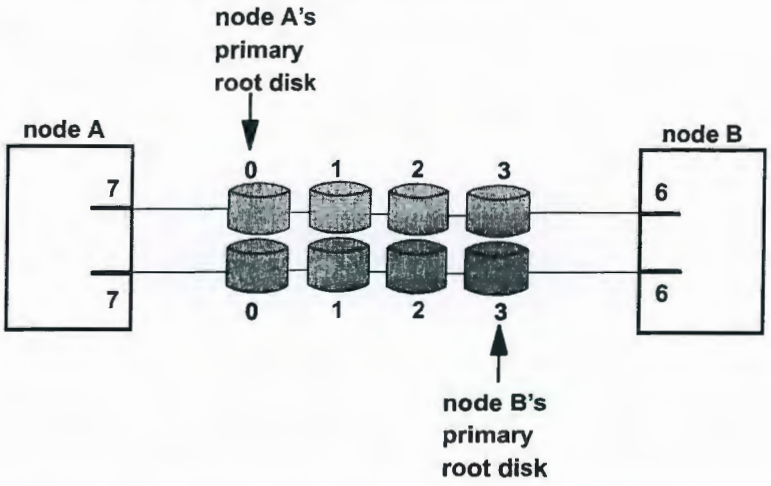
Root Disk Limitations on Shared Buses

The IODC firmware does not support two or more nodes booting from the same SCSI bus at the same time. For this reason, it is important not to attach more than one root disk per cluster to a single SCSI bus.

For example, Figure 2-8 shows a supported configuration in which two nodes share an external SCSI bus and Node A has its primary root disk connected to the bus, but node B has its primary root disk connected to a different bus. (Numbers 0 to 3, 6 and 7 are SCSI addresses on the different buses.)

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1287
3702
Doc:

Figure 2-8 **Root Disks on Different Shared Buses**

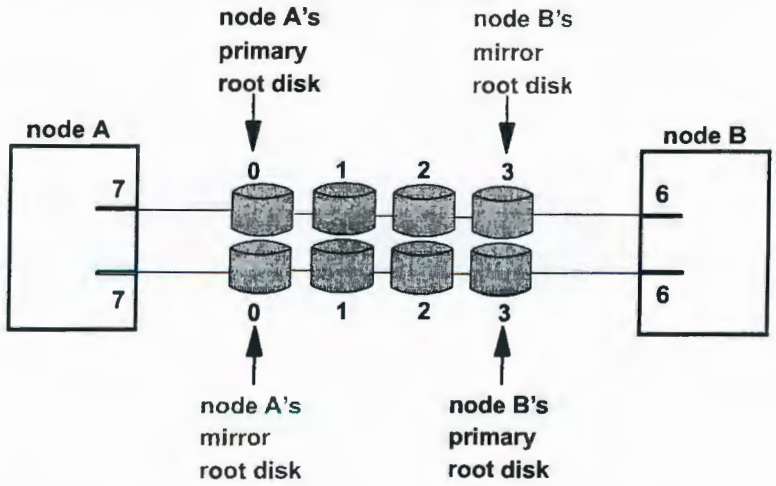


Note that if both nodes had their primary root disks connected to the *same* bus, you would have an unsupported configuration.

You *can* put a mirror copy of Node B's root disk on the same SCSI bus as Node A's primary root disk, because three failures would have to occur for both systems to boot at the same time, which is an acceptable risk. In such a scenario, Node B would have to lose its primary root disk and be rebooted, and Node A would have to be rebooted at the same time Node B is, for the IODC firmware to run into a problem. This configuration is shown in Figure 2-9.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1288
Doc 3702

Figure 2-9 **Primaries and Mirrors on Different Shared Buses**



Note that you *cannot* use a disk within a disk array as a root disk if the array is on a shared bus.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1289
Nº 3702
Doc:

Larger Clusters

You can create clusters of up to 8 nodes with MC/ServiceGuard. Clusters of up to 8 nodes may be built by connecting individual SPUs via Ethernet; and you can configure up to 8 Enterprise Parallel Server (EPS) systems as an MC/ServiceGuard cluster using FDDI or Fibre Channel. EPS solutions are factory-packaged groups of rack-mounted systems that use a high-speed interconnect for communication among the SPU's. When configured as a high availability cluster, the EPS can use the FDDI or Fibre Channel link for heartbeats as well.

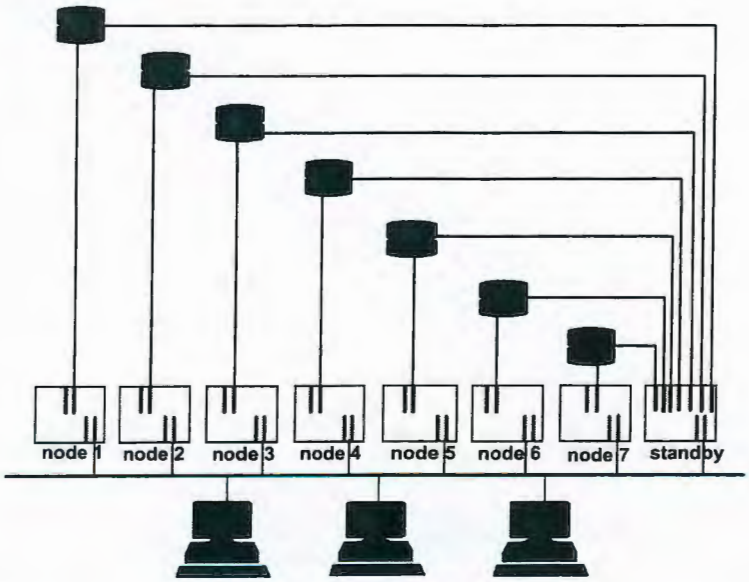
The possibility of configuring a cluster consisting of 8 nodes does not mean that all 8 nodes can be connected to the same disks using the same I/O bus. In the case of F/W SCSI, the practical limit on the number of nodes that can be attached to the same bus is four, because of bus loading and limits on cable length. However, 8 nodes could be set up as an administrative unit, and sub-groupings of four could be set up on different SCSI buses which are attached to different mass storage devices.

Active/Standby Model

An eight node configuration in which one node acts as the standby for the other seven can easily be set up by equipping the backup node with seven shared buses allowing separate connections to each of the active nodes. This configuration is shown in Figure 2-10.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1290
Doc: 3702

Figure 2-10 **Eight-Node Active/Standby Cluster**



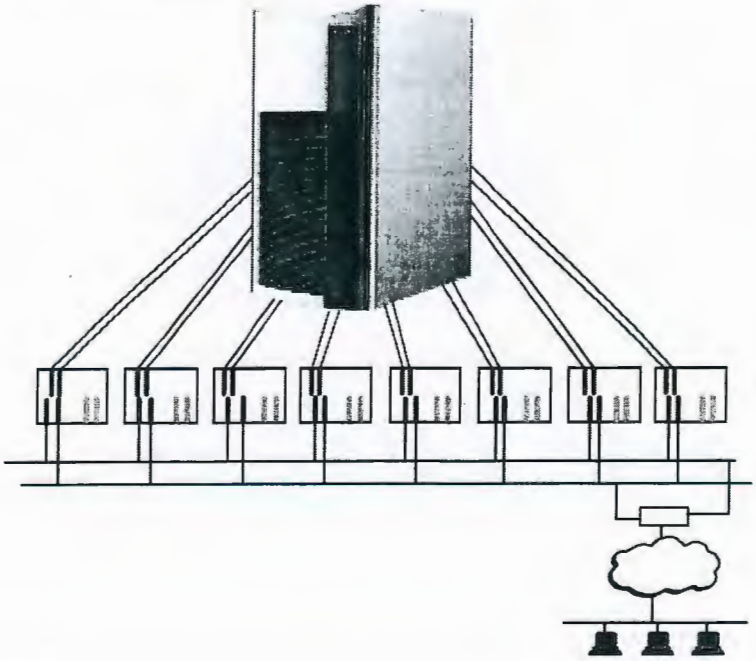
Point to Point Connections to Storage Devices

Some storage devices allow point-to-point connection to a large number of host nodes without using a shared SCSI bus. An example is shown in Figure 2-11, a cluster consisting of eight nodes with a Fibre Channel interconnect. (Client connection is provided through Ethernet.) The nodes access shared data on an EMC Symmetrix disk array, which has 16 I/O ports. Each node is connected to the array using two separate F/W SCSI channels configured with PV Links. Each channel is a dedicated bus; there is no daisy-chaining.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1291
3702

17.583

Figure 2-11 **Eight-Node Cluster with EMC Disk Array**



For additional information about supported cluster configurations, refer to the *HP 9000 Servers Configuration Guide*, available through your HP representative.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1292
3702
Doc:

ROS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1293
Nº 3702
Doc:

CPJ 7581 - 4C

3 Understanding MC/ServiceGuard Software Components

This chapter gives a broad overview of how the MC/ServiceGuard software components work. The following topics are presented:

- MC/ServiceGuard Architecture
- How the Cluster Manager Works
- How the Package Manager Works
- How the Network Manager Works
- Responses to Failures

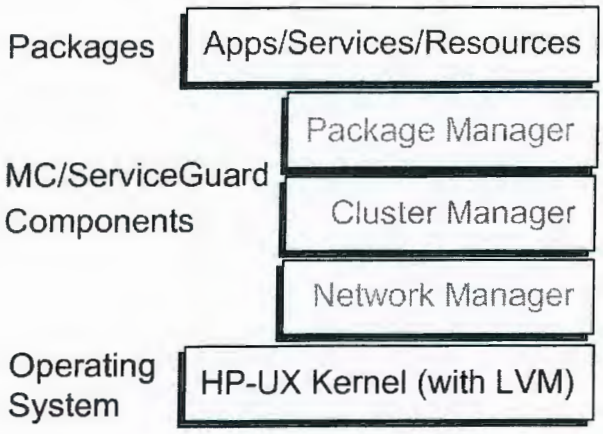
If you are ready to start setting up MC/ServiceGuard clusters, skip ahead to the "Planning" chapter.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1294
Doc 3702

MC/ServiceGuard Architecture

The following figure shows the main software components used by MC/ServiceGuard This chapter discusses these components in some detail.

Figure 3-1 **MC/ServiceGuard Software Components**



RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1295
Doc: 3702

How the Cluster Manager Works

The **cluster manager** is used to initialize a cluster, to monitor the health of the cluster, to recognize node failure if it should occur, and to regulate the re-formation of the cluster when a node joins or leaves the cluster. The cluster manager operates as a daemon process that runs on each node. During cluster startup and re-formation activities, one node is selected to act as the **cluster coordinator**. Although all nodes perform some cluster management functions, the cluster coordinator is the central point for inter-node communication.

Configuration of the Cluster

The system administrator sets up cluster configuration parameters and does an initial cluster startup; thereafter, the cluster regulates itself without manual intervention in normal operation. Configuration parameters for the cluster include the cluster name and nodes, networking parameters for the cluster heartbeat, cluster lock disk information, and timing parameters (discussed in detail in the "Planning" chapter). Cluster parameters are entered using SAM or by editing an ASCII cluster configuration template file. The parameters you enter are used to build a binary configuration file which is propagated to all nodes in the cluster. This binary cluster configuration file must be the same on all the nodes in the cluster.

Manual Startup of Entire Cluster

A manual startup forms a cluster out of all the nodes in the cluster configuration. Manual startup is normally done the first time you bring up the cluster, after cluster-wide maintenance or upgrade, or after reconfiguration.

Before startup, the same binary cluster configuration file must exist on all nodes in the cluster. The system administrator starts the cluster in SAM or with the cmruncl command issued from one node. The cmruncl command can only be used when the cluster is not running, that is, when none of the nodes is running the *cmcld* daemon.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1296
3702
Doc:

During startup, the cluster manager software checks to see if all nodes specified in the startup command are valid members of the cluster, are up and running, are attempting to form a cluster, and can communicate with each other. If they can, then the cluster manager forms the cluster.

Heartbeat Messages

Central to the operation of the cluster manager is the sending and receiving of **heartbeat messages** among the nodes in the cluster. Each node in the cluster sends a heartbeat message over over a stationary IP address on a monitored LAN or a serial (RS232) line to the cluster coordinator. (LAN monitoring is further discussed later in the section "Monitoring LAN Interfaces and Detecting Failure.")

The cluster coordinator looks for this message from each node, and if it is not received within the prescribed time, will re-form the cluster. At the end of the re-formation, if a new set of nodes form a cluster, that information is passed to the **package coordinator** (described further below, under "How the Package Manager Works"). Packages which were running on nodes that are no longer in the new cluster are transferred to their adoptive nodes in the new configuration. Note that if there is a transitory loss of heartbeat, the cluster may re-form with the same nodes as before. In such cases, packages do not halt or switch, though the application may experience a slight performance impact during the re-formation.

If heartbeat and data are sent over the same LAN subnet, data congestion may cause MC/ServiceGuard to miss heartbeats during the period of the heartbeat timeout and initiate a cluster re-formation that would not be needed if the congestion had not occurred. To prevent this situation, it is recommended that you have a dedicated heartbeat as well as configuring heartbeat over the data network or running heartbeat over a serial (RS232) line. A dedicated LAN is not required, but you may wish to use one if analysis of your networks shows a potential for loss of heartbeats in the cluster.

Multiple heartbeats are sent in parallel. It is recommended that you configure all subnets that interconnect cluster nodes as heartbeat networks, since this increases protection against multiple faults at no additional cost.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1297
Doc: 3702

Each node sends its heartbeat message at a rate specified by the cluster heartbeat interval. The cluster heartbeat interval is set in the **cluster configuration file**, which you create as a part of cluster configuration, described fully in the chapter "Building an HA Cluster Configuration."

Automatic Cluster Restart

An automatic cluster restart occurs when all nodes in a cluster have failed. This is usually the situation when there has been an extended power failure and all SPUs went down. In order for an automatic cluster restart to take place, all nodes specified in the cluster configuration file must be up and running, must be trying to form a cluster, and must be able to communicate with one another. Automatic cluster restart will take place if the flag AUTOSTART_CMCLD is set to 1 in the /etc/rc.config.d/cmcluster file.

Dynamic Cluster Re-formation

A dynamic re-formation is a temporary change in cluster membership that takes place as nodes join or leave a running cluster. Re-formation differs from reconfiguration, which is a permanent modification of the configuration files. Re-formation of the cluster occurs under the following conditions:

- An SPU or network failure was detected on an active node.
- An inactive node wants to join the cluster. The cluster manager daemon has been started on that node.
- A node has been added to or deleted from the cluster configuration.
- The system administrator halted a node.
- A node halts because of a package failure.
- A node halts because of a service failure.
- Heavy network traffic prohibited the heartbeat signal from being received by the cluster.
- The heartbeat network failed, and another network is not configured to carry heartbeat.

Typically, re-formation results in a cluster with a different composition. The new cluster may contain fewer or more nodes than in the previous incarnation of the cluster.

ROS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1298
Doc: 3702

Cluster Quorum for Re-formation

The algorithm for cluster re-formation generally requires a cluster quorum of a strict majority (that is, more than 50%) of the nodes previously running. However, exactly 50% of the previously running nodes may re-form as a new cluster provided there is a guarantee that the other 50% of the previously running nodes do not also re-form. In these cases, a tie-breaker is needed. For example, if there is a communication failure between the nodes in a two-node cluster, and each node is attempting to re-form the cluster, then MC/ServiceGuard only allows one node to form the new cluster. This is ensured by using a **cluster lock**.

Use of the Cluster Lock

The cluster lock is a disk area located in a volume group that is shared by all nodes in the cluster. The cluster lock volume group and physical volume names are identified in the cluster configuration file. The cluster lock is used as a tie-breaker only for situations in which a running cluster fails and, as MC/ServiceGuard attempts to form a new cluster, the cluster is split into two sub-clusters of equal size. Each sub-cluster will attempt to acquire the cluster lock. The sub-cluster which gets the cluster lock will form the new cluster, preventing the possibility of two sub-clusters running at the same time. If the two sub-clusters are of unequal size, the sub-cluster with greater than 50% of the nodes will form the new cluster, and the cluster lock is not used.

If you have a two node cluster, you are required to configure the cluster lock. If communications are lost between these two nodes, the node with the cluster lock will take over the cluster and the other node will shut down. Without a cluster lock, a failure of either node in the cluster will cause the other node, and therefore the cluster, to halt. Note also that if the cluster lock fails during an attempt to acquire it, the cluster will halt.

You can choose between two cluster lock options — a single or dual cluster lock — based on the kind of high availability configuration you are building. *A single cluster lock is recommended where possible.* With both single and dual locks, however, it is important that the cluster lock disk be available even if one node loses power; thus, the choice of a lock configuration depends partly on the number of power circuits available. Regardless of your choice, all nodes in the cluster must have access to the cluster lock to maintain high availability.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1299
Doc: 3702

If you have a cluster with more than 4 nodes, a cluster lock is not allowed.

NOTE Plan ahead for the future growth of the cluster. If the cluster will grow to more than 4 nodes, you should either not configure a cluster lock or else plan on taking down the cluster while the fifth node is added so the cluster lock can be removed.

Single Cluster Lock

It is recommended that you use a single cluster lock. A single cluster lock should be configured on a power circuit separate from that of any node in the cluster. For example, it is highly recommended to use three power circuits for a two-node cluster, with a single, separately powered disk for the cluster lock. For two-node clusters, this single lock disk may not share a power circuit with either node, and it must be an external disk. For three or four node clusters, the disk should not share a power circuit with 50% or more of the nodes.

Dual Cluster Lock

If you are using disks that are internally mounted in the same cabinet as the cluster nodes, then a single lock disk would be a single point of failure in this type of cluster, since the loss of power to the node that has the lock disk in its cabinet would also render the cluster lock unavailable. In this case only, a dual cluster lock, with two separately powered cluster disks, should be used to eliminate the lock disk as a single point of failure. For a dual cluster lock, the disks must not share either a power circuit or a node chassis with one another. In this case, if there is a power failure affecting one node and disk, the other node and disk remain available, so cluster re-formation can take place on the remaining node.

No Cluster Lock

Normally, you should not configure a cluster of three or fewer nodes without a cluster lock. In two-node clusters, a cluster lock is required. You may consider using no cluster lock with configurations of three or more nodes, although the decision should be affected by the fact that any cluster may require tie-breaking. For example, if one node in a

RQS nº 03/2005 - CPMI - CORREIOS
Fls Nº 1300
Doc: 3702

17.574

three-node cluster is removed for maintenance, the cluster reforms as a two-node cluster. If a tie-breaking scenario later occurs due to a node or communication failure, the entire cluster will become unavailable.

In a cluster with four or more nodes, you do not need a cluster lock since the chance of the cluster being split into two halves of equal size is very small. Cluster locks are *not* allowed in clusters of more than four nodes. However, be sure to configure your cluster to prevent the failure of exactly half the nodes at one time. For example, make sure there is no potential single point of failure such as a single LAN between equal numbers of nodes, or that you don't have exactly half of the nodes on a single power circuit.

Backing Up Cluster Lock Information

After you configure the cluster and create the cluster lock volume group and physical volume, you should create a backup of the volume group configuration data on each lock volume group. Use the vgcfgbackup command for each lock volume group you have configured, and save the backup file in case the lock configuration must be restored to a new disk with the vgcfgrestore command following a disk failure.

NOTE You must use the vgcfgbackup and vgcfgrestore commands to back up and restore the lock volume group configuration data regardless of whether you use SAM or HP-UX commands to create the lock volume group.

REG TP 03/2005 - CN -
CPMI - CORREIOS
1301
Fls Nº
3702
Doc:

How the Package Manager Works

Each node in the cluster runs an instance of the **package manager**; the package manager residing on the cluster coordinator is known as the **package coordinator**.

The package coordinator does the following:

- Decides when and where to run, halt or move packages.

The package manager on all nodes does the following:

- Executes the user-defined control script to run and halt packages and package services.
- Reacts to changes in the status of monitored resources.

Deciding When and Where to Run and Halt Packages

Each package is separately configured by means of a package configuration file, which can be edited manually or through SAM. This file assigns a name to the package and identifies the nodes on which the package can run, in order of priority. It also indicates whether or not switching is enabled for the package, that is, whether the package should switch to another node or not in the case of a failure. There may be many applications in a package. Package configuration is described in detail in the chapter "Configuring Packages and their Services."

Starting the Package and Running Application Services

After a cluster has formed, the package manager on each node starts up packages on that node. Starting a package means running individual application services on the node where the package is running.

To start a package, the package manager runs the **package control script** with the 'start' parameter. This script performs the following tasks:

- uses Logical Volume Manager (LVM) commands to activate volume groups needed by the package.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1302
Doc: 3702

- mounts filesystems from the activated volume groups to the local node.
- uses cmmodnet to add the package's IP address to the current network interface running on a configured subnet. This allows clients to connect to the same address regardless of the node the service is running on.
- uses the cmrunserv command to start up each application service configured in the package. This command also initiates monitoring of the service.
- executes a set of customer-defined run commands to do additional processing, as required..

While the package is running, services are continuously monitored. If any part of a package fails, the package halt instructions are executed as part of a recovery process. Failure may result in simple loss of the service, a restart of the service, transfer of the package to an adoptive node, or transfer of all packages to adoptive nodes, depending on the package configuration. In package transfers, MC/ServiceGuard sends a TCP/IP packet across the heartbeat subnet to the package's adoptive node telling it to start up the package.

NOTE

When applications run as services in an MC/ServiceGuard package, you do not start them directly; instead, the package manager runs packages on your behalf either when the cluster starts or when a package is enabled on a specific node. Similarly, you do not halt an individual application or service directly once it becomes part of a package. Instead you halt the package or the node. Refer the chapter on "Cluster and Package Maintenance" for a description of how to start and stop packages.

The package configuration file and control script are described in detail in the chapter "Configuring Packages and their Services."

Service Monitor

The Service Monitor checks the PIDs of services started by the package control script. If it detects a PID failure, the package is halted. Depending upon the parameters set in the package configuration file, MC/ServiceGuard will attempt to restart the service on the primary node, or the package will fail over to a specified adoptive node.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1303
Nº 3702

Using the Event Monitoring Service

Basic package resources include cluster nodes, LAN interfaces, and services, which are the individual processes within an application. All of these are monitored by MC/ServiceGuard directly. In addition, you can use the Event Monitoring Service registry through which add-on monitors can be configured. This registry allows other software components to supply monitoring of their resources for MC/ServiceGuard. Monitors currently supplied with other software products include an OTS/9000 monitor and an ATM monitor.

If a registered resource is configured in a package, the package manager calls the resource registrar to launch an external monitor for the resource. The monitor then sends messages back to MC/ServiceGuard, which can fail the package to another node or take other action if the resource is considered unavailable.

Using the EMS HA Monitors

The EMS HA Monitors, available as a separate product (A5735AA), can be used to set up monitoring of disks and other resources as package dependencies. Examples of resource attributes that can be monitored using EMS include the following:

- Logical volume status
- Physical volume status
- System load
- LAN health

Once a monitor is configured as a package dependency, the monitor will notify the package manager if an event occurs showing that a resource is down. The package may then be failed over to an adoptive node.

The EMS HA Monitors can also be used to report monitored events to a target application such as ClusterView for graphical display or for operator notification. Refer to the manual *Using EMS HA Monitors* (HP part number B5735-90001) for additional information.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1304
Nº 3702
Doc:

1705
J

Stopping the Package

The package manager is notified when a command is issued to shut down a package. In this case, the package control script is run with the 'stop' parameter. For example, if the system administrator chooses "Halt Package" from the "Package Administration" menu in SAM, the package manager will stop the package. Similarly, when a command is issued to halt a cluster node, the package manager will shut down all the packages running on the node, executing each package control script with the 'stop' parameter. When run with the 'stop' parameter, the control script:

- uses cmhaltserv to halt each service.
- unmounts filesystems that had been mounted by the package.
- uses Logical Volume Manager (LVM) commands to deactivate volume groups used by the package.
- uses cmmodnet to delete the package's IP address from the current network interface.

NOTE The package is automatically stopped on the failure of a package component. For more details, refer to "Responses to Package and Service Failures," below.

ROS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1305
3702
Doc:

1756

How the Network Manager Works

The purpose of the network manager is to detect and recover from network card and cable failures so that network services remain highly available to clients. In practice, this means assigning IP addresses for each package to the primary LAN interface card on the node where the package is running and monitoring the health of all interfaces, switching them when necessary.

Stationary and Relocatable IP Addresses

Each node (host system) should have an IP address for each active network interface. This address, known as a **stationary IP address**, is configured in the node's /etc/rc.config.d/netconf file. A stationary IP address is not transferrable to another node, but may be transferrable to a standby LAN interface card. The stationary IP address is *not* associated with packages. Stationary IP addresses are used to transmit heartbeat messages (described earlier in the section "How the Cluster Manager Works") and other data.

In addition to the stationary IP address, you normally assign one or more unique IP addresses to each package. The package IP address is assigned to the primary LAN interface card by the cmmodnet command in the package control script when the package starts up. The IP addresses associated with a package are called **relocatable IP addresses** (also known as **package IP addresses** or **floating IP addresses**) because the addresses can actually move from one cluster node to another. You can use up to 200 relocatable IP addresses in a cluster spread over as many as 30 packages.

A relocatable IP address is like a virtual host IP address that is assigned to a package. It is recommended that you configure names for each package through DNS (Domain Name System). A program then can use the package's name like a host name as the input to gethostbyname(), which will return the package's relocatable IP address.

Both stationary and relocatable IP addresses will switch to a standby LAN interface in the event of a LAN card failure. In addition, relocatable addresses (but not stationary addresses) can be taken over by an adoptive node if control of the package is transferred. This means that applications can access the package via its relocatable address without knowing which node the package currently resides on.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1306
Nº 3702
Doc:

17.568

Adding and Deleting Relocatable IP Addresses

When a package is started, a relocatable IP address can be added to a specified IP subnet. When the package is stopped, the relocatable IP address is deleted from the specified subnet. Adding and removing of relocatable IP addresses is handled through the cmmodnet command in the **package control script**, which is described in detail in the chapter "Configuring Packages and their Services."

IP addresses are configured only on each primary network interface card; standby cards are not configured with an IP address. Multiple IP addresses on the same network card must belong to the same IP subnet.

Load Sharing

It is possible to have multiple services on a node associated with the same IP address. If one service is moved to a new system, then the other services using the IP address will also be migrated. Load sharing can be achieved by making each service its own package and giving it a unique IP address. This gives the administrator the ability to move selected services to less loaded systems.

Monitoring LAN Interfaces and Detecting Failure

At regular intervals, MC/ServiceGuard polls all the network interface cards specified in the cluster configuration file. Network failures are detected in the following manner. One interface in a bridged net is assigned to be the poller. The poller will poll the other primary and standby interfaces in the bridged net to see whether they are still healthy. Normally, the poller is a standby interface; if there are no standby interfaces in a bridged net, the primary interface is assigned the polling task.

The polling interface sends LAN packet messages to all other interfaces on a bridged net and receives packets back from all other interfaces on the bridged net. If an interface cannot receive or send a message, and when the numerical count of packets sent and received on an interface does not increment for an amount of time, the interface is considered DOWN.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1307
Nº 3702
Doc:

Adding and Deleting Relocatable IP Addresses

When a package is started, a relocatable IP address can be added to a specified IP subnet. When the package is stopped, the relocatable IP address is deleted from the specified subnet. Adding and removing of relocatable IP addresses is handled through the cmmodnet command in the **package control script**, which is described in detail in the chapter "Configuring Packages and their Services."

IP addresses are configured only on each primary network interface card; standby cards are not configured with an IP address. Multiple IP addresses on the same network card must belong to the same IP subnet.

Load Sharing

It is possible to have multiple services on a node associated with the same IP address. If one service is moved to a new system, then the other services using the IP address will also be migrated. Load sharing can be achieved by making each service its own package and giving it a unique IP address. This gives the administrator the ability to move selected services to less loaded systems.

Monitoring LAN Interfaces and Detecting Failure

At regular intervals, MC/ServiceGuard polls all the network interface cards specified in the cluster configuration file. Network failures are detected in the following manner. One interface in a bridged net is assigned to be the poller. The poller will poll the other primary and standby interfaces in the bridged net to see whether they are still healthy. Normally, the poller is a standby interface; if there are no standby interfaces in a bridged net, the primary interface is assigned the polling task.

The polling interface sends LAN packet messages to all other interfaces on a bridged net and receives packets back from all other interfaces on the bridged net. If an interface cannot receive or send a message, and when the numerical count of packets sent and received on an interface does not increment for an amount of time, the interface is considered DOWN.

RQS nº 03/2005 - CN - CPMI - CORREIOS
1308
Fls Nº
3702
Doc:

1756

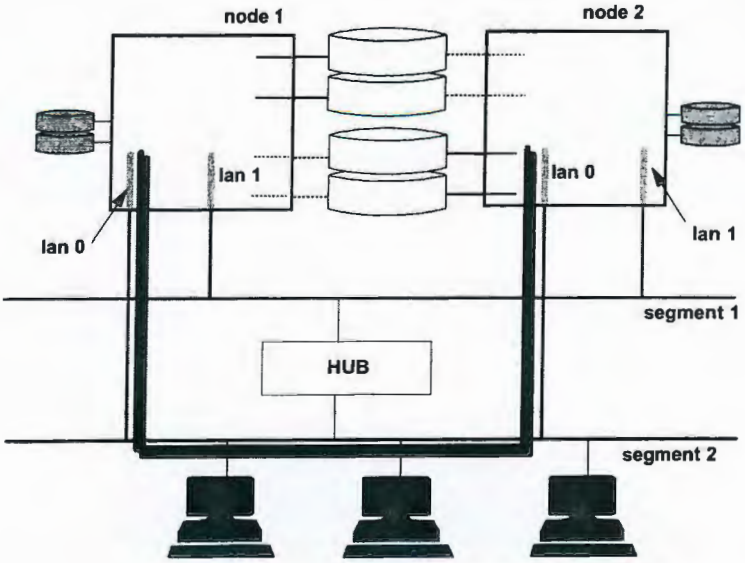
Local Switching

A local network switch involves the detection of a local network interface failure and a failover to the local backup LAN card. The backup LAN card must not have any IP addresses configured. In the case of a local network switch, TCP/IP connections are not lost for Ethernet, but IEEE 802.3 connections will be lost. Ethernet, Token Ring and FDDI use the ARP protocol, and HP-UX sends out an unsolicited ARP to notify remote systems of address mapping between MAC (link level) addresses and IP level addresses. IEEE 802.3 does not have the *rearp* function.

During the transfer, IP packets will be lost, but TCP (Transmission Control Protocol) will retransmit the packets. In the case of UDP (User Datagram Protocol), the packets will not be retransmitted automatically by the protocol. However, since UDP is an unreliable service, UDP applications should be prepared to handle the case of lost network packets and recover appropriately. Note that a local switchover is supported only between two LANs of the same type. For example, a local switchover between Ethernet and FDDI interfaces is not supported.

Figure 3-2 shows two nodes connected in one bridged net. LAN segments 1 and 2 are connected by a hub.

Figure 3-2 Cluster Before Local Network Switching

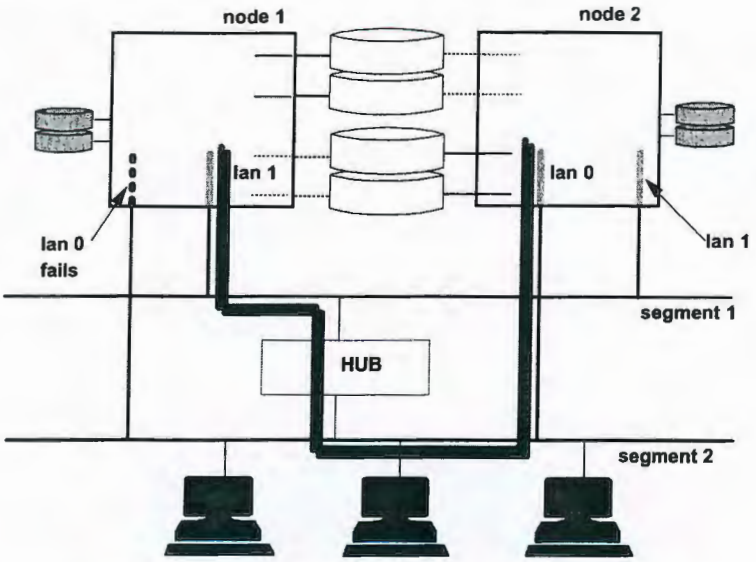


RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1309
3702

Node 1 and Node 2 are communicating over LAN segment 2. LAN segment 1 is a standby.

In Figure 3-3, we see what would happen if the LAN segment 2 network interface card to Node 2 were to fail.

Figure 3-3 Cluster After Local Network Switching



As the standby interface takes over, IP addresses will be switched to the hardware path associated with the standby interface. The switch is transparent at the TCP/IP level. All applications continue to run on their original nodes. During this time, IP traffic on Node 2 will be delayed as the transfer occurs. However, the TCP/IP connections will continue to be maintained and applications will continue to run. Control of the packages on Node 2 is not affected.

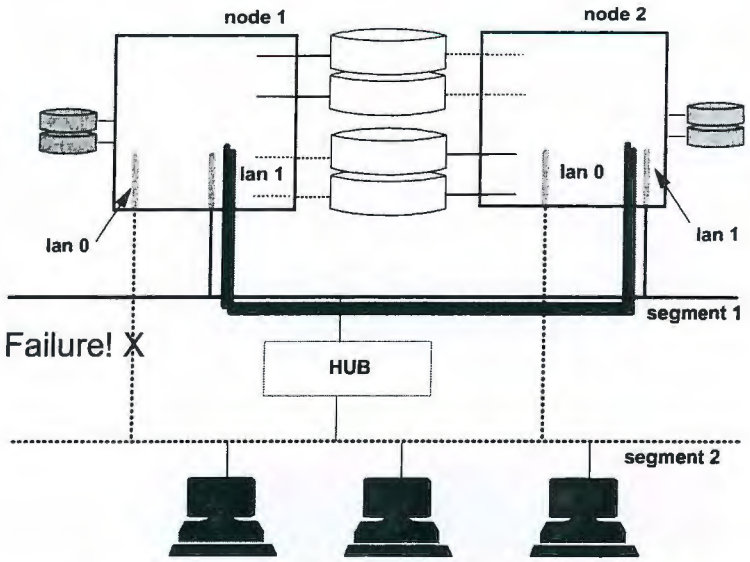
NOTE On Ethernet networks, MC/ServiceGuard supports local failover between network interfaces configured with "Ethernet protocol" or between network interfaces configured with "SNAP encapsulation within IEEE 802.3 protocol." You cannot use both protocols on the same interface, nor can you have a local failover between interfaces that are using different protocols.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1310
3702
Doc:

17.564

Another example of local switching is shown in Figure 3-4. In this case a failure affecting segment 2 causes both nodes to switch to the LAN cards attached to segment 1.

Figure 3-4 Local Switching After Cable Failure



Local network switching will work with a cluster containing one or more nodes. You may wish to design a single-node cluster in order to take advantages of this local network switching feature in situations where you need only one node and do not wish to set up a more complex cluster.

Remote Switching

A remote switch involves moving packages and their associated IP addresses to a new system. The new system must already have the same subnetwork configured and working properly, otherwise the packages will not be started. With remote switching, TCP connections are lost. TCP applications must reconnect to regain connectivity; this is not handled automatically. Note that if the package is dependent on multiple subnetworks, all subnetworks must be available on the target node before the package will be started.

The switching of relocatable IP addresses is shown in Figure 3-5 and Figure 3-6. Figure 3-5 shows a two node cluster in its original state with Package 1 running on Node 1 and Package 2 running on Node 2. Users

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1311
Nº 3702 Doc:

connect to node with the IP address of the package they wish to use. Each node has a stationary IP address associated with it, and each package has an IP address associated with it.

Figure 3-5 **Before Package Switching**

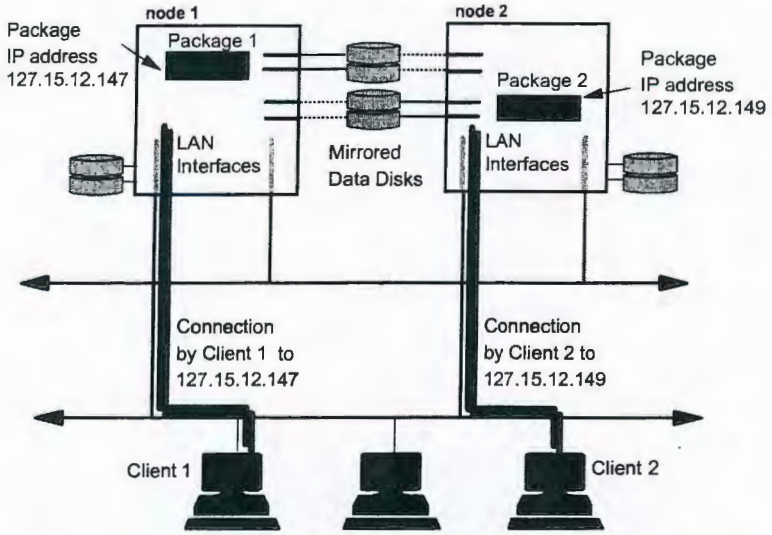
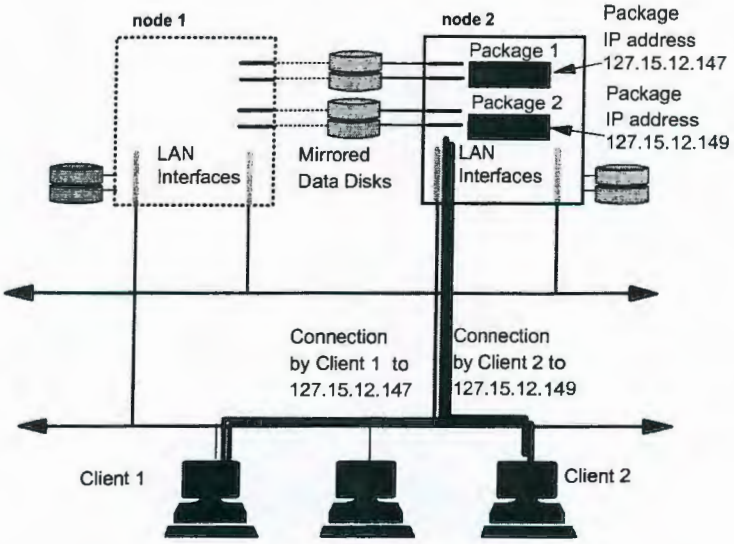


Figure 3-6 shows the condition where Node 1 has failed and Package 1 has been transferred to Node 2. Package 1's IP address was transferred to Node 2 along with the package. Package 1 continues to be available and is now running on Node 2. Also note that Node 2 can now access both Package A's disk and Package B's disk.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1312
Nº 3702

17.563

Figure 3-6 **After Package Switching**



ARP Messages after Switching

When a floating IP address is moved to a new interface, either locally or remotely, an ARP message is broadcast to indicate the new mapping between IP address and link layer address. An ARP message is sent for each IP address that has been moved. All systems receiving the broadcast should update the associated ARP cache entry to reflect the change.

Currently, the ARP messages are sent at the time the IP address is added to the new system. An ARP message is sent in the form of an ARP request. The sender and receiver protocol address fields of the ARP request message are both set to the same floating IP address. This ensures that nodes receiving the message will not send replies.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1313
3702
Doc:

Responses to Failures

MC/ServiceGuard responds to different kinds of failures in specific ways. For most hardware failures, the response is not user-configurable, but for package and service failures, you can choose the system's response, within limits.

Transfer of Control (TOC) When a Node Fails

The most dramatic response to a failure in an MC/ServiceGuard cluster is an HP-UX TOC (Transfer of Control), which is an immediate halt of the SPU without a graceful shutdown. This TOC is done to protect the integrity of your data.

A TOC is done if there is a kernel hang, a kernel spin, a runaway real-time process, or if the MC/ServiceGuard daemon, *cmcld*, fails. During this event, a system dump is performed and the following message is sent to the console:

```
MC/ServiceGuard: Unable to maintain contact with cmcld daemon.
Performing TOC to ensure data integrity.
```

A TOC is also initiated by MC/ServiceGuard itself under specific circumstances. If the service failfast parameter is enabled in the package configuration file, the entire node will fail with a TOC whenever there is a failure of that specific service. If the package failfast parameter is enabled in the package configuration file, the entire node will fail with a TOC whenever there is a failure causing the package control script to exit. In addition, a node-level failure may also be caused by events independent of a package and its services. Loss of the heartbeat or loss of the MC/ServiceGuard or other critical daemons will cause a node to fail even when its packages and their services are functioning.

Responses to Hardware Failures

If a serious system problem occurs, such as a panic or physical disruption of the SPU's circuits, MC/ServiceGuard recognizes a node failure and transfers the packages currently running on that node to an adoptive node elsewhere in the cluster. The new location for each package is determined by that package's configuration file, which lists primary and alternate nodes for the package. Transfer of a package to another node does not transfer the program counter. Processes in a transferred

CPMI - CORREIOS
Fls Nº 1314
3702
Doc:

package will restart from the beginning. In order for an application to be expeditiously restarted after a failure, it must be "crash-tolerant"; that is, all processes in the package must be written so that they can detect such a restart. This is the same application design required for restart after a normal system crash.

In the event of a LAN interface failure, a local switch is done to a standby LAN interface if one exists. If a heartbeat LAN interface fails and no standby is configured, the node fails with a TOC. If a data LAN interface fails without a standby, the node fails with a TOC only if *Package Failfast* (described further in the "Planning" chapter under "Package Configuration Planning") is enabled for the package.

Disk protection is provided by the separate product MirrorDisk/UX. In addition, separately available EMS disk monitors allow you to notify operations personnel when a failure takes place. Refer to the manual *Using the Event Monitoring Service* (HP part number B5735-90001) for additional information.

MC/ServiceGuard does not respond directly to power failures, although a loss of power to an individual cluster component may appear to MC/ServiceGuard like the failure of that component, and will result in the appropriate switching behavior.

Power protection is provided by PowerTrust, HP's uninterruptible power supply.

Responses to Package and Service Failures

In the default case, the failure of the package or of a service within a package causes the package to shut down by running the control script with the 'stop' parameter, and then restarting the package on an alternate node. If the package manager receives a report of an EMS monitor event showing that a resource is down, the package fails.

If you wish, you can modify this default behavior by specifying that the node should crash (TOC) before the transfer takes place. In cases where package shutdown may take a long time but the package is crash-tolerant and can recover quickly on restart, this option can make the package and its associated applications available to users more quickly. Remember, however, that when the node crashes, *all* packages on the node are halted abruptly.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1315
3702
Doc:

17.559

The settings of package and service failfast parameters during package configuration will determine the exact behavior of the package and the node in the event of failure. The section on "Package Configuration Parameters" in the "Planning" chapter contains details on how to choose an appropriate failover behavior.

Service Restarts

You can allow a service to restart locally following a failure. To do this, you indicate a number of restarts for each service in the package control script. When a service starts, the variable RESTART_COUNT is set in the service's environment. The service, as it executes, can examine this variable to see whether it has been restarted after a failure, and if so, it can take appropriate action such as cleanup.

Network Communication Failure

An important element in the cluster is the health of the network itself. As it continuously monitors the cluster, each node listens for heartbeat messages from the other nodes confirming that all nodes are able to communicate with each other. If a node does not hear these messages within the configured amount of time, a node timeout occurs, resulting in a TOC. In a two-node cluster, the use of an RS-232 line prevents a TOC from the momentary loss of heartbeat on the LAN due to network saturation. The RS232 line also assists in quickly detecting network failures when they occur.

RQS nº
CPMI - CORREIOS
Fls Nº 1316
3702
Doc

4 Planning and Documenting an HA Cluster

Building an MC/ServiceGuard cluster begins with a planning phase in which you gather and record information about all the hardware and software components of the configuration. Planning begins with a simple list of hardware and network components. As the installation and configuration continue, the list is extended and refined. After hardware installation, you can use the SAM high availability options or a variety of HP-UX commands to obtain information about your configuration; this information is entered on the worksheets provided in this chapter. During the creation of the cluster, the planning worksheets provide the values that are input with SAM or edited into the configuration files and control scripts.

This chapter assists you in the following planning areas:

- General Planning
- Hardware Planning
- Power Supply Planning
- Volume Group and Physical Volume Planning
- Cluster Configuration Planning
- Package Configuration Planning

The description of each planning step in this chapter is accompanied by a worksheet on which you can optionally record the parameters and other data relevant for successful setup and maintenance. As you go through each step, record all the important details of the configuration so as to document your production system. During the actual configuration of the cluster, refer to the information from these worksheets. A complete set of blank worksheets is in Appendix G.

NOTE Planning and installation overlap considerably, so you may not be able to complete the worksheets entirely before you proceed to the actual configuration. In cases where the worksheet is incomplete, fill in the missing elements to document the system as you proceed with the configuration.

ROS nº 03/2005 CN - CPMI - CORREIOS
Fls Nº 1317
3702
Doc:

17.557

Subsequent chapters describe configuration and maintenance tasks in detail.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1318
Doc 3702

17556

General Planning

A clear understanding of your high availability objectives will quickly help you to define your hardware requirements and design your system. Use the following questions as a guide for general planning:

1. What applications must continue to be available in the event of a failure?
2. What system resources (processing power, networking, SPU memory, disk space) are needed to support these applications?
3. How will these resources be distributed among the nodes in the cluster during normal operation?
4. How will these resources be distributed among the nodes of the cluster in all possible combinations of failures, especially node failures?
5. How will resources be distributed during routine maintenance of the cluster?
6. What are the networking requirements? Are all networks and subnets available?
7. Have you eliminated all single points of failure? For example:
   - network points of failure.
   - disk points of failure.
   - electrical points of failure.
   - application points of failure.

Planning for Expansion

When you first set up the cluster, you indicate a set of nodes and define a group of packages for the initial configuration. At a later time, you may wish to add additional nodes and packages, or you may wish to use additional disk hardware for shared data storage. If you intend to expand your cluster *without the need to bring it down*, careful planning of the initial configuration is required. Use the following guidelines:

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1319
Nº Doc. 3702

17.559

- Set the Maximum Configured Packages parameter (described later in this chapter in the "Cluster Configuration Planning" section) high enough to accomodate the additional packages you plan to add. Keep in mind that adding package capacity uses memory resources (600K per package).
- Plan SCSI bus cabling to allow the addition of more disk hardware for shared data storage if needed. You should attach inline SCSI terminator cables to SCSI ports that you intend to use for additional devices. This allows you to add them while the bus is still active.
- Remember the rules for cluster locks when considering expansion. A cluster of two nodes must have a cluster lock, while a cluster of five or more nodes may *not* have a cluster lock. This means that if you intend to expand to a size greater than four nodes while the cluster is running, you should begin with at least three nodes and not configure a cluster lock.
- Networks should be pre-configured into the cluster configuration if they will be needed for packages you will add later while the cluster is running.
- Resources monitored by EMS should be pre-configured into the cluster configuration if they will be needed for packages you will add later while the cluster is running. Once a resource dependency is configured for any package in the cluster, it will always be available for later packages to use. However, you cannot add a never-before-configured resource to a package while the cluster is running.

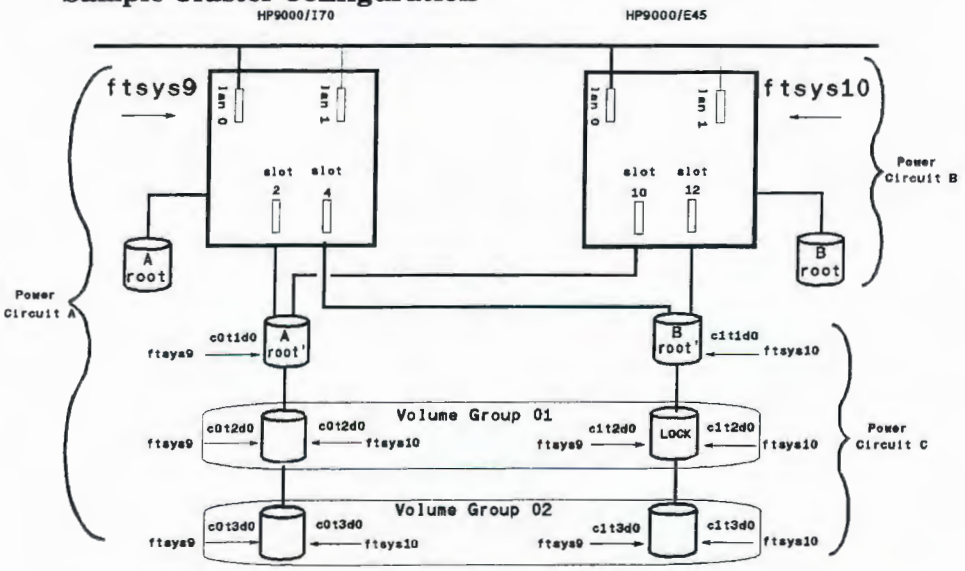
Refer to the chapter on "Cluster and Package Maintenance" for more information about changing the cluster configuration dynamically, that is, while the cluster is running.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1320
Doc: 3702

Hardware Planning

Hardware planning requires examining the physical hardware itself. One useful procedure is to sketch the hardware configuration in a diagram that shows adapter cards and buses, cabling, disks and peripherals. A sample diagram for a two-node cluster is shown in Figure 4-1.

Figure 4-1 Sample Cluster Configuration



Create a similar sketch for your own cluster, and record the information on the Hardware Worksheet. Indicate which device adapters occupy which slots, and determine the bus address for each adapter. Update the details as you do the cluster configuration (described in Chapter 3). *Use one form for each SPU*. The form has three parts:

- SPU Information
- Network Information
- Disk I/O Information

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1321
Doc: 3702

17.553

SPU Information

All HP 9000 Series 800 HP-PA SPUs are supported by MC/ServiceGuard and different models can be mixed in the same cluster. This includes both uniprocessor and multiprocessor computers. HP 9000 Series 700 SPUs are not supported by MC/ServiceGuard.

SPU information includes the basic characteristics of the S800 systems you are using in the cluster. On the worksheet, include the following items:

S800 Series Number — Enter the series number, e.g., T600.

Host Name — Enter the name to be used on the system as the host name.

Memory Capacity — Enter the memory in MB.

Number of I/O slots — Indicate the number of slots.

NFS diskless clusters and NetLS servers are not supported.

Network Information

MC/ServiceGuard monitors LAN interfaces as well as serial lines (RS232) configured to carry cluster heartbeat only.

LAN Information

While a minimum of one LAN interface per subnet is required, at least two LAN interfaces, one primary and one or more standby, are needed to eliminate single points of network failure.

It is recommended that you configure heartbeats on all subnets, including those to be used for client data. On the worksheet, enter the following for each LAN interface:

Subnet Name — Enter the IP address mask for the subnet. Note that heartbeat IP addresses must be on the same subnet on each node.

ECT 03/2005 - CN - CPMI - CORREIOS
1322
Fls Nº
Nº Doc: 3702

Interface Name	Enter the name of the LAN card as used by this node to access the subnet. This name is shown by lanscan after you install the card.
IP Address	Enter this node's host IP address intended to be used on this interface. The IP address is a string of digits separated with periods in the form 'nnn.nnn.nnn.nnn'. If the interface is a standby and does not have an IP address, enter 'Standby.'
Kind of LAN Traffic	Identify the purpose of the subnet. Valid types include the following: • Heartbeat • Client Traffic • Standby

Label the list to show the subnets that belong to a bridged net.

Information from this section of the worksheet is used in creating the subnet groupings and identifying the IP addresses in the configuration steps for the cluster manager and package manager.

RS232 Information

If you plan to configure a serial line (RS232) to carry heartbeat, you need to determine the serial device file that corresponds with the serial port on each node.

1. If you are using a MUX panel, make a note of the system slot number that corresponds to the MUX and also note the port number that appears next to the selected port on the panel.
2. On each node, use ioscan -fnC tty to display hardware addresses and device file names. For example:

   # ioscan -fnC tty

   This lists all the device files associated with each RS232 device on a specific node.
3. Once you have identified the device files, verify your connection as follows. Assume that node 1 uses /dev/tty0p0, and node 2 uses /dev/tty0p6.
   - From a terminal on node 1, issue the following command:

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1323
Doc 3702

 # cat < /dev/tty0p0

- From a terminal on node 2, issue the following command:

  # cat /etc/passwd > /dev/tty0p6

  The contents of the password file should be displayed on the terminal on node 1.

4. On the worksheet, enter the following:

Node Name	Name of the node
RS232 Device File	Enter the device file name corresponding to a serial interface on each node. This parameter is known as `SERIAL_DEVICE_FILE` in the ASCII configuration file.

Setting SCSI Addresses for the Largest Expected Cluster Size

SCSI standards define priority according to SCSI address. To prevent controller starvation on the SPU, the SCSI interface cards must be configured at the highest priorities. Therefore, when configuring a highly available cluster, you should give nodes the highest priority SCSI addresses, and give disks addresses of lesser priority.

For Fast/Wide SCSI, high priority starts at seven, goes down to zero, and then goes from 15 to eight. Therefore, seven is the highest priority and eight is the lowest priority. For example, if there will be a maximum of four nodes in the cluster, and all four systems will share a string of disks, then the SCSI address must be uniquely set on the interface cards in all four systems, and must be high priority addresses. So the addressing for the systems and disks would be as follows:

Table 4-1 Fast/Wide SCSI Addressing in Cluster Configuration

System or Disk	Host Interface SCSI Address
Primary System A	7
Primary System B	6
Primary System C	5

CPMI - CORREIOS
Fls Nº 1324
Doc:
Nº 3702

System or Disk	Host Interface SCSI Address
Primary System D	4
Disk #1	3
Disk #2	2
Disk #3	1
Disk #4	0
Disk #5	15
Disk #6	14
Others	13 - 8

Disk I/O Information

This part of the worksheet lets you indicate where disk device adapters are installed. Enter the following items on the worksheet for each disk connected to each disk device adapter on the node:

Bus Type Indicate the type of bus. Supported busses are single-ended SCSI, F/W SCSI and FL (fiber link).

Slot Number Indicate the slot number in which the card is inserted. For both F/W SCSI and FL disks, use the even number printed at the bottom of the slot. (Not relevant for D and K systems.)

Address Enter the bus hardware path number, which will be seen on the system later when you use ioscan to display hardware. The address is given by the formula 4*(slot number). E.g., for slot number 4, the hardware path number is 16. (Not relevant for D and K systems.)

Disk Device File Enter the disk device file name. To display the name use the ioscan -fnC *disk* command,

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1325
Doc 3702

Information from this section of the worksheet is used in creating the mirrored disk configuration using Logical Volume Manager. In addition, it is useful to gather as much information as possible about your disk configuration. You can obtain information about available disks by using the following commands:

- diskinfo
- ioscan -fnC *disk*
- lssf /dev/dsk/c*
- bdf
- mount
- swapinfo
- vgdisplay -v
- lvdisplay -v
- lssf /dev/*dsk/*d0

These are standard HP-UX commands. See their man pages for information of specific usage.

The commands should be issued from *all nodes* after installing the hardware and rebooting the system. The information will be useful when doing LVM and cluster configuration. The output from the lssf command can be marked to indicate which physical volume group a disk is assigned to.

ECT 1349 7
RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1326
3702
Doc:

Hardware Configuration Worksheet

The following worksheet will help you organize and record your specific cluster hardware configuration. Make as many copies as you need. Complete the worksheet and keep it for future reference.

```
=============================================================================
SPU Information:

S800 Host Name ____ftsys9__________    S800 Series No _____892___________

Memory Capacity ____128 MB _________   Number of I/O Slots _____12_______
=============================================================================
LAN Information:

Name of          Name of              Node IP              Traffic
Subnet __Blue___ Interface ___lan0___ Addr___35.12.16.10__ Type   ____HB_____

Name of          Name of              Node IP              Traffic
Subnet __Blue___ Interface ___lan2___ Addr_______________  Type   _standby___

Name of          Name of              Node IP              Traffic
Subnet __Red____ Interface ___lan1___ Addr___35.12.15.12_ Type   _HB, clien
=============================================================================
Serial (RS232) Heartbeat Interface Information:

Node Name ____node1___________ RS232 Device File ___/dev/tty0p0__

Node Name ____node2___________ RS232 Device File ___/dev/tty0p0__
=============================================================================
X.25 Information

OTS subnet  _____________________ OTS subnet  _____________________

=============================================================================
Disk I/O Information for Shared Disks:

Bus Type _SCSI_ Slot Number _4__ Address _16_ Disk Device File /dev/dsk/c0t1d0

Bus Type _SCSI_ Slot Number _6_  Address _24_ Disk Device File /dev/dsk/c0t2d0

Bus Type ______ Slot Number ___  Address ____ Disk Device File  ____________

Bus Type ______ Slot Number ___  Address ____ Disk Device File  ____________


Attach a printout of the output from ioscan -fnC disk command
after installing disk hardware and rebooting the system.  Mark this
printout to indicate which physical volume group each disk belongs to.
```


RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1327
Doc: 3702

Power Supply Planning

There are two sources of power for your cluster which you will have to consider in your design: line power and uninterruptible power sources (UPS). Loss of a power circuit should not bring down the cluster. No more than half of the nodes should be on a single power source. If a power source supplies exactly half of the nodes, it must not also supply the cluster lock disk or the cluster will not be able to reform after a failure. See the section on cluster locks in "Cluster Configuration Planning" for more information.

To provide a high degree of availability in the event of power failure, use a separate UPS at least for each node's SPU and for the cluster lock disk, and ensure that disks which will be configured as members of separate physical volume groups are connected to different power supplies. This last rule enables disk mirroring to take place between physical disks that are connected to different power supplies as well as being on different I/O busses.

To prevent confusion, it is suggested that you label each hardware unit and power supply unit clearly with a different unit number. Indicate on the Power Supply Worksheet the specific hardware units you are using and the power supply to which they will be connected. Enter the following label information on the worksheet:

S800 Host Name Enter the host name for each SPU.

Disk Unit Enter the disk drive unit number for each disk.

Tape Unit Enter the tape unit number for each backup device.

Other Unit Enter the number of any other unit.

Power Supply Enter the power supply unit number of the UPS to which the host or other device is connected.

Be sure to follow UPS and cabinet power limits as well as SPU power limits.

NOTE Battery backup functionality on the Series 890 system is not supported by MC/ServiceGuard.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1328
Doc: 3702

Power Supply Configuration Worksheet

The following worksheet will help you organize and record your specific power supply configuration. Make as many copies as you need. Fill out the worksheet and keep it for future reference.

```
================================================================================
SPU Power:

S800 Host Name ____ftsys9_________    Power Supply _____1_______________

S800 Host Name ____ftsys10________    Power Supply _____2_______________

================================================================================
Disk Power:

Disk Unit _________1_______________   Power Supply ____3_________________

Disk Unit _________2_______________   Power Supply ____4_________________

Disk Unit _____________________________   Power Supply _____________________

Disk Unit _____________________________   Power Supply _____________________

Disk Unit _____________________________   Power Supply _____________________

Disk Unit _____________________________   Power Supply _____________________

================================================================================
Tape Backup Power:

Tape Unit _____________________________   Power Supply _____________________

Tape Unit _____________________________   Power Supply _____________________

================================================================================
Other Power:

Unit Name _____________________________   Power Supply _____________________

Unit Name _____________________________   Power Supply _____________________
```


17.546
RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1329
Doc 3702

Volume Group and Physical Volume Planning

When designing your disk layout using LVM, you should consider the following:

- The root disk should belong to its own volume group.
- The volume groups that contain high availability applications, services, or data must be on a bus or busses available to the primary node and all adoptive nodes.
- High availability applications, services, and data should be placed in a separate volume groups from non-high availability applications, services, and data.
- You must group high availability applications, services, and data, whose control needs to be transferred together, onto a single volume group or a series of volume groups.
- You must not group two different high availability applications, services, or data, whose control needs to be transferred independently, onto the same volume group.
- Your root disk must not belong to a volume group that can be activated on another node.

If you plan to use the EMS HA Disk Monitor, refer to the section on "Rules for Using EMS Disk Monitor with MC/ServiceGuard" in the manual *Using EMS HA Monitors*.

Volume Group and Physical Volume Worksheet

The following worksheet will help you organize and record your specific physical disk configuration. Make as many copies as you need. Fill out the worksheet and keep it for future reference. If you are using disk arrays, use the worksheet in the next section, "Volume Group and PV Links Worksheet."

RQS nº 03/2005 - CN - CPMI - CORREIOS
1330
Fls Nº
3702

It is recommended that you use volume group names other than the default volume group names (vg01, vg02, etc.). Choosing volume group names that represent the high availability applications that they are associated with (for example, /dev/vgdatabase will simplify cluster administration.

This worksheet only includes volume groups and physical volumes. The Package Configuration worksheet (presented later in this chapter) contains more space for recording information about the logical volumes and filesystems that are part of each volume group.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1331
3702

Volume Group and PV Links Worksheet

The following worksheet will help you organize and record your specific physical disk configuration if you are using PV (alternate) links with disk arrays. Make as many copies as you need. Fill out the worksheet and keep it for future reference.

```
================================================================================

Volume Group Name:      _________/dev/vg01_____________________________________

Name of First Physical Volume Group:  _______bus0_____________________________

Physical Volume Name:   ____________/dev/dsk/c1t2d0____________________________

Physical Volume Name:   ____________/dev/dsk/c2t2d0____________________________

Physical Volume Name:   ____________/dev/dsk/c3t2d0____________________________

Physical Volume Name:   _______________________________________________________

Physical Volume Name:   _______________________________________________________

Physical Volume Name:   _______________________________________________________

Physical Volume Name:   _______________________________________________________

Name of Second Physical Volume Group: _______bus1_____________________________

Physical Volume Name:   _____________/dev/dsk/c4t2d0___________________________

Physical Volume Name:   _____________/dev/dsk/c5t2d0___________________________

Physical Volume Name:   _____________/dev/dsk/c6t2d0___________________________

Physical Volume Name:   _______________________________________________________

Physical Volume Name:   _______________________________________________________

Physical Volume Name:   _______________________________________________________

Physical Volume Name:   _______________________________________________________

Physical Volume Name:   _______________________________________________________
```


RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1332
Doc: 3102

Cluster Configuration Planning

A cluster should be designed to provide the quickest possible recovery from failures. The actual time required to recover from a failure depends on several factors:

- The length of the cluster heartbeat interval and node timeout. They should each be set as short as practical, but not shorter than 1000000 (one second) and 2000000 (two seconds), respectively.
- The design of the run and halt instructions in the package control script. They should be written for fast execution.
- The availability of raw disk access. Applications that use raw disk access should be designed with crash recovery services.
- The application and database recovery time. They should be designed for the shortest recovery time.

In addition, you must provide consistency across the cluster so that:

- User names are the same on all nodes.
- UIDs are the same on all nodes.
- GIDs are the same on all nodes.
- Applications in the system area are the same on all nodes.
- System time is consistent across the cluster.
- Files that could be used by more that one node, such as /usr files, must be the same on all nodes.

Choosing the Cluster Lock Volume Group

A specific disk is identified in the cluster configuration file as holding the cluster lock. This disk must be accessible from all nodes in the cluster. The purpose of the cluster lock is to ensure that only one new cluster is formed in the event that exactly half of the previously clustered nodes try to form a new cluster. It is critical that only one new cluster is formed and that it alone has access to the disks specified in its packages.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1333
Doc 3702

Cluster Lock and Re-formation Time

The acquisition of the cluster lock takes different amounts of time depending on the disk I/O interface that is used. After all the disk hardware is configured, use the cmquerycl command specifying all the nodes in the cluster to display a list of available disks and the re-formation time associated with each. Example:

 # cmquerycl -v -n ftsys9 -n ftsys10

Alternatively, you can use SAM to display a list of cluster lock physical volumes, including the re-formation time.

The following list shows disk interface types in descending order of cluster lock disk acquisition/re-formation time:

- Any combination of HP-HSC and HP-PB disks on F/W SCSI
- Fiber Link disks
- HP-PB disks on single-ended SCSI

By default, MC/ServiceGuard selects the disk with the fastest re-formation time. But you may need to choose a different disk because of power considerations. Remember that the cluster lock disk should be separately powered, if possible.

Heartbeat Subnet and Re-formation Time

The speed of cluster re-formation is partially dependent on the type of hearbeat network that is used. Ethernet results in a slower failover time than the other types. If two or more heartbeat subnets are used, the one with the fastest failover time is used.

Planning for Expansion

You can add additional cluster nodes after the cluster is up and running, but doing so without bringing down the cluster requires you to follow some rules. Recall that a cluster with more than 4 nodes may not have a cluster lock. Thus, if you plan to add enough nodes to bring the total to more than 4, you must start with 3 nodes, since a two-node cluster requires a cluster lock. Also, new nodes added to the cluster must be on the same subnet as the other cluster nodes.

ROS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1334
Doc: 3702

Cluster Manager Parameters

For the operation of the cluster manager, you need to define a set of cluster parameters. These are stored in the binary cluster configuration file, which is located on all nodes in the cluster. These parameters can be entered by using SAM or by editing the cluster configuration template file created by issuing the cmquerycl command, as described in the chapter "Building an HA Cluster Configuration." The parameter names given below are the names that appear in SAM. The names coded in the ASCII cluster configuration file appear at the end of each entry.

The following parameters must be identified:

Cluster Name

The name of the cluster as it will appear in the output of cmviewcl and other commands, and as it appears in the cluster configuration file.

In the ASCII cluster configuration file, this parameter is `CLUSTER_NAME`.

The cluster name must not contain any of the following illegal characters: '/', '\', and '*'. All other characters are legal.

Cluster Nodes

The hostname of each system that will be a node in the cluster.

In the ASCII cluster configuration file, this parameter is `NODE_NAME`.

Cluster Aware Volume Group

The name of a volume group whose disks are attached to at least two nodes in the cluster. Such disks are considered cluster aware.

In the ASCII cluster configuration file, this parameter is `VOLUME_GROUP`.

Heartbeat Subnet

IP notation in SAM indicating the subnet that will carry the cluster heartbeat. Note that heartbeat IP addresses must be on the same subnet on each node.

In the ASCII cluster configuration file, this parameter is `HEARTBEAT_IP`.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1335
Doc 3702

ECT 17.539 J

RS232 Heartbeat Network

The name of the device file that corresponds to serial (RS232) port that you have chosen on each node. Specify this parameter when you are using RS232 as a heartbeat line.

In the ASCII cluster configuration file, this parameter is `SERIAL_DEVICE_FILE`.

Monitored Non-Heartbeat Subnet

The IP address of each monitored subnet that does not carry the cluster heartbeat. You can identify any number of subnets to be monitored. If you want to separate application data from heartbeat messages, define a monitored non-heartbeat subnet here.

In the ASCII cluster configuration file, this parameter is `STATIONARY_IP`.

Lock Volume Group

The volume group containing the physical disk volume on which a cluster lock is written. Identifying a cluster lock volume group is essential in a two-node cluster. If you are creating two cluster locks, enter the volume group name or names for both locks.

In the ASCII cluster configuration file, this parameter is `FIRST_CLUSTER_LOCK_VG` for the first lock volume group. If there is a second lock volume group, the parameter `SECOND_CLUSTER_LOCK_VG` is included in the file on a separate line.

Physical Volumes

The name of the physical volume within the Lock Volume Group that will have the cluster lock written on it. Enter the physical volume name as it appears on both nodes in the cluster (the same physical volume may have a different name on each node). If you are creating two cluster locks, enter the physical volume names for both locks.

In the ASCII cluster configuration file, this parameter is `FIRST_CLUSTER_LOCK_PV` for the first physical lock volume and `SECOND_CLUSTER_LOCK_PV` for the second

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1336
Nº 3702
Doc:

physical lock volume. If there is a second physical lock volume, the parameter `SECOND_CLUSTER_LOCK_PV` is included in the file on a separate line.

Disk Unit

This information is for a label to be attached to each disk drive. Enter the number of the disk drive unit on which the physical volume is located.

Power Supply

This information is for a label to be attached to each UPS. Enter the number of the power supply to which the physical volume is connected.

Heartbeat Interval

The normal interval between the transmission of heartbeat messages from one node to the other in the cluster. Enter a number of seconds. Default: 1 second. The interval should not be set smaller than this.

In the ASCII cluster configuration file, this parameter is `HEARTBEAT_INTERVAL`, and its value is entered in microseconds.

Node Timeout

The time after which a node may decide that the other node has become unavailable and initiate reconfiguration. Enter a number of seconds. Default: 2 seconds. Minimum is 2 * (Heartbeat Interval).

In the ASCII cluster configuration file, this parameter is `NODE_TIMEOUT`, and its value is entered in microseconds.

Maximum Configured Packages

This parameter sets the maximum number of packages that can be configured in the cluster. The default is 0, which means that you must set this parameter if you want to use packages. The greatest possible value is 30.

Set this parameter to a value that is high enough to accomodate a reasonable amount of future package additions without the need to bring down the cluster to reset the parameter. However, be sure not to set the parameter so high that memory is wasted. Each configured package requires about 600 K of lockable memory.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1337
3702
Doc:

In the ASCII cluster configuration file, this parameter is known as MAX_CONFIGURED_PACKAGES.

Network Polling Interval

The frequency at which the networks configured for MC/ServiceGuard are checked. The current default is 2 seconds. Thus every 2 seconds, the cluster manager polls each network interface to make sure it can still send and receive information. Changing this value can affect how quickly a network failure is detected.

In the ASCII cluster configuration file, this parameter is NETWORK_POLLING_INTERVAL, and its value is entered in microseconds.

Autostart Delay

The amount of time a node waits before it stops trying to join a cluster during automatic cluster startup. All nodes wait this amount of time for other nodes to begin startup before the cluster completes the operation. The time should be selected based on the slowest boot time in the cluster. Enter a number of seconds equal to the boot time of the slowest booting node minus the boot time of the fastest booting node plus 600 seconds (ten minutes). Default: 600 seconds.

In the ASCII cluster configuration file, this parameter is AUTO_START_TIMEOUT, and its value is entered in microseconds.

ROS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1338
3702
Doc:

Cluster Configuration Worksheet

The following worksheet will help you to organize and record your cluster configuration. Make as many copies as you need. Complete and save this worksheet for future reference.

```
=============================================================================
Name and Nodes:
=============================================================================

Cluster Name: ____cluster1_____________

Node Names: ______ftsys9, ftsys10_____________________________

Maximum Configured Packages: _______6_____________

Cluster Volume Groups: ___/dev/vg01, /dev/vg02_________

=============================================================================
Subnets:
=============================================================================
Heartbeat IP Addresses: ____15.13.171.32 and 192.6.7.3_____________

Non-Heartbeat IP Addresses: __192.6.143.10_________

=============================================================================
Cluster Lock Volume Groups and Volumes:
=============================================================================
First Lock VG:  |    First Lock Physical Volume:

 ___/dev/vg01___|Name (Node 1): /dev/dsk/c1t2d0__Disk Unit No: __Power Unit:

                |Name (Node 2): /dev/dsk/c1t2d0__Disk Unit No: __Power Unit:

Second Lock VG: |  Second Lock Physical Volume:

 _______________|Name (Node 1): _______________Disk Unit No: __Power Unit:

                |Name (Node 2): _______________Disk Unit No: __Power Unit:

=============================================================================
Timing Parameters:
=============================================================================

Heartbeat Interval: __1 sec__
=============================================================================

Node Timeout: __2 sec_
=============================================================================

Network Polling Interval: _2 sec_
=============================================================================

Autostart Delay: __10 min__
```


RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1339
Nº Doc: 3702

Package Configuration Planning

Planning for packages involves assembling information about each group of highly available services. Some of this information is used in creating the package configuration file, and some is used for editing the package control script.

NOTE Volume groups that are to be activated by packages must also be defined as cluster aware in the cluster configuration file. See the previous section on "Cluster Configuration Planning."

Logical Volume and Filesystem Planning

You may need to use logical volumes in volume groups as part of the infrastructure for package operations on a cluster. When the package moves from one node to another, it must be able to access data residing on the same disk as on the previous node. This is accomplished by activating the volume group and mounting the file system that resides on it.

In MC/ServiceGuard, high availability applications, services, and data are located in volume groups that are on a shared bus. When a node fails, the volume groups containing the applications, services, and data of the failed node are deactivated on the failed node and activated on the adoptive node. In order to do this, you have to configure the volume groups so that they can be transferred from the failed node to the adoptive node.

As part of planning, you need to decide the following:

- What volume groups are needed?
- How much disk space is required, and how should this be allocated in logical volumes?
- What file systems need to be mounted for each package?
- Which nodes need to import which logical volume configurations.
- If a package moves to an adoptive node, what effect will its presence have on performance?

Create a list by package of volume groups, logical volumes, and file systems. Indicate which nodes need to have access to common filesystems at different times.

It is recommended that you use customized logical volume names that are different from the default logical volume names (lvol1, lvol2, etc.). Choosing logical volume names that represent the high availability applications that they are associated with (for example, lvoldatabase) will simplify cluster administration.

To further document your package-related volume groups, logical volumes, and file systems on each node, you can add *commented* lines to the /etc/fstab file. The following is an example for a database application:

```
# /dev/vg01/lvoldb1 /applic1 vxfs defaults 0 1    # These six entries are
# /dev/vg01/lvoldb2 /applic2 vxfs defaults 0 1    # for information purposes
# /dev/vg01/lvoldb3 raw_tables ignore ignore 0 0 # only. They record the
# /dev/vg01/lvoldb4 /general vxfs defaults 0 2    # logical volumes that
# /dev/vg01/lvoldb5 raw_free ignore ignore 0 0    # exist for MC/ServiceGuard's
# /dev/vg01/lvoldb6 raw_free ignore ignore 0 0    # HA package. Do not uncomment.
```

Create an entry for each logical volume, indicating its use for a file system or for a raw device.

CAUTION

Do *not* use /etc/fstab to mount file systems that are used by MC/ServiceGuard packages.

Details about creating, exporting, and importing volume groups in MC/ServiceGuard are given in the chapter on "Building an HA Cluster Configuration."

Monitoring Registered Package Resources

MC/ServiceGuard has access to a registry of resources that can be monitored as package dependencies. The registry is the core of the Event Monitoring Service (EMS). Once an EMS registered resource is configured as a package dependency, MC/ServiceGuard can fail a package to another node based on messages the resource's monitor returns. Monitors for individual resources may be provided by hardware or software vendors from time to time. A specific group of HA EMS monitors for disk, LAN, and system status information is available from HP as a separate product. Refer to the manual *Using EMS HA Monitors* (B5735-90001) for additional information.

You can specify a registered resource for a package by selecting it from the list of available resources displayed in the SAM package configuration area. The size of the list displayed by SAM depends on

... 03/2005 - CN -
... MI - CORREIOS
Fls Nº 1341
... 3702

ECT 7533

which resource monitors have been registered on your system. Alternatively, you can obtain information about registered resources on your system by using the command /opt/resmon/bin/resls. For additional information, refer to the man page for resls(1m).

Choosing Switching and Failover Behavior

Switching IP addresses from one LAN card to another may take place if Automatic Switching is set to Enabled in SAM (`NET_SWITCHING_ENABLED` set to YES in the ASCII package configuration file). Automatic Switching Enabled is the default. The following table describes different types of failover behavior and the settings that determine each behavior in SAM or in the ASCII package configuration file.

... 03/2005 - CN -
... - CORREIOS
Fls Nº 1342
Nº 3702

Table 4-2 Package Failover Behavior

Switching Behavior	Options in SAM	Parameters in ASCII File
Package IP address switches to standby LAN card transparently on LAN card failure	• Automatic Switching set to Enabled for the package (Default)	• NET_SWITCHING_ENABLED set to YES for the package (Default)
Package switches normally after detection of failure or report of an EMS monitor event showing that a resource on which the package depends is down. Halt script runs before switch takes place (default behavior.)	• Package Failfast set to Disabled. (Default) • Service Failfast set to Disabled for all services. (Default) • Automatic Switching set to Enabled for the package. (Default)	• NODE_FAIL_FAST_ENABLED set to NO. (Default) • SERVICE_FAIL_FAST_ENABLED set to NO for all services. (Default) • PKG_SWITCHING_ENABLED set to YES for the package. (Default)

- CORREIOS
Fls Nº 1343
Doc: 3702

Switching Behavior	Options in SAM	Parameters in ASCII File
All packages switch following a TOC (Transfer of Control, an immediate halt without a graceful shutdown) on the node when a specific service fails. Halt scripts are not run.	• Package Failfast set to Disabled • Service Failfast set to Enabled for a specific service • Automatic Switching set to Enabled for all packages.	• NODE_FAIL_FAST_ENABLED set to NO • SERVICE_FAIL_FAST_ENABLED set to YES for a specific service. • PKG_SWITCHING_ENABLED set to YES for all packages.
All packages switch following a TOC on the node when any service fails.	• Package Failfast set to Disabled. • Service Failfast set to Enabled for *all* services. • Automatic Switching set to Enabled for all packages.	• NODE_FAIL_FAST_ENABLED set to NO. • SERVICE_FAIL_FAST_ENABLED set to YES for *all* services. • PKG_SWITCHING_ENABLED set to YES for all packages.
All packages switch following a TOC on the node when the run or halt script exits with an error other than 0 or 1. This may be caused by an EMS monitor event showing that a resource is down	• Package Failfast set to Enabled. • Automatic Switching set to Enabled for all packages.	• NODE_FAIL_FAST_ENABLED set to YES. • PKG_SWITCHING_ENABLED set to YES for all packages.

Planning for Expansion

You can add packages to a running cluster. This process is described in the chapter "Cluster and Package Administration." When adding packages, be sure not to exceed the value of MAX_CONFIGURED_PACKAGES as defined in the cluster configuration file.

03/2005 - CN - CPMI - CORREIOS Fls Nº 1344 Nº 3702

Package Configuration File Parameters

Prior to generation of the package configuration file, assemble the following package configuration data. The parameter names given below are the names that appear in SAM. The names coded in the ASCII cluster configuration file appear at the end of each entry. The following parameters must be identified and entered on the worksheet *for each package*:

Package Name — The name of the package. The package name must be unique in the cluster. It is used to start, stop, modify, and view the package.

The package name must not contain any of the following illegal characters: '/', '\', and '*'. All other characters are legal.

Node Name — The names of primary and alternate nodes for the package, e.g., ftsys9 and ftsys10. The order in which you specify the node names is important. First list the primary node name, then the first adoptive node name, then the second adoptive node name, followed, in order, by additional node names. Transfer of control of the package will occur to the next adoptive node name listed in the package configuration file.

Control Script Pathname — Enter the full pathname of the package control script. (The script must reside in a directory that contains the string "cmcluster.") It is recommended that you use the same script as both the run and halt script. This script will contain both your package run instructions and your package halt instructions. When the package starts, its run script is executed and passed the parameter 'start'; similarly, at package halt time, the halt script is executed and passed the parameter 'stop'.

In the ASCII package configuration file, this parameter maps to the two separate parameters named `RUN_SCRIPT` and `HALT_SCRIPT`. Use the name of the single control script as the name of the `RUN_SCRIPT` and the `HALT_SCRIPT` in the ASCII file.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1345
Nº 3702
Doc:

If you wish to separate the package run instructions and package halt instructions into separate scripts, the package configuration file allows allows you to do this by naming two separate scripts. However, under most conditions, it is simpler to combine your run and halt instructions into a single package control script and repeat its name for both the `RUN_SCRIPT` and the `HALT_SCRIPT`.

NOTE If you choose to write separate package run and halt scripts, be sure to include identical configuration information (such as node names, IP addresses, etc.) in both scripts.

Ensure that this script is executable.

Run Script Timeout and Halt Script Timeout

Enter a number of seconds. If the script has not completed by the specified timeout value, MC/ServiceGuard will terminate the script. The default is 0, or no timeout.

If the timeout is exceeded:

- Control of the package will not be transferred.
- The run or halt instructions will not be run.
- Global switching will be disabled.
- The current node will be disabled from running the package.
- The control script will exit with status 1.

In the ASCII package configuration file, this parameter is called `RUN_SCRIPT_TIMEOUT` and `HALT_SCRIPT_TIMEOUT`. The default for both is 0 or `NO_TIMEOUT`. In the ASCII file, this parameter is entered in microseconds.

If the halt script timeout occurs, you may need to perform manual cleanup. See "Package Control Script Hangs or Failures" in Chapter 8.

RQS nº 03/2005 - CN - CPMI - CORREIOS
1346
Fls Nº
3702

Service Name Enter a unique name for each service. You can configure a maximum of 30 services per package.

In the ASCII package configuration file, this parameter is called `SERVICE_NAME`. Define one `SERVICE_NAME` entry for each service.

Service Fail Fast Enter Enabled or Disabled for each service. This parameter indicates whether or not the failure of a service results in the failure of a node. If the parameter is set to Enabled, in the event of a service failure, MC/ServiceGuard will halt the node on which the service is running with a TOC. The default is Disabled.

In the ASCII package configuration file, this parameter is `SERVICE_FAIL_FAST_ENABLED`, and possible values are YES and NO. The default is NO. Define one `SERVICE_FAIL_FAST_ENABLED` entry for each service.

The service name must not contain any of the following illegal characters: '/', '\', and '*'. All other characters are legal.

Service Halt Timeout In the event of a service halt, MC/ServiceGuard will first send out a SIGTERM signal to terminate the service. If the process is not terminated, MC/ServiceGuard will wait for the specified timeout before sending out the SIGKILL signal to force process termination. Default is 300 seconds (5 minutes).

In the ASCII package configuration file, this parameter is `SERVICE_HALT_TIMEOUT`. Define one `SERVICE_HALT_TIMEOUT` entry for each service.

Subnet Enter the IP subnets that are to be monitored for the package.

In the ASCII package configuration file, this parameter is called SUBNET.

Resource Name The name of a resource that is to be monitored by MC/ServiceGuard as a package dependency. A resource name is the name of an important attribute of a particular system resource. The resource name includes the entire hierarchy of resource class and subclass within which the resource exists on a system.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1347
Nº 3702

17.527

In the ASCII package configuration file, this parameter is called RESOURCE_NAME. Obtain the resource name from the list provided in SAM, or obtain it from the documentation supplied with the resource monitor.

A maximum of 60 resources may be defined per *cluster*. Note also the limit on Resource Up Values described below.

Resource Polling Interval

The frequency of monitoring an additional package resource. The default is 60 seconds. In the ASCII package configuration file, this parameter is called RESOURCE_POLLING_INTERVAL. The Resource Polling Interval appears on the list provided in SAM, or you can obtain it from the documentation supplied with the resource monitor.

Resource Up Value

The criteria for judging whether an additional package resource has failed or not. In the ASCII package configuration file, this parameter is called RESOURCE_UP_VALUE. The Resource Up Value appears on the list provided in SAM, or you can obtain it from the documentation supplied with the resource monitor.

You can configure a total of 15 Resource Up Values per package. For example, if there is only one resource in the package, then a maximum of 15 Resource Up Values can be defined. If there are two Resource Names defined and one of them has 10 Resource Up Values, then the other Resource Name can have only 5 Resource Up Values.

Automatic Switching

Enter Enabled or Disabled. The default is Enabled, which allows a package to start up normally on a cluster node. In the event of a failure, a value of Enabled permits MC/ServiceGuard to transfer the package to an adoptive node. If this parameter is set to Disabled, the package will not start up automatically when the cluster starts running.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1348
Nº Doc: 3702

In the ASCII package configuration file, this parameter is called PKG_SWITCHING_ENABLED, and possible values are YES and NO. The default is YES. If this parameter is set to NO, the package will not start up automatically when the cluster starts running.

Local Switching Enter Enabled or Disabled. In the event of a failure, this permits MC/ServiceGuard to switch LANs locally, that is, transfer to a standby LAN card. The default is Enabled.

In the ASCII package configuration file, this parameter is called NET_SWITCHING_ENABLED, and possible values are YES and NO. The default is YES.

Package Fail Fast Enabled In the event of the failure of the control script itself or the failure of a subnet or the report of an EMS monitor event showing that a resource is down, if this parameter is set to Enabled, MC/ServiceGuard will issue a TOC on the node where the control script fails. The default is Disabled.

In the ASCII package configuration file, this parameter is called NODE_FAIL_FAST_ENABLED, and possible values are YES and NO. The default is NO.

Package Control Script Variables

The control script that accompanies each package must also be edited to assign values to a set of variables. The following variables must be set:

Volume Groups, Logical Volumes, File Systems and Mount Options Determine the filesystems and corresponding logical volumes within the volume groups required. Example:

pkg1 requires /dev/vg01/lvol1 mounted on /vg01

Indicate the names of volume groups that are to be activated and deactivated, together with the logical volumes and file systems that are to be mounted. You

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1349
Doc: 3702

can also specify options that are to be used with the HP-UX **mount** command. On starting the package, the script activates a volume group, and it may mount logical volumes onto file systems. At halt time, the script unmounts the file systems and deactivates each volume group. All volume groups must be accessible on each target node.

In the ASCII package control script, these variables are arrays, as follows: `VG`, `LV`, `FS` and `FS_MOUNT_OPT`. For each file system (`FS`), you must identify a logical volume (`LV`). Include as many volume groups (`VG`s) as needed. If you are using raw files, the `LV`, `FS`, and `FS_MOUNT_OPT` entries are not needed.

Only cluster aware volume groups should be specified in package control scripts. To make a volume group cluster aware, enter it as part of the cluster configuration. See above, "Cluster Configuration Planning."

IP Addresses and SUBNETs

These are the IP addresses by which a package is mapped to a LAN card. Indicate the IP addresses and subnets for each IP address you want to add to an interface card.

In the ASCII package control script, these variables are entered in pairs. Example `IP[0]=192.10.25.12` and `SUBNET[0]=192.10.25.0`. (In this case the subnet mask is 255.255.255.0.)

Service Name

Enter a unique name for each specific service within the package. All services are monitored by MC/ServiceGuard. The service name, service command, and service restart parameters are entered in the package control script in groups of three. You may specify as many service names as you need. Each name must be unique within the cluster. The service name is the name used by cmrunserv and cmhaltserv inside the package control script.

In the ASCII package control script, enter values into an array known as `SERVICE_NAME`. Enter one service name for each service.

RQS nº 03/2005 - CN - CPMI - CORREIOS
1350
Fls Nº
3702
Doc:

17.524

Service Command

For each named service, enter a service command. This command will be executed through the control script by means of the cmrunserv command.

In the ASCII package control script, enter values into an array known as `SERVICE_CMD`. Enter one service command string for each service.

Service Restart Parameter

Enter a number of restarts. One valid form of the parameter is -r *n* where *n* is a number of retries. A value of "-r 0" indicates no retries. A value of "-R" indicates an infinite number of retries. The default is 0, or no restarts.

In the ASCII package control script, enter values into an array known as `SERVICE_RESTART`. Enter one restart value for each service.

For information on using a DTC with MC/ServiceGuard, see the chapter entitled "Configuring DTC Manager for Operation with MC/ServiceGuard" in the manual *Using the HP DTC Manager/UX*.

The package control script will clean up the environment and undo the operations in the event of an error.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1351
Doc 3702

Package Configuration Worksheet

Assemble your package configuration and control script data in a separate worksheet for each package.

```
================================================================================
Package Configuration File Data:
================================================================================

Package Name: _____pkg11_____________

Primary Node: _____ftsys9_____________

First Failover Node:____ftsys10_____________

Second Failover Node:_____________________________

Package Run Script: __/etc/cmcluster/pkg1/control.sh__Timeout: _NO_TIMEOUT_

Package Halt Script: __/etc/cmcluster/pkg1/control.sh_Timeout: _NO_TIMEOUT_

Package Switching Enabled?  __YES___ Local Switching Enabled?  ___YES__

Node Failfast Enabled?       ____NO____

Additional Package Resource:

Resource Name:___________ Polling Interval_______ Resource UP Value________

================================================================================

Package Control Script Data:
================================================================================

VG[0]___/dev/vg01 __LV[0]__/dev/vg01/lvol1__FS[0]____/mnt1__FS_MOUNT_OPT[0]___

VG[1]_____________LV[1]_____________FS[1]__________FS_MOUNT_OPT[1]___

VG[2]_____________LV[2]_____________FS[2]__________FS_MOUNT_OPT[2]___


IP[0] ___15.13.171.14 _____________ SUBNET[0]_______15.13.168________

IP[1] _____________________________ SUBNET[1]_____________________

X.25 Resource Name _____________

Service Name: __Svc1____ Run Command: __/usr/bin/MySvc -f_____Retries: _-r 2__

Service Fail Fast Enabled? ___NO___Service Halt Timeout __NO_TIMEOUT__________

Service Name: _________ Run Command: _____________________ Retries: _______

Service Fail Fast Enabled? _________Service Halt Timeout _________________
```


RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1352
Doc: 3702

- You must always deliberately select an item when choosing it from a list. Either click on the item or tab to it and press , then select **OK** to choose the item or items. An item is not selected by default even though it may appear to be highlighted.
- To make more than one selection from a list with a mouse, click on the first item with the left mouse button, then click on subsequent items by holding down **Ctrl** and pressing the left mouse button. Finally, select **OK** to choose the items.

The configuration and administration screens have extensive help associated with them.

If you are using MC/ServiceGuard commands to configure the cluster and packages, use the man pages for each command to obtain information about syntax and usage.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1353
Nº 3702
Doc:

- You must always deliberately select an item when choosing it from a list. Either click on the item or tab to it and press , then select **OK** to choose the item or items. An item is not selected by default even though it may appear to be highlighted.
- To make more than one selection from a list with a mouse, click on the first item with the left mouse button, then click on subsequent items by holding down **Ctrl** and pressing the left mouse button. Finally, select **OK** to choose the items.

The configuration and administration screens have extensive help associated with them.

If you are using MC/ServiceGuard commands to configure the cluster and packages, use the man pages for each command to obtain information about syntax and usage.

RQS nº 03/2005 - CN
CPMI - CORREIO
Fls Nº 1354
3702
Doc:

Preparing Your Systems

Before configuring your cluster, ensure that all cluster nodes possess the appropriate security files, kernel configuration and NTP (network time protocol) configuration.

Editing Security Files

MC/ServiceGuard makes use of ARPA services to ensure secure communication among cluster nodes. Before installing MC/ServiceGuard, you must identify the nodes in the cluster that permit access by the root user on other nodes. If you do not do this, MC/ServiceGuard will not be able to copy files among nodes during configuration.

Instead of using the `/.rhosts` file to enforce security in communication among all nodes within a cluster, MC/ServiceGuard allows you to specify an alternate file, `/etc/cmcluster/cmclnodelist`, for validating inter-node access within the cluster. MC/ServiceGuard will check for the existence of the `/etc/cmcluster/cmclnodelist` file first. If the `/etc/cmcluster/cmclnodelist` file exists, MC/ServiceGuard will only use this file to verify access within the cluster; otherwise, the `/.rhosts` file will be used.

The format for entries in the /etc/cmcluster/cmclnodelist file is as follows:

```
[hostname]      [rootuser]      [#comment]
```

The following is an example:

```
node1                   root
node2.sys.dom.com       root
```

where *node1* and *node2* are the names of the cluster nodes. The `/.rhosts` or `/etc/cmcluster/cmclnodelist` file should be copied to all cluster nodes. MC/ServiceGuard supports full domain names in both the `/etc/cmcluster/cmclnodelist` and `/.rhosts` files.

You can also use the `/etc/hosts.equiv` and `/var/adm/inetd.sec` files to provide other levels of cluster security. For more information, refer to the HP-UX guide, *Managing Systems and Workgroups*.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1355
3702
Doc:

Ensuring Consistency of Kernel Configuration

Make sure that the kernel configurations of all cluster nodes are consistent with the expected behavior of the cluster during failover. In particular, if you change any kernel parameters on one cluster node, they may also need to be changed on other cluster nodes that can run the same packages.

Enabling the Network Time Protocol

It is strongly recommended that you enable network time protocol (NTP) services on each node in the cluster. The use of NTP, which runs as a daemon process on each system, ensures that the system time on all nodes is consistent, resulting in consistent timestamps in log files and consistent behavior of message services. This ensures that applications running in the cluster are correctly synchronized. The NTP services daemon, *xntpd*, should be running on all nodes before you begin cluster configuration. The NTP configuration file is `/etc/ntp.conf`.

For information about configuring NTP services, refer to the chapter "Configuring NTP," in the HP-UX manual, *Installation and Administration of Internet Services*.

Preparing for Changes in Cluster Size

If you intend to add additional nodes to the cluster online, while it is running, ensure that they are connected to the same heartbeat subnets and to the same lock disks as the other cluster nodes. In selecting a cluster lock configuration, be careful to anticipate any potential need for additional cluster nodes. Remember that a cluster of more than four nodes *may not use* a cluster lock, but a two-node cluster *must* use a cluster lock. Thus, if you will eventually need five nodes, you should build an initial configuration with at least three to avoid the use of a cluster lock.

If you intend to remove a node from the cluster configuration while the cluster is running, ensure that the resulting cluster configuration will still conform to the rules for cluster locks described above.

To facilitate moving nodes in and out of the cluster configuration, you can use SCSI cables with inline terminators, which allow a node to be removed from the bus without breaking SCSI termination. See the

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1356
Doc: 3702

section "Online Hardware Maintenance with In-line SCSI Terminator" in the "Troubleshooting" chapter for more information on inline SCSI terminators.

If you are planning to add a node online, and a package will run on the new node, ensure that any existing cluster bound volume groups for the package have been imported to the new node.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1357
Doc: 3702

Installing MC/ServiceGuard

Installing MC/ServiceGuard includes updating the software and rebuilding the kernel to support high availability cluster operation for OPS. It is assumed that you have already installed HP-UX 11.0.

Use the following steps *for each node*:

1. Mount the distribution media in the tape drive or CD ROM reader.
2. Run Software Distributor, using the `swinstall` command.
3. Specify the correct input device.
4. Choose the following bundle from the displayed list:

   `B3935BA` `MC/ServiceGuard`
5. After choosing the bundle, select OK. The software is loaded.
6. Run `ioscan` on each node to validate that disks and drivers have been configured correctly.

For details about running `swinstall` and for creating new user accounts, refer to the HP-UX guide, *Managing Systems and Workgroups*.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1358
Doc 3702

Creating the Logical Volume Infrastructure

Before configuring the cluster, you create the appropriate logical volume infrastructure to provide access to data from different nodes. This is done with Logical Volume Manager. Separate procedures are given for the following:

- Mirrored Root
- Mirrored Individual Disks for Data
- Disk Arrays for Data

The Event Monitoring Service HA Disk Monitor provides the capability to monitor the health of LVM disks. If you intend to use this monitor for your mirrored disks, you should configure them in physical volume groups. For more information, refer to the manual *Using EMS HA Monitors* (B5735-90001).

Creating Mirrors of Root Logical Volumes

It is highly recommended that you use mirrored root volumes on all cluster nodes. The following procedure assumes that you are using separate boot and root volumes; you create a mirror of the boot volume (/dev/vg00/lvol1), root volume (/dev/vg00/lvol3), and primary swap (/dev/vg00/lvol2). The procedure cannot be carried out with SAM. In this example and in the following commands, /dev/dsk/c4t5d0 is the primary disk and /dev/dsk/c4t6d0 is the mirror; be sure to use the correct device file names for the root disks on your system.

1. Create a bootable LVM disk to be used for the mirror.

```
# pvcreate -B /dev/rdsk/c4t6d0
```

2. Add this disk to the current root volume group.

```
# vgextend /dev/vg00 /dev/dsk/c4t6d0
```

3. Make the new disk a boot disk.

```
# mkboot /dev/rdsk/c4t6d0
```

4. Copy the correct AUTO file into the new LIF area.

```
# mkboot -a "hpux -l q (;0)/vmunix" /dev/rdsk/c4t6d0
```


RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1359
Nº 3702
Doc:

5. Mirror the boot, root and primary swap logical volumes to the new bootable disk. Ensure that all devices in vg00, such as /usr, /swap, etc., are mirrored.

   The following is an example of mirroring the boot logical volume:

   ```
   # lvextend -m 1 /dev/vg00/lvol1 /dev/dsk/c4t6d0
   ```

   The following is an example of mirroring the root logical volume:

   ```
   # lvextend -m 1 /dev/vg00/lvol3 /dev/dsk/c4t6d0
   ```

   The following is an example of mirroring the primary swap logical volume:

   ```
   # lvextend -m 1 /dev/vg00/lvol2 /dev/dsk/c4t6d0
   ```

NOTE The boot logical volume (/dev/vg00/lvol1 by default) *must* be done first to ensure that it occupies the first contiguous set of extents on the new disk.

6. Update the boot information contained in the BDRA for the mirror copies of boot, root and primary swap.

   ```
   # /usr/sbin/lvlnboot -b /dev/vg00/lvol1
   # /usr/sbin/lvlnboot -v -r /dev/vg00/lvol3
   # /usr/sbin/lvlnboot -s /dev/vg00/lvol2
   ```

7. Check if the BDRA is correct.

   ```
   # /usr/sbin/lvlnboot -R /dev/vg00
   ```

8. Verify that the mirrors were properly created.

   ```
   # lvlnboot -v
   ```

   The output of this command is shown in a display like the following:

```
Boot Definitions for Volume Group /dev/vg00:
Physical Volumes belonging in Root Volume Group:
         /dev/dsk/c4t5d0 (10/0.5.0)   Boot Disk
         /dev/dsk/c4t6d0 (10/0.6.0)   Boot Disk
Boot:   lvol1     on:       /dev/dsk/c4t5d0
                            /dev/dsk/c4t6d0
Root:   lvol3     on:       /dev/dsk/c4t5d0
                            /dev/dsk/c4t6d0
Swap:   lvol2     on:       /dev/dsk/c4t5d0
                            /dev/dsk/c4t6d0
Dump:   lvol2     on:       /dev/dsk/c4t6d0, 0
```


RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1360
Doc: 3702

Creating Volume Groups for Mirrored Individual Data Disks

The procedure described in this section uses **physical volume groups** for mirroring of individual disks to ensure that each logical volume is mirrored to a disk on a different I/O bus. This kind of arrangement is known as **PVG-strict mirroring**. It is assumed that your disk hardware is already configured in such a way that a disk to be used as a mirror copy is connected to each node on a different bus than the bus that is used for the other (primary) copy.

For more information on using LVM, refer to the chapter "Using HP-UX Commands to Manage Mirrors" in the "Logical Volume Manager" chapter of the *System Administration Tasks* manual for HP-UX 10.0 Series 800.

Using SAM to Create Volume Groups and Logical Volumes

You can use SAM to prepare the volume group and logical volume structure needed for HA packages. In SAM, choose the "Disks and File Systems Area." Then use the following procedure for each volume group and file system you are using with the package:

1. Select the Volume Groups subarea.
2. From the Actions menu, choose Create or Extend.
3. Choose the first physical disk you wish to use in the volume group by selecting it from the list of available disks.
4. Enter the volume group name, e.g., `vgdatabase`.
5. Choose Create or Extend Volume Group.
6. Choose Add New Logical Volumes.
7. When adding logical volumes to the volume group, ensure that you are creating mirrored logical volumes with PVG strict allocation.
8. Specify the file system that is to be mounted on the volume group, for example, `/mnt1`.
9. Repeat the procedure for additional volume groups, logical volumes, and file systems.

Skip ahead to the section "Deactivating the Volume Group".

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1361
3702
Doc:

Using LVM Commands to Create Volume Groups and Logical Volumes

If your volume groups have not been set up, use the procedure in the next sections. If you have already done LVM configuration, skip ahead to the section "Configuring the Cluster."

Selecting Disks for the Volume Group. Obtain a list of the disks on both nodes and identify which device files are used for the same disk on both. Use the following command on each node to list available disks as they are known to each system:

```
# lssf /dev/dsk/*
```

In the following examples, we use /dev/rdsk/c1t2d0 and /dev/rdsk/c0t2d0, which happen to be the device names for the same disks on both *ftsys9* and *ftsys10*. In the event that the device file names are different on the different nodes, make a careful note of the correspondences.

Creating Physical Volumes. On the configuration node (ftsys9), use the `pvcreate` command to define disks as physical volumes. This only needs to be done on the configuration node. Use the following commands to create two physical volumes for the sample configuration:

```
# pvcreate -f /dev/rdsk/c1t2d0
# pvcreate -f /dev/rdsk/c0t2d0
```

Creating a Volume Group with PVG-Strict Mirroring. Use the following steps to build a volume group on the configuration node (ftsys9). Later, the same volume group will be created on other nodes.

1. First, set up the group directory for vgdatabase:

   ```
   # mkdir /dev/vgdatabase
   ```

2. Next, create a control file named *group* in the directory /dev/vgdatabase, as follows:

   ```
   # mknod /dev/vgdatabase/group c 64 0xhh0000
   ```

   The major number is always 64, and the hexadecimal minor number has the form

   ```
   0xhh0000
   ```

   where *hh* must be unique to the volume group you are creating. Use the next hexadecimal number that is available on your system, after the volume groups that are already configured. Use the following command to display a list of existing volume groups:

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1362
3702
Doc:

```
# ls -l /dev/*/group
```

3. Create the volume group and add physical volumes to it with the following commands:

```
# vgcreate -g bus1 /dev/vgdatabase /dev/dsk/c1t2d0
# vgextend -g bus2 /dev/vgdatabase /dev/dsk/c0t2d0
```

   The first command creates the volume group and adds a physical volume to it in a physical volume group called *bus1*. The second command adds the second drive to the volume group, locating it in a different physical volume group named *bus2*. The use of physical volume groups allows the use of PVG-strict mirroring of disks and PV links.

4. Repeat this procedure for additional volume groups.

Creating Logical Volumes

Use the following command to create logical volumes (the example is for /dev/vgdatabase):

```
# lvcreate  -L 120 -m 1 -s g /dev/vgdatabase
```

This command creates a 120 MB mirrored volume named *lvol1*. The name is supplied by default, since no name is specified in the command. The *-s g* option means that mirroring is PVG-strict, that is, the mirror copies of data will be in different physical volume groups.

NOTE If you are using disk arrays in RAID 1 or RAID 5 mode, omit the `-m 1` and `-s g` options.

Creating File Systems

If your installation uses file systems, create them next. Use the following commands to create a file system for mounting on the logical volume just created:

1. Create the file system on the newly created logical volume:

```
# newfs -F vxfs /dev/vgdatabase/rlvol1
```

   Note the use of the raw device file for the logical volume.

2. Create a directory to mount the disk:

```
# mkdir /mnt1
```

3. Mount the disk to verify your work:

```
# mount /dev/vgdatabase/lvol1 /mnt1
```


RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1363
Doc: 3702

Note the `mount` command uses the block device file for the logical volume.

4. Verify the configuration:

```
# vgdisplay -v /dev/vgdatabase
```

Creating Volume Groups on Disk Arrays Using PV Links

If you are configuring volume groups that use mass storage on HP's HA disk arrays, you should use redundant I/O channels from each node, connecting them to separate ports on the array. Then you can define alternate links (also called PV links) to the LUNs or logical disks you have defined on the array. In SAM, choose the type of disk array you wish to configure, and follow the menus to define alternate links.

The following example shows how to configure alternate links using LVM commands. In the example, the following disk configuration is assumed:

```
8/0.15.0 /dev/dsk/c0t15d0  /* I/O Channel 0 (8/0) SCSI address 15 LUN 0 */
8/0.15.1 /dev/dsk/c0t15d1  /* I/O Channel 0 (8/0) SCSI address 15 LUN 1 */
8/0.15.2 /dev/dsk/c0t15d2  /* I/O Channel 0 (8/0) SCSI address 15 LUN 2 */
8/0.15.3 /dev/dsk/c0t15d3  /* I/O Channel 0 (8/0) SCSI address 15 LUN 3 */
8/0.15.4 /dev/dsk/c0t15d4  /* I/O Channel 0 (8/0) SCSI address 15 LUN 4 */
8/0.15.5 /dev/dsk/c0t15d5  /* I/O Channel 0 (8/0) SCSI address 15 LUN 5 */

10/0.3.0 /dev/dsk/c1t3d0   /* I/O Channel 1 (10/0) SCSI address 3 LUN 0 */
10/0.3.1 /dev/dsk/c1t3d1   /* I/O Channel 1 (10/0) SCSI address 3 LUN 1 */
10/0.3.2 /dev/dsk/c1t3d2   /* I/O Channel 1 (10/0) SCSI address 3 LUN 2 */
10/0.3.3 /dev/dsk/c1t3d3   /* I/O Channel 1 (10/0) SCSI address 3 LUN 3 */
10/0.3.4 /dev/dsk/c1t3d4   /* I/O Channel 1 (10/0) SCSI address 3 LUN 4 */
10/0.3.5 /dev/dsk/c1t3d5   /* I/O Channel 1 (10/0) SCSI address 3 LUN 5 */
```

Assume that the disk array has been configured, and that both the following device files appear for the same LUN (logical disk) when you run the `ioscan` command:

```
/dev/dsk/c0t15d0
/dev/dsk/c1t3d0
```

Use the following steps to configure a volume group for this logical disk:

1. First, set up the group directory for vgdatabase:

```
# mkdir /dev/vgdatabase
```

2. Next, create a control file named *group* in the directory /dev/vgdatabase, as follows:

```
# mknod /dev/vgdatabase/group c 64 0xhh0000
```


RCS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1364
3702
Doc:

The major number is always 64, and the hexadecimal minor number has the form

```
0xhh0000
```

where *hh* must be unique to the volume group you are creating. Use the next hexadecimal number that is available on your system, after the volume groups that are already configured. Use the following command to display a list of existing group files:

```
# ls -l /dev/*/group
```

3. Use the `pvcreate` command on one of the device files associated with the LUN to define the LUN to LVM as a physical volume.

   ```
   # pvcreate /dev/dsk/c0t15d0
   ```

   It is only necessary to do this with *one* of the device file names for the LUN.

4. Use the following commands to create the volume group itself:

   ```
   #  vgcreate /dev/vgdatabase /dev/dsk/c0t15d0
   # vgextend /dev/vgdatabase /dev/dsk/c1t3d0
   ```

You can now use the `vgdisplay -v` command to see the primary and alternate links. LVM will now recognize the I/O channel represented by /dev/dsk/c0t15d0 as the primary link to the disk; if the primary link fails, LVM will automatically switch to the alternate I/O channel represented by /dev/dsk/c1t3d0.

To create logical volumes, use the procedure described in the previous section, "Creating Logical Volumes."

Deactivating the Volume Group

At the time you create the volume group, it is active on the configuration node (*ftsys9*, for example). Before setting up the volume group for use on other nodes, you must first unmount any file systems that reside on the volume group, then deactivate it. At run time, volume group activation and file system mounting are done through the package control script.

Continuing with the example presented in earlier sections, do the following on *ftsys9*:

```
# umount /mnt1
# vgchange -a n /dev/vgdatabase
```


RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1365
Doc: 3702

17.509

Distributing the Volume Group to Other Nodes

After creating volume groups for cluster data, you must make them available to any cluster node that will need to activate the volume group.

Distributing the Volume Group to Other Cluster Nodes with SAM

In SAM, choose the Disks and File Systems area, then choose Volume Groups. Select the volume group that is to be distributed to one or more additional nodes. Enter the name of each node that is to receive the volume group and select "Add." When the list is complete, press OK. SAM automatically configures the volume group for use on the other nodes.

After distributing the volume groups, check the /etc/lvmpvg files on each node to ensure that each physical volume group contains the correct physical volume names for that node.

Distributing the Volume Group to Other Cluster Nodes with LVM Commands

Use the following commands to set up the same volume group on another cluster node. In this example, the commands set up a new volume group on *ftsys10* which will hold the same physical volume that was available on *ftsys9*. You must carry out the same procedure separately for each node on which the volume group's package can run.

To set up the volume group on ftsys10, use the following steps:

1. On *ftsys9*, copy the mapping of the volume group group to a specified file.

   ```
   # vgexport -p -s -m /tmp/vgdatabase.map  /dev/vgdatabase
   ```

2. Still on *ftsys9*, copy the map file to *ftsys10*:

   ```
   # rcp /tmp/vgdatabase.map ftsys10:/tmp/vgdatabase.map
   ```

3. On *ftsys10*, create the volume group directory:

   ```
   # mkdir /dev/vgdatabase
   ```

4. Still on ftsys10, create a control file named *group* in the directory /dev/vgdatabase, as follows:

   ```
   # mknod /dev/vgdatabase/group c 64 0xhh0000
   ```


RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1366
Doc: 3102

The major number is always 64, and the hexadecimal minor number has the form

```
0xhh0000
```

where *hh* must be unique to the volume group you are creating. If possible, use the same number as on *ftsys9*. Use the following command to display a list of existing volume groups:

```
# ls -l /dev/*/group
```

5. Import the volume group data using the map file from node ftsys9. On node fsys10, enter:

   ```
   # vgimport -s -m /tmp/vgdatabase.map /dev/vgdatabase
   ```

   Note that the disk device names on ftsys10 may be different from their names on ftsys9. You should check to ensure that the physical volume names are correct throughout the cluster.

6. If you are using mirrored individual disks in physical volume groups, check the /etc/lvmpvg file to ensure that each physical volume group contains the correct physical volume names for *ftsys10*.

NOTE

When you use PVG-strict mirroring, the physical volume group configuration is recorded in the /etc/lvmpvg file on the configuration node. This file defines the physical volume groups which are the basis of mirroring and indicate which physical volumes belong to each PVG. Note that on each cluster node, the /etc/lvmpvg file must contain the correct physical volume names for the PVG's disks *as they are known on that node*. Physical volume names for the same disks may not be the same on different nodes. After distributing volume groups to other nodes, you must ensure that each node's /etc/lvmpvg file correctly reflects the contents of all physical volume groups on that node. Refer to the following section, "Making Physical Volume Group Files Consistent."

7. Enable the volume group on *ftsys10*:

   ```
   # vgchange -a y /dev/vgdatabase
   ```

8. Create a directory to mount the disk:

   ```
   # mkdir /mnt1
   ```

9. Mount and verify the volume group on ftsys10:

   ```
   # mount /dev/vgdatabase/lvol1 /mnt1
   ```

10. Unmount the volume group on *ftsys10*:

    ```
    # umount /mnt1
    ```


ROS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1367
3702
Doc:

11. Deactivate the volume group on *ftsys10*:

```
# vgchange -a n /dev/vgdatabase
```

Making Physical Volume Group Files Consistent

Skip ahead to the next section if you do not use physical volume groups for mirrored individual disks in your disk configuration.

Different volume groups may be activated by different subsets of nodes within an MC/ServiceGuard cluster. In addition, the physical volume name for any given disk may be different on one node than it is on another. For these reasons, you must carefully merge the /etc/lvmpvg files on all nodes so that each node has a complete and consistent view of all cluster-aware disks as well as of its own private (non-cluster-aware) disks. To make merging the files easier, be sure to keep a careful record of the physical volume group names on the volume group planning worksheet (described in the "Planning" chapter).

Use the following procedure to merge files between the configuration node (*ftsys9*) and a new node (*ftsys10*) to which you are importing volume groups:

1. Copy `/etc/lvmpvg` from *ftsys9* to `/etc/lvmpvg.new` on *ftsys10*.
2. If there are volume groups in `/etc/lvmpvg.new` that do not exist on *ftsys10*, remove all entries for that volume group from `/etc/lvmpvg.new`.
3. If `/etc/lvmpvg` on *ftsys10* contains entries for volume groups that do not appear in `/etc/lvmpvg.new`, then copy all PVG entries for that volume group to `/etc/lvmpvg.new`.
4. Adjust any physical volume names in `/etc/lvmpvg.new` to reflect their correct names on *ftsys10*.
5. On *ftsys10*, copy `/etc/lvmpvg` to `/etc/lvmpvg.old` to create a backup. Copy `/etc/lvmvpg.new` to `/etc/lvmpvg` on *ftsys10*.

Creating Additional Volume Groups

The foregoing sections show in general how to create volume groups and logical volumes for use with MC/ServiceGuard. Repeat the procedure for as many volume groups as you need to create, substituting other volume group names, logical volume names, and physical volume names. Pay close attention to the disk device names. For example, */dev/dsk/c0t2d0* on one node may not be */dev/dsk/c0t2d0* on another node.

RCS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1368
Nº 3702

Configuring the Cluster

This section describes how to define the basic cluster configuration. To do this in SAM, read the next section. If you want to use MC/ServiceGuard commands, skip ahead to the section entitled "Using MC/ServiceGuard Commands to Configure the Cluster."

Using SAM to Configure the Cluster

To configure a high availability cluster, use the following steps on the configuration node (ftsys9):

1. In SAM, select Clusters, then the High Availability Clusters option.
2. Choose the Cluster Configuration option. SAM displays a Cluster Configuration screen. If no clusters have yet been configured, the list area will be empty. If there are one or more HA clusters already configured on your local network, you will see them listed.
3. Select the Actions menu, and choose Create Cluster Configuration. A step menu appears.
4. Choose each required step in sequence, filling in the dialog boxes with required information, or accepting the default values shown. For information about each step, choose Help.
5. When finished with all steps, select **OK** at the Step Menu screen. This action creates the cluster configuration file and then copies the file to all the nodes in the cluster. When the file copying is finished, you return to the Cluster Configuration screen.
6. Exit from the Cluster Configuration screen, returning to the High Availability Clusters menu.

NOTE In addition to creating and distributing a binary cluster configuration file, SAM creates an ASCII cluster configuration file, named /etc/cmcluster/cmclconfig.ascii. This file is available as a record of the choices entered in SAM.

Skip ahead to the section "Setting up Autostart Features."

RQS nº 03/2005 - CN - CPMI - CORREIOS
1369
Fls Nº
3702
Doc:

17-505

Using MC/ServiceGuard Commands to Configure the Cluster

Use the *cmquerycl* command to specify a set of nodes to be and to generate a template for the cluster configuration file. Here is an example of the command as issued from node ftsys9:

```
# cmquerycl -v -C /etc/cmcluster/cmclconf.ascii -n ftsys9 -n
ftsys10
```

The example creates an ASCII template file in the default cluster configuration directory, /etc/cmcluster. The ASCII file is partially filled in with the names and characteristics of cluster components on the two nodes *ftsys9* and *ftsys10*. Edit the filled-in cluster characteristics as needed to define the desired cluster. It is strongly recommended that you edit the file to send heartbeat over all possible networks, as shown in the following example.

Cluster Configuration Template File

```
# **********************************************************************
# ********* HIGH AVAILABILITY CLUSTER CONFIGURATION FILE ***************
# ***** For complete details about cluster parameters and how to     ****
# ***** set them, consult the cmquerycl(1m) manpage or your manual. ****
# **********************************************************************

# Enter a name for this cluster.  This name will be used to identify the
# cluster when viewing or manipulating it.

CLUSTER_NAME            cluster1


# Cluster Lock Device Parameters.  This is the volume group that
# holds the cluster lock which is used to break a cluster formation
# tie.  This volume group should not be used by any other cluster
# as cluster lock device.

FIRST_CLUSTER_LOCK_VG   /dev/vg01


# Definition of nodes in the cluster.
# Repeat node definitions as necessary for additional nodes.

NODE_NAME               ftsys9
  NETWORK_INTERFACE     lan0
    HEARTBEAT_IP        15.13.171.32
  NETWORK_INTERFACE     lan3
    HEARTBEAT_IP        192.6.7.3
  NETWORK_INTERFACE     lan4
  NETWORK_INTERFACE     lan1
    HEARTBEAT_IP        192.6.143.10
  FIRST_CLUSTER_LOCK_PV /dev/dsk/c1t2d0


# List of serial device file names
# For example:
# SERIAL_DEVICE_FILE    /dev/tty0p0


# Primary Network Interfaces on Bridged Net 1: lan0.
#    Warning: There are no standby network interfaces on bridged net 1.
```


Nº 03/2005 - CN -
CPMI - CORREIOS
1370
Fls Nº
3702
Doc:

17504


```
# Primary Network Interfaces on Bridged Net 2: lan3.
#   Possible standby Network Interfaces on Bridged Net 2: lan4.
# Primary Network Interfaces on Bridged Net 3: lan1.
#   Warning: There are no standby network interfaces on bridged net 3.

NODE_NAME               ftsys10
  NETWORK_INTERFACE     lan0
    HEARTBEAT_IP        15.13.171.30
  NETWORK_INTERFACE     lan3
    HEARTBEAT_IP        192.6.7.4
  NETWORK_INTERFACE     lan4
  NETWORK_INTERFACE lan1
    HEARTBEAT_IP        192.6.143.20
  FIRST_CLUSTER_LOCK_PV /dev/dsk/c1t2d0


# List of serial device file names
# For example:
# SERIAL_DEVICE_FILE    /dev/tty0p0


# Primary Network Interfaces on Bridged Net 1: lan0.
#   Warning: There are no standby network interfaces on bridged net 1.
# Primary Network Interfaces on Bridged Net 2: lan3.
#   Possible standby Network Interfaces on Bridged Net 2: lan4.
# Primary Network Interfaces on Bridged Net 3: lan1.
#   Warning: There are no standby network interfaces on bridged net 3.


# Cluster Timing Parameters (microseconds).

HEARTBEAT_INTERVAL      1000000
NODE_TIMEOUT            2000000


# Configuration/Reconfiguration Timing Parameters (microseconds).

AUTO_START_TIMEOUT      600000000
NETWORK_POLLING_INTERVAL 2000000

# Package Configuration Parameters.
# Enter the maximum number of packages which will be configured in the cluster.
# You can not add packages beyond this limit.
# This parameter is required.
MAX_CONFIGURED_PACKAGES          10


#
# List of cluster aware Volume Groups. These volume groups
# will be used by clustered applications via the vgchange -a e command.
# For example:
# VOLUME_GROUP          /dev/vgdatabase
# VOLUME_GROUP          /dev/vg02
VOLUME_GROUP            /dev/vg01
VOLUME_GROUP            /dev/vg02
```

The man page for the `cmquerycl` command lists the definitions of all the parameters that appear in this file. Many are also described in the "Planning" chapter. Modify your */etc/cmcluster/cmclconf.ascii* file to your requirements, using the data on the cluster configuration worksheet.

In the file, keywords are separated from definitions by white space. Comments are permitted, and must be preceded by a pound sign (#) in the far left column. See the man page for the `cmquerycl` command for more details.

ROS nº 03/2003 - CN - CPMI - CORREIOS
Fls Nº 1371
Nº 3702 Doc.

Identifying Cluster Volume Groups

The file will include an entry for all volume groups that are to be defined as cluster-aware, that is, those which can be accessed by different nodes in the cluster at different times. A separate VOLUME_GROUP line should appear for each volume group that will be activated by any package running in the cluster. To leave a volume group unmarked, remove the volume group name from the ASCII file.

NOTE If a volume group is not cluster-aware, then it cannot be activated by a package control script.

Redeploying Previously Configured Volume Groups

In configuring a new cluster, if you are using volume groups that were used in a previous cluster configuration, you should ensure that they are not currently cluster aware (marked with a cluster id). You can use the following command to remove the cluster id if necessary:

```
# vgchange -c n
```

Identifying the Cluster Lock Volume Group and Disk

A cluster lock disk is required for two node clusters like the one in this example. The disk must be accessible to all nodes and must be powered separately from the nodes. Refer to the section "Use of the Cluster Lock" in Chapter 3 for additional information.

The default FIRST_CLUSTER_LOCK_VG and FIRST_CLUSTER_LOCK_PV supplied in the ASCII template created with cmquerycl are the volume group and physical volume name of a disk chosen based on minimum failover time calculations. You should ensure that this disk meets your power wiring requirements. If necessary, choose a disk powered by a circuit which powers *fewer* than half the nodes in the cluster.

If necessary, you can configure a second cluster lock. Enter the following parameters in the cluster configuration file:

```
SECOND_CLUSTER_LOCK_VG /dev/volume-group
SECOND_CLUSTER_LOCK_PV /dev/dsk/block-special-file
```

where the */dev/volume-group* is the name of the second volume group and *block-special-file* is the physical volume name of a lock disk in the chosen volume group. These lines should be added to the information for each node.

RQS nº 03/2005 - CN - CPMI - CORREIOS
1372
Fls Nº
3702
Doc:

17.502

To display the failover times of disks, use the `cmquerycl` command, specifying all the nodes in the cluster:

```
# cmquerycl -v -n ftsys9 -n ftsys10
```

The output of the command lists the disks connected to each node together with the re-formation time associated with each.

Specifying Maximum Number of Configured Packages

MC/ServiceGuard preallocates memory and threads at cluster startup time. It calculates these values based on the number of packages specified in the `MAX_CONFIGURED_PACKAGES` parameter in the cluster configuration file. This value must be equal to or greater than the number of packages currently configured in the cluster. The default is 0, which means that you must enter a value if you wish to use packages. The absolute maximum number of packages per cluster is 30.

Identifying Serial Heartbeat Connections

If you are using a serial (RS232) line as a heartbeat connection, use the `SERIAL_DEVICE_FILE` parameter and enter the device file name that corresponds to the serial port you are using on each node. Be sure that the serial cable is securely attached during and after configuration.

Adding or Removing Nodes While the Cluster is Running

You can reconfigure the cluster by adding or removing nodes while the cluster is up and running. The procedures are described in the chapter on "Cluster and Package Maintenance."

RQS nº 03/2005 - CN - CPMI - CORREIOS
1373
Fls Nº
3702
Doc:

Verifying the Cluster Configuration

SAM automatically checks the configuration you enter and reports any errors. If you have edited an ASCII cluster configuration file, use the following command to verify the content of the file:

```
# cmcheckconf -v -C /etc/cmcluster/cmclconf.ascii
```

This command or automatic verification in SAM both check the following:

- Network addresses and connections.
- Cluster lock connectivity.
- Validity of configuration parameters for the cluster and packages.
- Uniqueness of names.
- Existence and permission of scripts specified in the command line.
- If all nodes specified are in the same heartbeat subnet.
- If you specify the wrong configuration filename.
- If all nodes can be accessed.
- No more than one `CLUSTER_NAME`, `HEARTBEAT_INTERVAL`, and `AUTO_START_TIMEOUT` are specified.
- The value for `HEARTBEAT_INTERVAL` is at least one second.
- The value for `NODE_TIMEOUT` is at least twice the value of `HEARTBEAT_INTERVAL`.
- The value for `AUTO_START_TIMEOUT` variables is >=0.
- Heartbeat network minimum requirement. The cluster must have one heartbeat LAN configured with a standby, or two heartbeat LANs, or one heartbeat LAN and an RS232 connection.
- At least one `NODE_NAME` is specified.
- Each node is connected to each heartbeat network.
- All heartbeat networks are of the same type of LAN.
- The network interface device files specified are valid LAN device files.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1374
3702
Doc:

- RS-232 is configured on a two node cluster, and there is no more than one serial (RS232) port connection per node.
- VOLUME_GROUP entries are not currently marked as cluster-aware.

If the cluster is online, SAM (or the `cmcheckconf` command) also verifies that all the conditions for the specific change in configuration have been met.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1375
Doc. 3702

17.499

Distributing the Binary Configuration File

After specifying all cluster parameters, you use SAM or HP-UX commands to apply the configuration. This action distributes the binary configuration file to all the nodes in the cluster. We recommend doing this separately *before* you configure packages (described in the next chapter). In this way, you can verify the cluster lock, heartbeat networks, and other cluster-level operations by using the `cmviewcl` command on the running cluster. Before distributing the configuration, ensure that your security files permit copying among the cluster nodes. See "Preparing Your Systems" at the beginning of this chapter.

Distributing the Configuration File with SAM

When you have finished entering parameters in the Cluster Configuration subarea in SAM, you are asked to verify the copying of the files to all the nodes in the cluster. When you respond OK to the verification prompt, MC/ServiceGuard copies the binary configuration file and the ASCII configuration file to all the nodes in the cluster.

Distributing the Configuration File with HP-UX Commands

Use the following steps to generate the binary configuration file and distribute the configuration to all nodes in the cluster:

- Activate the cluster lock volume group so that the lock disk can be initialized:

```
# vgchange -a y /dev/vglock
```

- Generate the binary configuration file and distribute it across the nodes.

```
# cmapplyconf -v -C /etc/cmcluster/cmclconf.ascii -P \
  /etc/cmcluster/pkg1/pkglconf.ascii
```

- Deactivate the cluster lock volume group.

```
# vgchange -a n /dev/vglock
```


RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1376
Dos: 3702

The `cmapplyconf` command creates a binary version of the cluster configuration file and distributes it to all nodes in the cluster. This action ensures that the contents of the file are consistent across all nodes. Note that the **`cmapplyconf`** command does not distribute the ASCII configuration file.

CAUTION

The cluster lock volume group must be activated *only* on the node from which you issue the `cmapplyconf` command, so that the lock disk can be initialized. If you attempt to configure a cluster either using SAM or by issuing the `cmapplyconf` command on one node while the lock volume group is active on another, different node, the cluster lock will be left in an unknown state. Therefore, you must ensure that when you configure the cluster, the cluster lock volume group is active only on the configuration node and deactivated on all other nodes.

Be sure to deactivate the cluster lock volume group on the configuration node after `cmapplyconf` is executed.

Storing Volume Group and Cluster Lock Configuration Data

After configuring the cluster, create a backup copy of the volume group configuration by using the `vgcfgbackup` command for each volume group you have created. If a disk in a volume group must be replaced, you can then restore the disk's metadata by using the `vgcfgrestore` command. The procedure is described under "Replacing Disks" in the "Troubleshooting" chapter.

Be sure to use `vgcfgbackup` for all volume groups, including the cluster lock volume group.

NOTE

You *must* use the `vgcfgbackup` command to store a copy of the cluster lock disk's configuration data whether you created the volume group using SAM or using HP-UX commands.

The lock disk is normally configured with redundant copies either through mirroring or RAID. If the cluster lock disk ever needs to be replaced while the cluster is running, you *must* use the `vgcfgrestore` command to restore lock information to the replacement disk. Failure to do this might result in a failure of the entire cluster if all redundant copies of the lock disk have failed and if replacement mechanisms or LUNs have not had the lock configuration restored.

RQS nº 03/2005 - CN
CPMI - CORREIOS
1377
Fls Nº
3702
Doc:

17.497

Checking Cluster Operation

MC/ServiceGuard also provides several commands for manual control of the cluster:

- `cmrunnode` is used to start a node.
- `cmhaltnode` is used to manually stop a running node. (This command is also used by `shutdown(1m)`.)
- `cmruncl` is used to manually start a stopped cluster.
- `cmhaltcl` is used to manually stop a cluster.

You can use these commands to test cluster operation, as in the following:

1. If the cluster is not already online, run the cluster, as follows:

   ```
   # cmruncl -f -v
   ```

2. When the cluster has started, use the following command to ensure that cluster components are operating correctly:

   ```
   # cmviewcl -v
   ```

   Make sure that all nodes and networks are functioning as expected. For information about using `cmviewcl`, refer to the chapter on "Cluster and Package Maintenance."

3. Use the following sequence of commands to verify that nodes leave and enter the cluster as expected:

   - On a cluster node, issue the `cmhaltnode` command.
   - Use the `cmviewcl` command to verify that the node has left the cluster..
   - Issue the `cmrunnode` command.
   - Use the `cmviewcl` command again to verify that the node has returned to operation.

4. Use the following command to bring down the cluster:

   ```
   # cmhaltcl -v -f
   ```

Additional cluster testing is described in the "Troubleshooting" chapter. Refer to Appendix A for a complete list of MC/ServiceGuard commands

RQS nº 03/2005 - CN -
CPMI - CORREIOS
1378
Fls Nº
3702
Doc:

Preventing Automatic Activation of Volume Groups

It is important to prvent package volume groups from being activated at system boot time by the /etc/lvmrc file. To ensure that this does not happen, edit the /etc/lvmrc file on all nodes. Set `AUTO_VG_ACTIVATE` to 0, then include all the volume groups that are not cluster bound in the `custom_vg_activation` function. Volume groups that will be used by packages should *not* be included anywhere in the file, since they will be activated and deactivated by control scripts.

NOTE The root volume group does not need to be included in the `custom_vg_activation` function, since it is automatically activated before the /etc/lvmrc file is used at boot time.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1379
3702

Setting up Autostart Features

Automatic startup is the process in which each node individually joins a cluster. If a cluster already exists, the node attempts to join it; if no cluster is running, the node attempts to form a cluster consisting of all configured nodes. Automatic cluster start is the preferred way to start a cluster. No action is required by the system administrator. To enable automatic cluster start, set the flag `AUTOSTART_CMCLD` to 1 in the `/etc/rc.config.d/cmcluster` file; the node will then join the cluster at boot time.

In order to automate the startup of cluster nodes after a system boot, you must modify the */etc/rc.config.d/cmcluster* file on each node. MC/ServiceGuard provides this startup script to control the startup process:

```
#*************************** CMCLUSTER ************************
# Highly Available Cluster configuration
#
# @(#) $Revision: 72.2 $
#
# AUTOSTART_CMCLD:      If set to 1, the node will attempt to
#                       join it's CM cluster automatically when
#                       the system boots.
#                       If set to 0, the node will not attempt
#                       to join it's CM cluster.
#
AUTOSTART_CMCLD=1
```


RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1380
3702
Doc:

Changing the System Message

You may find it useful to modify the system's login message to include a statement such as the following:

```
This system is a node in a high availability cluster.
Halting this system may cause applications and services to
start up on another node in the cluster.
```

You might wish to include a list of all cluster nodes in this message, together with additional cluster-specific information.

The /etc/issue and /etc/motd files may be customized to include cluster-related information.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1381
Doc: 3702

17.493

Deleting the Cluster Configuration

You can delete a cluster configuration from all cluster nodes by using SAM or by issuing the `cmdeleteconf` command. The command prompts for a verification before deleting the files unless you use the `-f` option. You can only delete the configuration when the cluster is down. The action removes the binary configuration file from all the nodes in the cluster and resets all cluster-aware volume groups to be no longer cluster-aware.

NOTE

Although the cluster must be halted, all nodes in the cluster should be powered up and accessible before you use the `cmdeleteconf` command. If a node is powered down, power it up and boot. If a node is inaccessible, you will see a list of inaccessible nodes together with the following message:

```
It is recommended that you do not proceed with the configuration
operation unless you are sure these nodes are permanently
unavailable.Do you want to continue?
```

Reply Yes to remove the configuration. Later, if the inaccessible node becomes available, you should run the `cmdeleteconf` command on that node to remove the configuration file.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
1382
Fls Nº
Doc: 3702

IBM TotalStorage™ Enterprise Storage Server™

Interoperability Matrix

June 27, 2003

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1383
3702
Doc:

Fibre Channel

Servers

Pentium Pro or later 32 bit processors
- 200 MHz processor or faster
- 128 MB memory or greater
- Excludes IBM Netfinity 3000 and IBM PC Server 325

IBM eServer BladeCenter [7]
- BladeCenter HS20

Operating Systems

Microsoft Windows NT
- Server 4.0
- Server 4.0, Enterprise Edition including Microsoft Cluster Server (MSCS)

Microsoft Windows 2000
- Server
- Advanced Server including Cluster service
- Datacenter Server

Microsoft Windows Server 2003 [6]
- Standard Edition
- Enterprise Edition including cluster service
- Datacenter Edition including cluster server

Host Adapters

Emulex
- LP7000E
- LP8000
- LP9002L / LP9002DC [2]
- LP9402DC [2]
- LP9802 [2]

IBM BladeCenter
- P/N 48P7062

IBM Netfinity/xSeries
- P/N 01K7297
- P/N 00N6881
- P/N 19K1246
- P/N 24P0960

QLogic
- QLA2100F
- QLA2200F
- QLA2310F / QLA2310FL [2]
- QLA2340/L / QLA2342/L [2]

Fabric Support

Cisco [2]
- MDS 9216
- MDS 9509

IBM
- 2103 Model H07 [3]
- 2109 Models F16 and F32 [2]
- 2109 Model M12 [2]
- 2109 Models S08 and S16
- 3534 Model F08 [2]
- 3534 Model 1RU [3]

INRANGE
- FC/9000-64 [4]
- FC/9000-128 [4]
- FC/9000- 256 [5]

McDATA
- ED-5000
- ES-3016 and ES-3032
- Intrepid
  - 6064 [2]
  - 6140 [2]
- Sphereon
  - 3216 [2]
  - 3232 [2]
  - 4500 [2]

[2] Requires ESS LIC level 1.5.2, or later.

[3] Supported for distance solutions only. Multiple initiators or targets on the same loop are not supported.

[4] Requires ESS LIC level 1.3.2.50, or later.

[5] Requires ESS LIC level 2.1.0, or later, for the ESS Model 800, and ESS LIC level 1.5.2, or later, for the ESS Models F10 and F20.

[6] Requires ESS LIC level 2.2.0, or later. Windows 2003 is not supported on the Emulex LP7000E, QLogic QLA2100F, and IBM P/N 01K7297 host adapters, and the Cisco fabric switches.

[7] Requires ESS LIC level 2.1.1, or later, and is supported on only Windows 2000 (non-clustered configurations). The following fabric products are supported: IBM 2109 Model F16, IBM 3534 Model F08, INRANGE, and McDATA (excluding ED-5000).

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1384
Nº 3702
Doc:

General Notes:

- Fibre channel support:
  - Requires ESS LIC level 1.2.0, or later.
- ESS API – CIM Agent:
  - Available for all levels of Windows 2000.
  - Requires ESS LIC level 2.1.1, or later.
  - Not available for the ESS Models E10 and E20.
- ESS CLI:
  - Available for all levels of Windows 2000, and Windows Server 2003.
  - Requires ESS LIC level 2.1.0, or later.
  - Not available for the ESS Models E10 and E20.
- CS CLI:
  - Available for all levels of Windows NT, Windows 2000, and Windows Server 2003.
- SDD:
  - Available for all levels of Windows NT and Windows 2000 and Windows 2003 (see additional notes on following page).
  - Load balancing is not available in Windows NT or Windows 2000 cluster configurations.
- Boot device support:
  - The ESS is supported as a boot device on Windows 2000 servers that support Fibre Channel boot capability. This support requires ESS LIC level 2.2.0, or later, with host adapters QLA2310F / QLA2310FL, and QLA2340 / QLA2342L. Requires SDD level 1.4.0.0. Refer to the *IBM TotalStorage Enterprise Storage Server Host Systems Attachment Guide* for additional information.

- <u>The following items are not interoperable with the ESS Model 800:</u>
  - Host adapters:
    - Emulex LP7000E.
    - IBM 01K7297.
    - QLogic QLA1041 and QLA2100F.
    - Symbios SYM8751D.
  - Fabric products:
    - IBM 2103 Model H07.
    - IBM 3534 Model 1RU.

- <u>The following items are not interoperable with the ESS Models E10 and E20</u>
  - BladeCenter.
  - ESS CLI.
  - Operating systems:
    - Datacenter Server.
  - Host adapters:
    - Emulex LP9002L / LP9002DC.
    - Emulex LP9802 and LP9402DC.
    - QLogic QLA2310F / QLA2310FL and QLA2340 / QLA2342L.
  - ESS API.
  - Fabric products:
    - Cisco MDS 9216 and MDS 9509.
    - IBM 2109 Models F32 and M12.
    - IBM 3534 Model F08.
    - INRANGE FC/9000- 256
    - McDATA Intrepid 6140.
    - McDATA Sphereon 3216, 3232, and 4500.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1385
Nº 3702
Doc:

ANEXO UNIDADE DE BACKUP ROBOTIZADO
PARTE C

17.486 - AC

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

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1386
3702
Dos:

17.485

6 Configuring Packages and Their Services

In addition to configuring the cluster, you must identify your highly available application services, and group them into packages. This chapter describes the following *package configuration* tasks:

- Creating the Package Configuration
- Writing the Package Control Script
- Distributing the Binary Cluster Configuration File

Each of these tasks is described in a separate section below.

In configuring your own packages, use data from the Package Configuration Worksheet described in the "Planning" chapter. Package configuration data from the worksheet becomes part of the binary cluster configuration file on all nodes in the cluster. The control script data from the worksheet goes into an executable package control script which runs specific applications (services) and monitors their operation.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1387
Doc: 3702

17.484

Creating the Package Configuration

The package configuration process defines a set of application services that are run by the package manager when a package starts up on a node in the cluster. The configuration also includes a prioritized list of cluster nodes on which the package can run together with definitions of the acceptable types of failover allowed for the package.

You can create a package using SAM or using HP-UX commands and editors. The following section describes SAM configuration. If you are using MC/ServiceGuard commands, skip ahead to the section entitled "Using MC/ServiceGuard Commands to Create a Package."

Using SAM to Configure a Package

To configure a high availability package use the following steps on the configuration node (ftsys9):

1. In SAM, choose the "Clusters" area, then the High Availability Clusters option.
2. Choose the Package Configuration option. SAM displays a Package Configuration screen. If no packages have yet been configured, the list area will be empty. If there are one or more MC/ServiceGuard packages already configured on clusters in your network, you will see them listed.
3. Select the Actions menu, and choose Create/Add a Package. A step menu appears.
4. Choose each required step in sequence, filling in the dialog boxes with required information, or accepting the default values shown. For information about each step, choose Help.
5. When finished with all steps, select OK at the Step Menu screen. This action creates (or modifies) the package configuration file and then copies the file to all the nodes in the cluster. This action also creates a package control script which is copied to all nodes.
6. When the file copying is finished, you return to the Package Configuration screen.
7. Exit from the Package Configuration screen, returning to the High Availability Clusters menu.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1388
3702
Doc:

17483

Skip ahead to the section on "Writing the Package Control Script."

Using MC/ServiceGuard Commands to Create a Package

Use the following procedure to create packages by editing and processing a package configuration file.

1. First, create a subdirectory for each package you are configuring in the /etc/cmcluster directory:

   ```
   # mkdir /etc/cmcluster/pkg1
   ```

   You can use any directory names you wish.

2. Next, generate a package configuration template for the package:

   ```
   # cmmakepkg -p /etc/cmcluster/pkg1/pkg1conf.ascii
   ```

   You can use any file names you wish for the ASCII templates.

3. Edit these template files to specify package name, prioritized list of nodes, the location of the control script, and failover parameters for each package. Include the data recorded on the Package Configuration Worksheet.

Configuring in Stages

It is recommended to configure packages on the cluster in stages, as follows:

1. Configure volume groups and mount points only.
2. Apply the configuration.
3. Distribute the control script to all nodes.
4. Run the cluster and ensure that packages can be moved from node to node.
5. Halt the cluster.
6. Configure package IP addresses and application services in the control script.
7. Distribute the control script to all nodes.
8. Run the cluster and ensure that applications run as expected and that packages fail over correctly when services are disrupted.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
1389
Fls Nº
3702
Doc:

Package Configuration Template File

The following is a sample package configuration file template customized for a typical package.

```
# **********************************************************************
# ****** HIGH AVAILABILITY PACKAGE CONFIGURATION FILE (template) *******
# **********************************************************************
# ******* Note: This file MUST be edited before it can be used. ********
# * For complete details about package parameters and how to set them, *
# * consult the MC/ServiceGuard or MC/LockManager manpages or manuals. *
# **********************************************************************

# Enter a name for this package.  This name will be used to identify the
# package when viewing or manipulating it.  It must be different from
# the other configured package names.

PACKAGE_NAME  pkg1


# Enter the names of the nodes configured for this package.  Repeat
# this line as necessary for additional adoptive nodes.
# Order IS relevant.  Put the second Adoptive Node AFTER the first
# one.
# Example : NODE_NAME  original_node
#           NODE_NAME  adoptive_node

NODE_NAME ftsys9
NODE_NAME ftsys10


# Enter the complete path for the run and halt scripts.  In most cases
# the run script and halt script specified here will be the same script,
# the package control script generated by the cmmakepkg command.  This
# control script handles the run(ning) and halt(ing) of the package.
# If the script has not completed by the specified timeout value,
# it will be terminated.  The default for each script timeout is
# NO_TIMEOUT.  Adjust the timeouts as necessary to permit full
# execution of each script.
# Note: The HALT_SCRIPT_TIMEOUT should be greater than the sum of
# all SERVICE_HALT_TIMEOUT specified for all services.

RUN_SCRIPT   /etc/cmcluster/pkg1/control.sh
RUN_SCRIPT_TIMEOUT      NO_TIMEOUT
HALT_SCRIPT  /etc/cmcluster/pkg1/control.sh
HALT_SCRIPT_TIMEOUT     NO_TIMEOUT


# Enter the SERVICE_NAME, the SERVICE_FAIL_FAST_ENABLED and the
# SERVICE_HALT_TIMEOUT values for this package.  Repeat these
# three lines as necessary for additional service names.  All
# service names MUST correspond to the service names used by
# cmrunserv and cmhaltserv commands in the run and halt scripts.
#
# The value for SERVICE_FAIL_FAST_ENABLED can be either YES or
# NO.  If set to YES, in the event of a service failure, the
# cluster software will halt the node on which the service is
# running.  If SERVICE_FAIL_FAST_ENABLED is not specified, the
# default will be NO.
#
# SERVICE_HALT_TIMEOUT is represented in the number of seconds.
# This timeout is used to determine the length of time (in
# seconds) the cluster software will wait for the service to
# halt before a SIGKILL signal is sent to force the termination
# of the service.  In the event of a service halt, the cluster
# software will first send a SIGTERM signal to terminate the
# service.  If the service does not halt, after waiting for the
# specified SERVICE_HALT_TIMEOUT, the cluster software will send
# out the SIGKILL signal to the service to force its termination.
# This timeout value should be large enough to allow all cleanup
```


RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1390
3702

17.481


```
# processes associated with the service to complete.  If the
# SERVICE_HALT_TIMEOUT is not specified, a zero timeout will be
# assumed, meaning the cluster software will not wait at all
# before sending the SIGKILL signal to halt the service.
#
# Example: SERVICE_NAME                  DB_SERVICE
#          SERVICE_FAIL_FAST_ENABLED     NO
#          SERVICE_HALT_TIMEOUT          300
#
# To configure a service, uncomment the following lines and
# fill in the values for all of the keywords.
#
SERVICE_NAME                  service1
SERVICE_FAIL_FAST_ENABLED     NO
SERVICE_HALT_TIMEOUT          300


# Enter the network subnet name that is to be monitored for this package.
# Repeat this line as necessary for additional subnet names.  If any of
# the subnets defined goes down, the package will be switched to another
# node that is configured for this package and has all the defined subnets
# available.

#SUBNET   15.16.168.0


# The following keywords (RESOURCE_NAME, RESOURCE_POLLING_INTERVAL, and
# RESOURCE_UP_VALUE) are used to specify Package Resource Dependencies.  To
# define a Package Resource Dependency, a RESOURCE_NAME line with a fully
# qualified resource path name, and one or more RESOURCE_UP_VALUE lines are
# required.  A RESOURCE_POLLING_INTERVAL line (how often in seconds the resource
# is to be monitored) is optional and defaults to 60 seconds.  An operator and
# a value are used with RESOURCE_UP_VALUE to define when the resource is to be
# considered up.  The operators are =, !=, >, <, >=, and <=, depending on the
# type of value.  Values can be string or numeric.  If the type is string, then
# only = and != are valid operators.  If the string contains whitespace, it
# must be enclosed in quotes.  String values are case sensitive.  For example,
#
# Resource is up when its value is
# --------------------------------
# RESOURCE_UP_VALUE = UP "UP"
# RESOURCE_UP_VALUE!= DOWN Any value except "DOWN"
# RESOURCE_UP_VALUE= "On Course" "On Course"
#
# If the type is numeric, then it can specify a threshold, or a range to
# define a resource up condition.  If it is a threshold, then any operator
# may be used.  If a range is to be specified, then only > or >= may be used
# for the first operator, and only < or <= may be used for the second operator.
# For example,
# Resource is up when its value is
# --------------------------------
# RESOURCE_UP_VALUE     = 55     (threshold)
# RESOURCE_UP_VALUE     > 5.1    greater than 5.1     (threshold)
# RESOURCE_UP_VALUE     > -5 and < 10  between -5 and 10    (range)
#
# Note that "and" is required between the lower limit and upper limit
# when specifying a range.  The upper limit must be greater than the lower
# limit.  If RESOURCE_UP_VALUE is repeated within a RESOURCE_NAME block, then
# they are inclusively OR'd together.  Package Resource Dependencies may be
# defined by repeating the entire RESOURCE_NAME block.
#
# Example : RESOURCE_NAME/net/lan/lan0/res1
#     RESOURCE_POLLING_INTERVAL120
#     RESOURCE_UP_VALUE= RUNNING
#     RESOURCE_UP_VALUE= ONLINE
#
#     Means that the value of resource /net/lan/lan0/res1 will be
#    checked every 120 seconds, and is considered to be 'up' when
#    its value is "RUNNING" or "ONLINE".
#
# Uncomment the following lines to specify Package Resource Dependencies.
#
```


RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1391
3702
Doc:

```
#RESOURCE_NAME     <Full_path_name>
#RESOURCE_POLLING_INTERVAL  <numeric_seconds>
#RESOURCE_UP_VALUE     <op> <string_or_numeric> [and <op> <numeric>]


# The default for PKG_SWITCHING_ENABLED is YES. In the event of a
# failure, this permits the cluster software to transfer the package
# to an adoptive node.  Adjust as necessary.

PKG_SWITCHING_ENABLED    YES


# The default for NET_SWITCHING_ENABLED is YES.  In the event of a
# failure, this permits the cluster software to switch LANs locally
# (transfer to a standby LAN card).  Adjust as necessary.

NET_SWITCHING_ENABLED    YES


# The default for NODE_FAIL_FAST_ENABLED is NO.  If set to YES,
# in the event of a failure, the cluster software will halt the node
# on which the package is running.  Adjust as necessary.

NODE_FAIL_FAST_ENABLED    NO
```

Use the information on the Package Configuration worksheet to complete the file. Refer also to the comments on the configuration template for additional explanation of each parameter. You may include the following information:

- NODE_NAME. Enter the name of each node in the cluster on a separate line.
- RUN_SCRIPT and HALT_SCRIPT. Specify the pathname of the package control script (described in the next section). No default is provided.
- If your package contains services, enter the SERVICE_NAME, SERVICE_FAIL_FAST_ENABLED and SERVICE_HALT_TIMEOUT. values. Enter a group of these three for each service. You can configure no more than 30 services per package.
- If your package has IP addresses associated wtih it, enter the SUBNET. This must be a subnet that is already specified in the cluster confiugration.
- NODE_FAIL_FAST_ENABLED parameter. Enter YES or NO.

To configure monitoring within the package for a registered resource, enter values for the following parameters. Use the "Additional Package Resources" part of the "Package Configuration" subarea in SAM to obtain a list of resource names, polling intervals, and up values that you can set up as dependencies for your packages.

RQS nº 03/2005 - CN - CPMI - CORREIOS
1392
Fls Nº 3702
Doc:

- RESOURCE_NAME. Enter the name of a registered resource that is to be monitored by MC/ServiceGuard.
- RESOURCE_POLLING_INTERVAL. Enter the time between attempts to assure that the resource is healthy.
- RESOURCE_UP_VALUE. Enter the value or values that determine when the resource is considered to be up. During monitoring, if a different value is found for the resource, the package will fail.

This package configuration data is later combined with the cluster configuration data in the binary cluster configuration file.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1393
Doc: 3702

Writing the Package Control Script

The package control script contains all the information necessary to run all the services in the package, monitor them during operation, react to a failure, and halt the package when necessary. You can use either SAM or HP-UX commands to create or modify the package control script. For security reasons, the control script must reside in a directory with the string *cmcluster* in the path.

Using SAM to Write the Package Control Script

Select the High Availability options in SAM, then choose "Package Configuration." From the Action menu, choose "Create/Add a Package." The step menu appears, showing a group of options. The last two steps on the menu are for choosing the pathname of the package control script. Select each option after you define the package itself. For more information, use the Help key.

When you create a package control script this way, you do not need to do any further editing, but you may customize the script if you wish.

Using Commands to Write the Package Control Script

Each package must have a separate control script. The control script is placed in the package directory and is given the same name that it has in the package configuration file. The package control script contains both the run instructions and the halt instructions for the package. It must be executable. Use the following procedure to create a control scripts for the sample package *pkg1*.

First, generate a control script template:

```
# cmmakepkg -s /etc/cmcluster/pkg1/control.sh
```

You may customize the script, as described in the next section.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1394
Nº 3702
Doc:

17.477

Customizing the Package Control Script

Check the definitions and declarations at the beginning of the control script using the information in the Package Configuration worksheet. You need to customize as follows:

- Update the PATH statement to reflect any required paths needed to start your services.
- Enter the names of volume groups that will be activated.
- Add the names of logical volumes and file systems that will be mounted on them.
- Define IP subnet and IP address pairs for your package.
- Add service name(s).
- Add service command(s)
- Add a service restart parameter, if desired.

NOTE

Use care in defining service run commands. Each run command is executed by the control script in the following way:

- The `cmrunserv` command executes each run command and then monitors the process id of the process created by the run command.
- When the command started by `cmrunserv` exits, MC/ServiceGuard determines that a failure has occurred and takes appropriate action, which may include transferring the package to an adoptive node.
- If a run command is a shell script that runs some other command and then exits, MC/ServiceGuard will consider this normal exit as a *failure*.

To avoid problems in the execution of control scripts, ensure that each run command is the name of an actual service and that its process remains alive until the actual service stops.

If you need to define a set of run and halt operations in addition to the defaults, create functions for them in the sections under the heading `CUSTOMER DEFINED FUNCTIONS`. The next section shown an excerpt from the control script for a sample package configuration.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1395
Doc. 3702

Package Control Script Template File

```
# **********************************************************************
# *                                                                    *
# *        HIGH AVAILABILITY PACKAGE CONTROL SCRIPT (template)         *
# *                                                                    *
# *       Note: This file MUST be edited before it can be used.        *
# *                                                                    *
# **********************************************************************

# UNCOMMENT the variables as you set them.

# Set PATH to reference the appropriate directories.
PATH=/sbin:/usr/bin:/usr/sbin:/etc:/bin

# VOLUME GROUP ACTIVATION:
# Specify the method of activation for volume groups.
# Leave the default ("VGCHANGE="vgchange -a e") if you want volume
# groups activated in exclusive mode. This assumes the volume groups have
# been initialized with 'vgchange -c y' at the time of creation.
#
# Uncomment the first line (VGCHANGE="vgchange -a e -q n"), and comment
# out the default, if your disks are mirrored on separate physical paths,
#
# Uncomment the second line (VGCHANGE="vgchange -a y") if you wish to
# use non-exclusive activation mode. Single node cluster configurations
# must use non-exclusive activation.
#
# VGCHANGE="vgchange -a e -q n"
# VGCHANGE="vgchange -a y"
VGCHANGE="vgchange -a e"# Default

# VOLUME GROUPS
# Specify which volume groups are used by this package. Uncomment VG[0]=""
# and fill in the name of your first volume group. You must begin with
# VG[0], and increment the list in sequence.
#
# For example, if this package uses your volume groups vg01 and vg02, enter:
#         VG[0]=vg01
#         VG[1]=vg02
#
# The volume group activation method is defined above. The filesystems
# associated with these volume groups are specified below.
#
#VG[0]=""

# FILESYSTEMS
# Specify the filesystems which are used by this package. Uncomment
# LV[0]=""; FS[0]=""; FS_MOUNT_OPT[0]="" and fill in the name of your first
# logical volume, filesystem and mount option for the file system. You must
# begin with LV[0], FS[0] and FS_MOUNT_OPT[0] and increment the list in
# sequence.
#
# For example, if this package uses the file systems pkg1a and pkg1b,
# which are mounted on the logical volumes lvol1 and lvol2 with read and
# write options enter:
#         LV[0]=/dev/vg01/lvol1; FS[0]=/pkg1a; FS_MOUNT_OPT[0]="-o rw"
#         LV[1]=/dev/vg01/lvol2; FS[1]=/pkg1b; FS_MOUNT_OPT[1]="-o rw"
#
# The filesystems are defined as triplets of entries specifying the logical
# volume, the mount point and the mount options for the file system. Each
# filesystem will be fsck'd prior to being mounted. The filesystems will be
# mounted in the order specified during package startup and will be unmounted
# in reverse order during package shutdown. Ensure that volume groups
# referenced by the logical volume definitions below are included in
# volume group definitions above.
#
#LV[0]=""; FS[0]=""; FS_MOUNT_OPT[0]=""

# IP ADDRESSES
# Specify the IP and Subnet address pairs which are used by this package.
```


RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1396
Nº 3702 Doc:

475
- 17 -


```
# Uncomment IP[0]="" and SUBNET[0]="" and fill in the name of your first
# IP and subnet address. You must begin with IP[0] and SUBNET[0] and
# increment the list in sequence.
#
# For example, if this package uses an IP of 192.10.25.12 and a subnet of
# 192.10.25.0 enter:
#         IP[0]=192.10.25.12
#         SUBNET[0]=192.10.25.0 # (netmask=255.255.255.0)
#
# Hint: Run "netstat -i" to see the available subnets in the Network field.
#
# IP/Subnet address pairs for each IP address you want to add to a subnet
# interface card.  Must be set in pairs, even for IP addresses on the same
# subnet.
#
#IP[0]=""
#SUBNET[0]=""

# SERVICE NAMES AND COMMANDS.
# Specify the service name, command, and restart parameters which are
# used by this package. Uncomment SERVICE_NAME[0]="", SERVICE_CMD[0]="",
# SERVICE_RESTART[0]="" and fill in the name of the first service, command,
# and restart parameters. You must begin with SERVICE_NAME[0], SERVICE_CMD[0],
# and SERVICE_RESTART[0] and increment the list in sequence.
#
# For example:
#         SERVICE_NAME[0]=pkg1a
#         SERVICE_CMD[0]="/usr/bin/X11/xclock -display 192.10.25.54:0"
#         SERVICE_RESTART[0]=""  # Will not restart the service.
#
#         SERVICE_NAME[1]=pkg1b
#         SERVICE_CMD[1]="/usr/bin/X11/xload -display 192.10.25.54:0"
#         SERVICE_RESTART[1]="-r 2"    # Will restart the service twice.
#
#         SERVICE_NAME[2]=pkg1c
#         SERVICE_CMD[2]="/usr/sbin/ping"
#         SERVICE_RESTART[2]="-R" # Will restart the service an infinite
#                                 number of times.
#
# Note: No environmental variables will be passed to the command, this
# includes the PATH variable. Absolute path names are required for the
# service command definition.  Default shell is /usr/bin/sh.
#
#SERVICE_NAME[0]=""
#SERVICE_CMD[0]=""
#SERVICE_RESTART[0]=""

# DTC manager information for each DTC.
# Example: DTC[0]=dtc_20
#DTC_NAME[0]=
```

The above excerpt from the control script shows the assignment of values to a set of variables. The remainder of the script uses these variables to control the package by executing Logical Volume Manager commands, HP-UX commands, and MC/ServiceGuard commands including `cmrunserv`, `cmmodnet`, and `cmhaltserv`. Examine a copy of the control script template to see the flow of logic. Use the following command:

```
# cmmakepkg -s | more
```

The main function appears at the end of the script.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1397
Nº 3702
Doc:

Note that individual variables are optional; you should include only as many as you need for proper package operation. For example, if your package does not need to activate a volume group, omit the VG variables; if the package does not use services, omit the corresponding SERVICE_NAME, SERVICE_CMD, and SERVICE_RESTART variables; and so on.

After customizing the script, distribute it to each node in the cluster using rcp, ftp, or your favorite method of copying.

Adding Customer Defined Functions to the Package Control Script

You can add additional shell commands to the package control script to be executed whenever the package starts or stops. Simply enter these commands in the CUSTOMER DEFINED FUNCTIONS area of the script. This gives you the ability to further customize the control script.

An example of this portion of the script is shown below, with the date and echo commands included to log starts and halts of the package to a special file.

```
# START OF CUSTOMER DEFINED FUNCTIONS

# This function is a place holder for customer defined functions.
# You should define all actions you want to happen here, before the service is
# started.  You can create as many functions as you need.

function customer_defined_run_cmds
{
# ADD customer defined run commands.
: # do nothing instruction, because a function must contain some command.
 date >> /tmp/pkg1.datelog
 echo 'Starting pkg1' >> /tmp/pkg1.datelog
 test_return 51
}

# This function is a place holder for customer defined functions.
# You should define all actions you want to happen here, before the service is
# halted.

function customer_defined_halt_cmds
{
# ADD customer defined halt commands.
: # do nothing instruction, because a function must contain some command.
 date >> /tmp/pkg1.datelog
 echo 'Halting pkg1' >> /tmp/pkg1.datelog
 test_return 52
}

# END OF CUSTOMER DEFINED FUNCTIONS
```


RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1398
3702

17.473

Adding MC/ServiceGuard Commands in Customer Defined Functions

You can add MC/ServiceGuard commands (such as `cmmodpkg`) in the Customer Defined Functions section of a package control script. However, these commands must not interact with the package itself. Additionally, if an MC/ServiceGuard command interacts with another package, then you need to check all packages with MC/ServiceGuard commands for the possibility of a command loop.

For instance, a command loop might occur under the following circumstances. Suppose Pkg1 does a `cmmodpkg -d` of Pkg2, and Pkg2 does a `cmmodpkg -d` of Pkg1. If both Pkg1 and Pkg2 start at the same time, Pkg1 tries to `cmmodpkg` Pkg2. However, that `cmmodpkg` command has to wait for Pkg2 startup to complete. Pkg2 tries to `cmmodpkg` Pkg1, but Pkg2 has to wait for Pkg1 startup to complete, thereby causing a command loop.

To avoid this situation, it is a good idea to alway specify a `RUN_SCRIPT_TIMEOUT` and a `HALT_SCRIPT_TIMEOUT` for all packages, especially packages that use ServiceGuard commands in their control scripts. If a timeout is not specified and your configuration has a command loop as described above, inconsistent results can occur, including a hung cluster.

Adding or Removing Packages on a Running Cluster

You can add or remove packages while the cluster is running, subject to the limit of `MAX_CONFIGURED_PACKAGES`. To add or remove packages online, refer to the chapter on "Cluster and Package Maintenance."

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1399
Nº 3702 Doc.

Verify and Distribute the Configuration

You can use SAM or HP-UX commands to verify and distribute the binary cluster configuration file among the nodes of the cluster.

Distributing the Configuration File And Control Script with SAM

When you have finished creating a package in the Package Configuration subarea in SAM, you are asked to verify the copying of the files to all the nodes in the cluster. When you respond OK to the verification prompt, MC/ServiceGuard copies the binary configuration file and package control script to all the nodes in the cluster.

Copying Package Control Scripts with HP-UX commands

Use HP-UX commands to copy package control scripts from the configuration node to the same pathname on all nodes which can possibly run the package. Use your favorite method of file transfer (e. g., `rcp` or `ftp`). For example, from *ftsys9*, you can issue the `rcp` command to copy the package control script to *ftsys10*:

```
# rcp /etc/cmcluster/pkg1/control.sh
ftsys10:/etc/cmcluster/pkg1/control.sh
```

Distributing the Binary Cluster Configuration File with HP-UX Commands

Use the following steps from the node on which the ASCII cluster and package configuration files exist:

- Verify that the configuration file is correct. Use the following command:

```
# cmcheckconf -C /etc/cmcluster/cmclconf.ascii -P \
 /etc/cmcluster/pkg1/pkg1conf.ascii
```

- Activate the cluster lock volume group so that the lock disk can be initialized:

```
# vgchange -a y /dev/vg01
```


RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1400
Doc: 3702

- Generate the binary configuration file and distribute it across the nodes.

```
# cmapplyconf -v -C /etc/cmcluster/cmclconf.ascii -P \
 /etc/cmcluster/pkg1/pkg1conf.ascii
```

- Deactivate the cluster lock volume group.

```
# vgchange -a n /dev/vg01
```

The `cmapplyconf` command creates a binary version of the cluster configuration file and distributes it to all nodes in the cluster. This action ensures that the contents of the file are consistent across all nodes.

NOTE `cmcheckconf` and `cmapplyconf` must be used again any time changes are made to the cluster and package configuration files.

Verifying Cluster and Package Configuration

While configuring your MC/ServiceGuard cluster, it's a good idea to test that the various components of the cluster behave correctly in case of a failure. See the chapter "Troubleshooting Your Cluster" for an explanation of how to test that your cluster responds properly in the event of a package failure, a node failure, or a LAN failure.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1401
3702

17.470

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1402
Nº 3702
Doc:

7 Cluster and Package Maintenance

This chapter describes how to start and halt a cluster or an individual node, how to perform permanent reconfiguration, and how to start, halt, move, and modify packages during routine maintenance of the cluster. Topics are as follows:

- Managing the Cluster and Nodes
- Reconfiguring a Running Cluster
- Managing Packages and Services
- Reconfiguring Packages in a Running Cluster
- Responding to Cluster Events
- Single Node Operation
- Removing MC/ServiceGuard Software from a System

All administration tasks can be carried out using SAM or HP-UX commands. From the SAM main menu, choose Clusters, then High Availability Clusters, and select the appropriate type of administration — cluster or package administration.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1403
Nº 3702

Managing the Cluster and Nodes

Managing the cluster involves the following tasks:

- Starting the Cluster When All Nodes are Down
- Adding Previously Configured Nodes to a Running Cluster
- Removing Nodes from Operation in a Running Cluster
- Halting the Entire Cluster
- Reconfiguring a Halted Cluster

You can use SAM or MC/ServiceGuard commands to start or stop the cluster, and to modify the cluster configuration. Starting the cluster means running the cluster daemon on one or more of the nodes in a cluster. You use different MC/ServiceGuard commands to start the cluster depending on whether all nodes are currently down (that is, no cluster daemons are running), or whether you are starting the cluster daemon on an individual node.

Note the distinction that is made in this chapter between adding an already configured node to the cluster and adding a new node to the cluster configuration. An already configured node is one that is already entered in the cluster configuration file; a new node is added to the cluster by modifying the cluster configuration file.

Starting the Cluster When all Nodes are Down

You can use SAM or MC/ServiceGuard commands to start the cluster.

Using SAM to Start the Cluster

In SAM, choose Clusters, then High Availability Clusters. In the Cluster Administration area, highlight the cluster you wish to start, then select "Start Cluster" from the Actions menu. Indicate whether you wish to bring up the cluster on all nodes or on a subset of nodes. If you choose a subset, then you must select the nodes from the list. This option should be used only when you are sure that the cluster is not already running on any node.

At the verification prompt, select OK to start the cluster.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1404
3702
Doc:

Using MC/ServiceGuard Commands to Start the Cluster

Use the `cmruncl` command to start the cluster when all cluster nodes are down. Use the `-n` option to specify a particular group of nodes. Without this option, all nodes will be started. The following starts all nodes configured in the cluster:

```
# cmruncl -v
```

The following example starts up the locally configured cluster only on *ftsys9* and *ftsys10*. (This form of the command should only be used when you are sure that the cluster is not already running on any node.)

```
# cmruncl -v -n ftsys9 -n ftsys10
```

WARNING **MC/ServiceGuard cannot guarantee data integrity if you try to start a cluster with the `cmruncl -n` command while a subset of the cluster's nodes are already running a cluster. If the network connection is down between nodes, using `cmruncl -n` might result in a second cluster forming, and this second cluster might start up the same applications that are already running on the other cluster. The result could be two applications overwriting each other's data on the disks.**

Adding Previously Configured Nodes to a Running Cluster

You can use SAM or MC/ServiceGuard commands to bring a configured node up within a running cluster.

Using SAM to Add Previously Configured Nodes to a Running Cluster

In the Cluster Administration area, highlight the cluster you are adding the node to, then select "Specify Nodes to Join the Cluster." Choose the node or nodes you are adding, then choose OK. Only nodes that are members of the current cluster configuration may be selected.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1405
3702

Using MC/ServiceGuard Commands to Add Previously Configured Nodes to a Running Cluster

Use the `cmrunnode` command to add one or more nodes to an already running cluster. Any node you add must already be a part of the cluster configuration. The following example adds node *ftsys8* to the cluster that was just started with only nodes *ftsys9* and *ftsys10*:

```
# cmrunnode -v ftsys8
```

Since the node's cluster is already running, the node joins the cluster and packages may be started. If the node does not find its cluster running, or the node is not part of the cluster configuration, the command fails.

Removing Nodes from Operation in a Running Cluster

You can use SAM or HP-UX commands to remove nodes from operation in a cluster. This operation removes the node from cluster operation by halting the cluster daemon, but it does not modify the cluster configuration. To remove a node from the cluster configuration permanently, you must recreate the cluster configuration file. See the next section.

Using SAM to Remove Nodes from Operation

In the Cluster Administration area, highlight the cluster you are interested in, then select "Specify Nodes to Leave the Cluster" from the Actions menu. Choose the node or nodes, then select OK.

If a package is running on a node you are shutting down, you will see a message asking for a verification that you wish to shut down the node anyway. Reply OK to verify shutdown. Following shutdown, any package that can switch to an adoptive node will start up on the adoptive node.

Using MC/ServiceGuard Commands to Remove Nodes from Operation

Use the `cmhaltnode` command to halt one or more nodes in a cluster. The cluster daemon on the specified node stops, and the node is removed from active participation in the cluster.

To halt a node with a running package, use the `-f` option. If a package was running that can be switched to an adoptive node, the switch takes place and the package starts on the adoptive node. For example, the

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1406
3702

following command causes the ServiceGuard daemon running on node *ftsys9* in the sample configuration to halt and the package running on *ftsys9* to move to *ftsys10*:

```
# cmhaltnode -f -v  ftsys9
```

This halts any packages running on the node *ftsys9* by executing the halt instructions in each package's control script. *ftsys9* is halted and the packages start on the adoptive node, *ftsys10*.

The use of `cmhaltnode` is a convenient way of bringing a node down for system maintenance while keeping its packages available on other nodes. After maintenance, the package can be returned to its primary node. See "Moving a Package," below.

To return a node to the cluster, use `cmrunnode`.

Halting the Entire Cluster

You can use SAM or MC/ServiceGuard commands to halt a running cluster.

Using SAM to Halt the Cluster

In the Cluster Administration area, highlight the cluster you wish to halt, then select "Shut Down Cluster" from the Actions menu to halt the selected cluster on all nodes. At the verification prompt, choose OK.

Using MC/ServiceGuard Commands to Halt a Cluster

The `cmhaltcl` command can be used to halt the entire cluster. This command causes all nodes in a configured cluster to halt their MC/ServiceGuard daemons. You can use the `-f` option to force the cluster to halt even when packages are running. This command can be issued from any running node. Example:

```
# cmhaltcl -f -v
```

This halts all nodes that are configured in the cluster.

RQS nº 03/2005 - CN - CPMI - CORREIOS
1407
Fls Nº
3702
Doc:

Reconfiguring a Halted Cluster

You can also make a permanent change in cluster configuration when the cluster is halted. This procedure *must* be used for changes to the lock disk configuration, changes in timing prarmeters, and changes to the Maximum Number of Packages parameter, but it can be used for any other cluster configuration changes as well.

Use the following steps:

1. Halt the cluster on all nodes.
2. On one node, reconfigure the cluster as described in the chapter "Building an HA Cluster Configuration." You can do this by using SAM or by issuing the `cmquerycl` command to generate an ASCII file, which you then edit.
3. Make sure that all nodes listed in the cluster configuration file are powered up and accessible. Use SAM or the `cmapplyconf` command to copy the binary cluster configuration file to all nodes. This file overwrites any previous version of the binary cluster configuration file.
4. Use SAM or the `cmruncl` command to start the cluster on all nodes or on a subset of nodes, as desired.

Using SAM to Change the Maximum Packages Parameter

After halting the cluster, go to the Cluster Configuration area, and choose "Modify Cluster Configuration" from the Actions menu. Then select "Modify Cluster Package Requirements." Enter the new maximum number of packages in the space provided, and click OK.

Using MC/ServiceGuard Commands to Change MAX_CONFIGURED_PACKAGES

Use the `cmgetconf` command to obtain a current copy of the cluster's existing configuration. Example:

```
# cmgetconf -C clconfig.ascii
```

Edit the `clconfig.ascii` file to include the desired value for MAX_CONFIGURED_PACKAGES. Then use the `cmcheckconf` command to verify the new configuration. Use the `cmapplyconf` command to apply the changes to the configuration and send the new configuration file to all cluster nodes.

Automatically Restarting the Cluster

You can configure your cluster to automatically restart after an event, such as a long-term power failure, which brought down all nodes in the cluster. This is done by setting `AUTOSTART_CMCLD` to 1 in the `/etc/rc.config.d/cmcluster` file.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1409
3702

17462

Reconfiguring a Running Cluster

You can add new nodes to the cluster configuration or delete nodes from the cluster configuration while the cluster is up and running. Note the following, however:

- You cannot change the lock disk configuration while the cluster is running.
- You cannot remove an active node from the cluster. You must halt the node first.
- You cannot delete an active volume group from the cluster configuration. You must halt any package that uses the volume group and ensure that the volume is inactive before deleting it.
- You cannot change cluster timing parameters.
- The only configuration change allowed while a node is unreachable (for example, completely disconnected from the network) is to delete the unreachable node from the cluster configuration. If there are also packages that depend upon that node, the package configuration must also be modified to delete the node. This all must be done in one configuration request (`cmapplyconf` command).

Changes to the package configuration are described in a later section.

Table 7-1 Types of Changes to Permanent Cluster Configuration

Change to the Cluster Configuration	Required Cluster State
Add a new node	All cluster nodes must be running. Serial heartbeat must not be configured.
Delete a node	A node can be deleted even though it is unavailable or unreachable.
Change Maximum Configured Packages	Cluster must not be running.
Change Timing Parameters	Cluster must not be running.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1410
3702

Change to the Cluster Configuration	Required Cluster State
Change Cluster Lock Configuration	Cluster must not be running.
Change serial device files	Cluster must not be running
Change IP addresses for heartbeats or monitored subnets	Cluster must not be running

The following sections describe how to perform dynamic reconfiguration tasks using SAM or using MC/ServiceGuard commands.

Using SAM to Add Nodes to the Configuration While the Cluster is Running

Use the Cluster Configuration area of SAM, and choose "Modify Cluster Configuration" from the Actions menu. Then select "Modify Cluster Name and Nodes." Highlight the name of the node you wish to add to the cluster in the list on the right of the screen, then click the Add button. When you are finished changing the node list, click OK.

Using MC/ServiceGuard Commands to Add Nodes to the Configuration While the Cluster is Running

Use the following procedure to add a node with HP-UX commands. For this example, nodes *ftsys8* and *ftsys9* are already configured in a running cluster named *cluster1*, and you are adding node *ftsys10*.

1. Use the following command to store a current copy of the existing cluster configuration in a temporary file:

```
# cmgetconf -C temp.ascii
```

2. Specify a new set of nodes to be configured and generate a template of the new configuration:

```
# cmquerycl -C clconfig.ascii -c cluster1 \
  -n ftsys8 -n ftsys9 -n ftsys10
```

3. Edit the file `clconfig.ascii` to check the information about the new node.
4. Verify the new configuration:

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1411
Doc: 3702

```
# cmcheckconf -C clconfig.ascii
```

5. Apply the changes to the configuration and send the new binary configuration file to all cluster nodes:

```
# cmapplyconf -C clconfig.ascii
```

Use `cmrunnode` to start the new node, and, if desired, set the AUTOSTART_CMCLD parameter to 1 in the `/etc/rc.config.d/cmcluster` file to enable the new node to join the cluster automatically each time it reboots.

Using SAM to Delete Nodes from the Configuration While the Cluster is Running

In the Cluster Administration area of SAM, halt the node that you wish to remove from the cluster configuration. Then go to the Cluster Configuration area, and choose "Modify Cluster Configuration" from the Actions menu. Then select "Modify Cluster Name and Nodes." Highlight the name of the node you wish to delete from the cluster in the list of configured nodes, then click the Remove button. When you are finished changing the node list, click OK.

If the node you wish to delete is unreachable (disconnected from the LAN, for example), you can use SAM to delete the node only if there are no packages which specify the unreachable node. If there are packages that depend on the unreachable node, use MC/ServiceGuard commands as described in the next section.

Using MC/ServiceGuard Commands to Delete Nodes from the Configuration While the Cluster is Running

Use the following procedure to delete a node with HP-UX commands. For this example, nodes *ftsys8*, *ftsys9* and *ftsys10* are already configured in a running cluster named *cluster1*, and you are deleting node *ftsys10*.

1. Use the following command to store a current copy of the existing cluster configuration in a temporary file:

```
# cmgetconf -C temp.ascii
```

2. Specify the new set of nodes to be configured (omitting *ftsys10*) and generate a template of the new configuration:

```
# cmquerycl -C clconfig.ascii -c cluster1 -n ftsys8 -n ftsys9
```


RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1412
Doc: 3702

3. Edit the file `clconfig.ascii` to check the information about the new node.
4. Verify the new configuration:

```
# cmcheckconf -C clconfig.ascii
```

5. Apply the changes to the configuration and send the new binary configuration file to all cluster nodes:

```
# cmapplyconf -C clconfig.ascii
```

Use `cmrunnode` to start the new node, and, if desired, set the AUTOSTART_CMCLD parameter to 1 in the `/etc/rc.config.d/cmcluster` file to enable the new node to join the cluster automatically each time it reboots.

NOTE If you are attempting to remove an unreachable node that has many packages dependent on it, especially if the dependent packages use a large number of EMS resources, you may see the following message:

```
The configuration change is too large to process while the cluster is running.
Split the configuration change into multiple requests or halt the cluster.
```

In this situation, you must halt the cluster to remove the unreachable node.

Using SAM to Change the Volume Group Configuration While the Cluster is Running

In SAM, go to the Cluster Configuration area, and choose "Modify Cluster Configuration" from the Actions menu. Then select "Modify Cluster Package Requirements." You can add or delete volume groups by highlighting the volume group name and adding it to or removing it from the list of cluster-aware volume groups.

You *cannot* change the cluster lock volume group or physical volume configuration while the cluster is running.

NOTE If you are removing a volume group from the cluster configuration, make sure that you also modify or delete any package control script that activates and deactivates this volume group. In addition, you should use the LVM `vgexport` command on the removed volume group from each node that will no longer be using the volume group.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1413
Doc 3702

Using MC/ServiceGuard Commands to Change the Volume Group Configuration While the Cluster is Running

Use the `cmgetconf` command to obtain a current copy of the cluster's existing configuration. Example:

```
# cmgetconf -C clconfig.ascii
```

Edit the file `clconfig.ascii` to add or delete volume groups. Then use the `cmcheckconf` command to verify the new configuration. Use the `cmapplyconf` command to apply the changes to the configuration and send the new configuration file to all cluster nodes.

NOTE If you are deleting from the cluster a volume group that is currently activated by a package, the configuration will be changed but the deletion will not take effect until the package is halted; thereafter, the package will no longer be able to run without further modification, such as removing the volume group from the package control script.

RQS nº 03/2005 CN - CPMI - CORREIOS
Fls Nº 1414
3702

Managing Packages and Services

Managing packages and services involves the following tasks:

- Starting a Package
- Halting a Package
- Moving a Package
- Adding a Package to a Running Cluster
- Deleting a Package from a Running Cluster
- Reconfiguring a Package on a Running Cluster
- Reconfiguring a Package on a Halted Cluster

You can use SAM or MC/ServiceGuard commands to perform these tasks.

Starting a Package

Ordinarily, a package configured as part of the cluster will start up on its primary node when the cluster starts up. You may need to start a package manually after it has been halted manually. You can do this either in SAM or with MC/ServiceGuard commands.

Using SAM to Start a Package

In SAM, select "Package Administration," then choose the package you wish to start. From the "Actions" menu, choose "Start Package." If you wish to start the package on a specific node, choose "Start a Package on a Specific Node." Otherwise, choose "Start Package," and reply Yes to the verification prompt.

Using MC/ServiceGuard Commands to Start a Package

Use the `cmrunpkg` command to run the package on a particular node, then use the `cmmodpkg` command to enable switching for the package. Example:

```
# cmrunpkg -n ftsys9 pkg1
# cmmodpkg -e pkg1
```


RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1415
Doc: 3702

This starts up the package on *ftsys9*, then enables package switching. This sequence is necessary when a package has previously been halted on some node, since halting the package disables switching.

Halting a Package

You halt an MC/ServiceGuard package when you wish to bring the package out of use but wish the node to continue in operation. You can halt a package using SAM or using MC/ServiceGuard commands. Halting a package has a different effect than halting the node. When you halt the node, its packages may switch to adoptive nodes (assuming that switching is enabled for them); when you halt the package, it is disabled from switching to another node, and must be restarted manually on another node or on the same node.

Using SAM to Halt a Package

In the SAM "Package Administration" area, choose a package from the list, then select "Halt Package" from the Actions menu. Choose OK in response to the verification prompt. When you halt the package in this way, it is disabled from switching to another node.

Using MC/ServiceGuard Commands to Halt a Package

Use the `cmhaltpkg` command to halt a package, as follows:

```
# cmhaltpkg pkg1
```

This halts pkg1 and disables it from switching to another node.

Moving a Package

You can use SAM or MC/ServiceGuard commands to move a package from one node to another.

Using SAM to Move a Running Package

From the Package Administration screen in SAM, choose a package, then select "Move a Package" from the Actions menu. Choose the node you wish to move the package to, then select OK. Reply Yes to the verification prompt.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1416
Doc. 3702

17.455

Using MC/ServiceGuard Commands to Move a Running Package

Before you move the package, halt it on its original node using the `cmhaltpkg` command. This action not only halts the package, but also disables switching the package back to the node on which it halts.

After you have moved the package you must restart it and enable switching. You can do this in SAM or by issuing the `cmrunpkg` command followed by `cmmodpkg -e` *package_name*. `cmmodpkg` can be used with the `-n` option to enable a package to run on a node if the package has been disabled from running on that node due to some sort of error. If no node is specified, the node the command is run on is the implied node.

Example:

```
# cmhaltpkg pkg1
# cmrunpkg -n ftsys10 pkg1
# cmmodpkg -e pkg1
```

Reconfiguring on a Halted Cluster

You can also make permanent changes in package configuration while the cluster is not running. Use the following steps:

- On one node, reconfigure the package as described earlier in this chapter. You can do this by using SAM or by editing the package ASCII file.
- Edit the package control script directly or use the "Edit a Package Control Script" option in SAM. Any changes in service names will also require changes in the package configuration file.
- Use SAM or the `cmapplyconf` command to copy the binary cluster configuration file to all nodes. Use the -P option, specifying the package to be changed; do not use the -C option. This file overwrites any previous version of the binary cluster configuration file.
- Copy the modified control script to all nodes that can run the package.
- Use SAM or the `cmruncl` command to start the cluster on all nodes or on a subset of nodes, as desired. The package will start up as nodes come online.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1417
Nº 3702
Doc:

J7454

Reconfiguring a Package on a Running Cluster

You can reconfigure a package while the cluster is running, and in some cases you can reconfigure the package while the package itself is running. Only certain changes may be made while the package is running.

To modify the package, use the SAM "Package Configuration" subarea, and choose options as described in Chapter 6. Alternatively, with HP-UX commands, use the following procedure (*pkg1* is used as an example):

1. Halt the package if necessary:

   ```
   # cmhaltpkg  pkg1
   ```

   See Table 7-2 to determine whether this step is needed.

2. If it is not already available, you can obtain a copy of the package's ASCII configuration file by using the `cmgetconf` command, specifying the package name.

   ```
   # cmgetconf -P pkg1.ascii
   ```

3. Edit the ASCII package configuration file.

4. Verify your changes as follows:

   ```
   # cmcheckconf -v -P pkg1.ascii
   ```

5. Distribute your changes to all nodes:

   ```
   # cmapplyconf -v -P pkg1.ascii
   ```

6. Copy the package control script to all nodes that can run the package.

Adding a Package to a Running Cluster

You can create a new package and add it to the cluster configuration while the cluster is up and while other packages are running. The number of packages you can add is subject to the value of *Maximum Configured Packages* as set in SAM or as defined in the cluster configuration file.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
1418
Fls Nº
Nº 3702
Doc:

17453

To create the package, follow the steps given in the chapter "Configuring Packages and Services" with the following difference: *do not* specify the cluster name when verifying and distributing the configuration with HP-UX commands. For example, to use HP-UX commands to verify the configuration of newly created *pkg1* on a running cluster:

```
# cmcheckconf -P /etc/cmcluster/pkg1/pkg1conf.ascii
```

Use an HP-UX command like the following to distribute the new package configuration to all nodes in the cluster:

```
# cmapplyconf -P /etc/cmcluster/pkg1/pkg1conf.ascii
```

Remember to copy the control script to the /etc/cmcluster/pkg1 directory on all nodes that can run the package.

Deleting a Package from a Running Cluster

You can delete a package from all cluster nodes by using the `cmdeleteconf` command. The command can only be executed when the package is not running; the cluster may be up. The command removes the package information from the binary configuration file on all the nodes in the cluster.

The following example halts package *mypkg* and removes the package configuration from the cluster:

```
# cmhaltpkg mypkg
# cmdeleteconf -p mypkg
```

The command prompts for a verification before deleting the files unless you use the `-f` option. The directory `/etc/cmcluster/mypkg` is not deleted by this command.

Changing the PACKAGE_SWITCHING_ENABLED Flag

To change package switching behavior in a running cluster so that the new behavior remains in effect across cluster restarts, perform the following steps:

1. To immediately change package switching behavior while the cluster is running, use the `cmmodpkg` command. For example, if you want to disable switching for a running package on a given node, enter the following:

   ```
   # cmmodpkg -d pkg1
   ```


RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1419
Doc 3702

2. To change the default configuration so that the next time the cluster restarts the change you made in package switching is still in effect, you must change the PACKAGE_SWITCHING_ENABLED flag in the package configuration file. (Any change in this flag will only take effect the next time the cluster is restarted.)

   See the previous section "Reconfiguring a Package on a Running Cluster" for detailed instructions.

Allowable Package States During Reconfiguration

All nodes in the cluster must be powered up and accessible when making configuration changes.

Refer to Table 7-2 to determine whether or not the package may be running while you implement a particular kind of change. Note that for all of the following cases the cluster may be running, and also packages other than the one being reconfigured may be running.

Table 7-2 Types of Changes to Packages

Change to the Package	Required Package State
Add a new package	Other packages may be in any state.
Delete a package	Package must not be running.
Add a service	Package must not be running.
Remove a service	Package must not be running.
Add a subnet	Package must not be running. Subnet must already be configured into the cluster.
Remove a subnet	Package must not be running.
Add a resource	Package must not be running. Resource must already be configured into the cluster.
Remove a resource	Package must not be running.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1420
3702
Doc:

Change to the Package	Required Package State
Add a volume group	Package must not be running. Volume group must already be configured into the cluster.
Remove a volume group	Package must not be running.
Change run script contents	It is recommended that the package be halted. If the run script for the package is modified while the package is running, timing may cause problems.
Change halt script contents	It is recommended that the package be halted. If the halt script for the package is modified while the package is running, timing may cause problems.
Script timeouts	Package may be either running or halted.
Service timeouts	Package must not be running.
Service failfast	Package must not be running.
Package switching	Package may be either running or halted.
Network switching	Package may be either running or halted.
Change the order of nodes where a package may run	Package may be either running or halted.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1421
Nº 3702
Doc:

17.450

Responding to Cluster Events

MC/ServiceGuard does not require much ongoing system administration intervention. As long as there are no failures, your cluster will be monitored and protected. In the event of a failure, those packages that you have designated to be transferred to another node will be transferred automatically. Your ongoing responsibility as the system administrator will be to monitor the cluster and determine if a transfer of package has occurred. If a transfer has occurred, you have to determine the cause and take corrective actions.

The Event Monitoring Service and its HA monitors can provide monitoring for disks, LAN cards, and some system events. Refer to the manual *Using EMS HA Monitors* (B5735-90001) for more information.

The typical corrective actions to take in the event of a transfer of package include:

- Determining when a transfer has occurred.
- Determining the cause of a transfer.
- Repairing any hardware failures.
- Correcting any software problems.
- Restarting nodes.
- Transferring packages back to their original nodes.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1422
Doc: 3702

Single-Node Operation

The number of nodes you will need for your MC/ServiceGuard cluster depends on the processing requirements of the applications you want to protect. You may want to configure a single node cluster to take advantage of MC/ServiceGuard's network failure protection. Even in a multi-node cluster, you could have a situation where all but one node has failed, or where you have shut down all but one node, leaving your cluster in single-node operation. This remaining node will probably have applications running on it. As long as the MC/ServiceGuard daemon *cmcld* is active, other nodes can re-join the cluster at a later time.

If the MC/ServiceGuard daemon fails when in single-node operation, it will leave the single node up and your applications running. This is different from the loss of the MC/ServiceGuard daemon in a multi-node cluster, which halts the node with a TOC, and causes packages to be switched to adoptive nodes. It is not necessary to halt the single node in this scenario, since the application is still running, and no other node is currently available for package switching. However, you should *not* try to restart MC/ServiceGuard, since data corruption might occur if another node were to attempt to start up a new instance of the application that is still running on the single node.

Instead of restarting the cluster, choose an appropriate time to shutdown and reboot the node, which will allow the applications to shut down and then permit MC/ServiceGuard to restart the cluster after rebooting.

RQS nº 03/2005 - CN - CPMI - CORREIOS
1423
Fls Nº
Doc: 3702

Removing MC/ServiceGuard from a System

If you wish to remove a node from MC/ServiceGuard use, use the `swremove` command to delete the software. Note the following:

- The cluster should not be running on the node from which you will be deleting MC/ServiceGuard.
- The node from which you are deleting MC/ServiceGuard should not be in the cluster configuration.
- If you are removing MC/ServiceGuard from more than one node, **`swremove`** should be issued on one node at a time.

CPMI - CORREIOS
1424
3702

8 Troubleshooting Your Cluster

This chapter describes how to verify cluster operation, how to review cluster status, and how to solve some typical cluster problems. Topics are as follows:

- Testing Cluster Operation
- Monitoring Hardware
- Replacing Disks
- Troubleshooting Approaches
- Solving Problems

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1425
Doc: 3702

Testing Cluster Operation

Once you have configured your MC/ServiceGuard cluster, it's a good idea to verify that the various components of the cluster behave correctly in case of a failure. In this section, the following procedures test that the cluster responds properly in the event of a package failure, a node failure, or a LAN failure.

CAUTION In testing the cluster in the following procedures, be aware that you are causing various components of the cluster to fail, so that you can determine that the cluster responds correctly to failure situations. As a result, the availability of nodes and applications may be disrupted.

Start the Cluster using SAM

If you have just finished configuring your cluster, start the cluster running before you proceed.

To start the cluster, in SAM:

1. Choose Clusters, then High Availability Clusters.
2. In the Cluster Administration area, highlight the cluster you wish to start, then select "Start Cluster" from the Actions menu.
3. Indicate whether you wish to bring up the cluster on all nodes or on a subset of nodes. If you choose a subset, then you must select the nodes from the list. This option should be used only when you are sure that the cluster is not already running on any node.
4. At the verification prompt, select OK to start the cluster.

Testing the Package Manager

To test that the package manager is operating correctly, perform the following procedure for each package on the cluster:

1. Obtain the PID number of a service in the package by entering

   ```
   # ps -ef | grep "service_cmd"
   ```

   where *service_cmd* is the executable specified in the package control script with the parameter SERVICE_CMD. The service selected must not have restarts specified.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1426
Doc 3702

2. To kill the *service_cmd* PID, enter

   ```
   # kill PID
   ```

3. To view the package status, enter

   ```
   # cmviewcl -v
   ```

   The package should be running on the specified adoptive node.

4. Move the package back to the primary node using SAM.

   From the Package Administration screen in SAM, choose a package, then select "Move a Package" from the Actions menu. Choose the node you wish to move the package to, then select OK. Reply Yes to the verification prompt.

   Depending on the specific databases you are running, perform the appropriate database recovery.

Testing the Cluster Manager

To test that the cluster manager is operating correctly, perform the following steps for each node on the cluster:

1. Turn off the power to the node SPU.
2. To observe the cluster reforming, enter the following command on some other configured node:

   ```
   # cmviewcl -v
   ```

   You should be able to observe that the powered down node is halted, and that its packages have been correctly switched to other nodes.

3. Turn on the power to the node SPU.
4. To verify that the node is rejoining the cluster, enter the following command on any configured node:

   ```
   # cmviewcl -v
   ```

   The node should be recognized by the cluster, but its packages should *not* be running.

5. Move the packages back to original node using SAM.

   From the Package Administration screen in SAM, choose a package, then select "Move a Package" from the Actions menu. Choose the node you wish to move the package to, then select OK. Reply Yes to the verification prompt.

RQS nº 03/2005 - CN
CPMI - CORREIOS
1427
Fls. Nº
3702
Doc.

Depending on the specific databases you are running, perform the appropriate database recovery.

6. Repeat this procedure for all nodes in the cluster one at a time.

Testing the Network Manager

To test that the network manager is operating correctly, for each node on the cluster do the following:

1. To identify primary and standby lan cards on the node, enter

   ```
   # lanscan
   ```

   and then

   ```
   # cmviewcl -v
   ```

2. Disconnect the LAN connection from the Primary card. (Be careful not to break the subnet if you are using ThinLAN cables.)
3. Using `cmviewcl -v`, verify that a local switch has taken place so that the Standby card is now the Primary card.
4. Reconnect the LAN to the original Primary card, and verify its status using `cmviewcl -v`.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1428
Doc: 3702

17.443

Monitoring Hardware

Good standard practice in handling a high availability system includes careful fault monitoring so as to prevent failures if possible or at least to react to them swiftly when they occur. The following should be monitored for errors or warnings of all kinds:

- Disks
- CPUs
- Memory
- LAN cards
- Power sources
- All cables
- Disk interface cards

Some monitoring can be done through simple physical inspection, but for the most comprehensive monitoring, you should examine the system log file (/var/adm/syslog/syslog.log) periodically for reports on all configured HA devices. The presence of errors relating to a device will show the need for maintenance.

Using Event Monitoring Service

Event Monitoring Service (EMS) allows you to configure monitors of specific devices and system resources. You can direct alerts to an administrative workstation where operators can be notified of further action in case of a problem. For example, you could configure a disk monitor to report when a mirror was lost from a mirrored volume group being used in the cluster

Refer to the *Using EMS HA Monitors* (B5735-90001) for additional information.

Using HP Predictive Monitoring

In addition to messages reporting actual device failure, the logs may accumulate messages of lesser severity which, over time, can indicate that a failure may happen soon. One product that provides a degree of

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1429
Doc: 3702

17443

automation in monitoring is called HP Predictive, which gathers information from the status queues of a monitored system to see what errors are accumulating. This tool will report failures and will also predict failures based on statistics for devices that are experiencing specific non-fatal errors over time. In an MC/ServiceGuard cluster, HP Predictive should be run on all nodes.

HP Predictive also reports error conditions directly to an HP Response Center, alerting support personnel to the potential problem. HP Predictive is available through various support contracts. For more information, contact your HP representative.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1430
Doc: 3702

Replacing Disks

The procedure for replacing a faulty disk mechanism depends on the type of disk configuration you are using. Separate descriptions are provided for replacing an array mechanism and a disk in a high availability enclosure.

Replacing a Faulty Array Mechanism

With any HA disk array configured in RAID 1 or RAID 5, refer to the array's documentation for instruction on how to replace a faulty mechanism. After the replacement, the device itself automatically rebuilds the missing data on the new disk. No LVM activity is needed. This process is known as *hot swapping* the disk.

Replacing a Faulty Mechanism in an HA Enclosure

If you are using software mirroring with MirrorDisk/UX and the mirrored disks are mounted in a high availability disk enclosure, you can use the following steps to *hot plug* a disk mechanism:

1. Identify the physical volume name of the failed disk and the name of the volume group in which it was configured. In the following examples, the volume group name is shown as /dev/vg_sg01 and the physical volume name is shown as /dev/c2t3d0. Substitute the volume group and physical volume names that are correct for your system.
2. Identify the names of any logical volumes that have extents defined on the failed physical volume.
3. On the node on which the volume group is currently activated, use the following command *for each logical volume that has extents on the failed physical volume*:

   ```
   # lvreduce -m 0 /dev/vg_sg01/lvolname /dev/dsk/c2t3d0
   ```

4. At this point, remove the failed disk and insert a new one. The new disk will have the same HP-UX device name as the old one.
5. On the node from which you issued the `lvreduce` command, issue the following command to restore the volume group configuration data to the newly inserted disk:

RQS nº 03/2005 - CN
CPMI - CORREIOS
1431
Fls Nº
3702
Doc:

```
# vgcfgrestore /dev/vg_sg01 /dev/dsk/c2t3d0
```

6. Issue the following command to extend the logical volume to the newly inserted disk:

```
# lvextend -m1 /dev/vg_sg01 /dev/dsk/c2t3d0
```

7. Finally, use the `lvsync` command *for each logical volume that has extents on the failed physical volume.* This synchronizes the extents of the new disk with the extents of the other mirror.

```
# lvsync /dev/vg_sg01/lvolname
```

Replacing a Lock Disk

Replacing a failed lock disk mechanism is the same as replacing a data disk. If you are using a *dedicated* lock disk (one with no user data on it), then you need to issue only one LVM command:

```
# vgcfgrestore /dev/vg_lock /dev/dsk/c2t3d0
```

Online Hardware Maintenance with In-line SCSI Terminator

MC/ServiceGuard allows online SCSI disk controller hardware repairs to all cluster nodes if you use HP's *in-line terminator* (C2980A) on nodes connected to the end of the shared FW/SCSI bus. The in-line terminator cable is a 0.5 meter extension cable with the terminator on the male end, which connects to the controller card for an external bus. The in-line terminator is used *instead of* the termination pack that is attached to the controller card and makes it possible to physically disconnect the node from the end of the F/W SCSI bus without breaking the bus's termination. (Nodes attached to the middle of a bus using a Y cable also can be detached from the bus without harm.) When using in-line terminators and Y cables, ensure that all orange-socketed termination packs are *removed* from the controller cards.

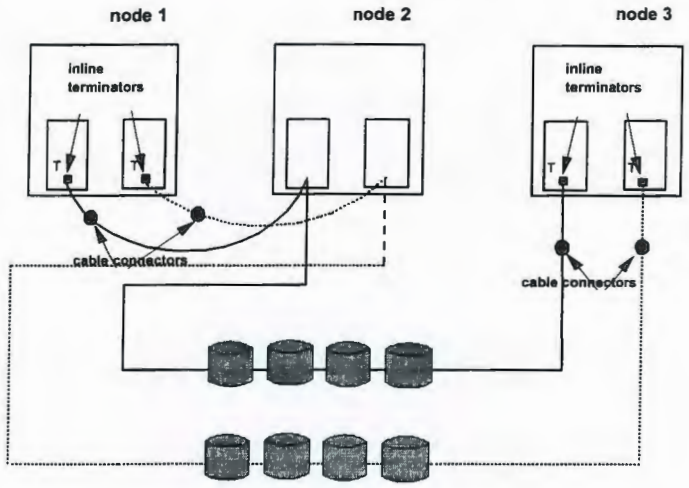
NOTE You cannot use inline terminators with internal FW/SCSI buses on D and K series systems, and you cannot use the inline terminator with single-ended SCSI buses. You must *not* use an inline terminator to connect a node to a Y cable.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1432
Doc: 3702

17.439

Figure 8-1 shows a three-node cluster with two F/W SCSI buses. The solid line and the dotted line represent different buses, both of which have inline terminators attached to nodes 1 and 3. Y cables are also shown attached to node 2.

Figure 8-1 F/W SCSI Buses with In-line Terminators



The use of in-line SCSI terminators allows you to do hardware maintenance on a given node by temporarily moving its packages to another node and then halting the original node while its hardware is serviced. Following the replacement, the packages can be moved back to the original node.

Use the following procedure to disconnect a node that is attached to the bus with an in-line SCSI terminator or with a Y cable:

1. Move any packages on the node that requires maintenance to a different node.
2. Halt the node that requires maintenance. The cluster will re-form, and activity will continue on other nodes. Packages on the halted node will switch to other available nodes if they are configured to switch.
3. Disconnect the power to the node.

RQS nº 03/2005 - CN - CPMI - CORREIOS
1433
Fls Nº
3702
Doc.

4. Disconnect the node from the in-line terminator cable or Y cable if necessary. The other nodes accessing the bus will encounter no problems as long as the in-line terminator or Y cable remains connected to the bus.
5. Replace or upgrade hardware on the node, as needed.
6. Reconnect the node to the in-line terminator cable or Y cable if necessary.
7. Reconnect power and reboot the node. If AUTOSTART_CMCLD is set to 1 in the /etc/rc.config.d/cmcluster file, the node will rejoin the cluster.
8. If necessary, move packages back to the node from their alternate locations and restart them.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1434
Doc: 3702

17437

Troubleshooting Approaches

The following sections offer a few suggestions for troubleshooting by reviewing the state of the running system and by examining cluster status data, log files, and configuration files. Topics include:

- Reviewing Cluster and Package States
- Reviewing Package IP addresses
- Reviewing the System Log File
- Reviewing Configuration Files
- Reviewing the Package Control Script
- Using `cmquerycl` and `cmcheckconf`
- Using `cmscancl` and `cmgetconf`
- Reviewing the LAN Configuration

Reviewing Cluster and Package States

A cluster or its component nodes may be in several different states at different points in time. Status information for clusters, packages and other cluster elements is shown in the output of the `cmviewcl` command and in some displays in SAM. This section explains the meaning of many of the common conditions the cluster or package may be in.

Information about cluster status is stored in the status database, which is maintained on each individual node in the cluster. You can display information contained in this database by issuing the `cmviewcl` command:

```
# cmviewcl -v
```

The command when issued with the `-v` option displays information about the whole cluster. See the man page for a detailed description of other `cmviewcl` options.

Cluster Status

The *status* of a cluster may be one of the following:

- Up. At least one node has a running cluster daemon, and reconfiguration is not taking place.

ROS nº 03/2005 - CN - CPMI - CORREIOS
1435
Fls. Nº
3702
Doc:

- Down. No cluster daemons are running on any cluster node.
- Starting. The cluster is in the process of determining its active membership. At least one cluster daemon is ruuning.

Node Status and State

The *status* of a node is either up (*active* as a member of the cluster) or down (*inactive* in the cluster), depending on whether its cluster daemon is running or not. Note that a node might be down from the cluster perspective, but still up and running HP-UX.

A node may also be in one of the following states:

- Failed. A node never sees itself in this state. Other active members of the cluster will see a node in this state if that node was in an active cluster, but is no longer, and is not halted.
- Cluster Reforming. A node in this state is running the protocols which ensure that all nodes agree to the new membership of an active cluster. If agreement is reached, the status database is updated to reflect the new cluster membership.
- Running. A node in this state has completed all required activity for the last re-formation and is operating normally.
- Halted. A node never sees itself in this state. Other nodes will see it in this state after the node has gracefully left the active cluster, for instance with a `cmhaltnode` command.
- Unknown. A node never sees itself in this state. Other nodes assign a node this state if it has never been an active cluster member.

Package Status and State

The *status* of a package can be one of the following:

- Up. The package control script is active.
- Down. The package control script is not active.
- Unknown.

The *state* of the package can be one of the following:

- Starting. The start instructions in the control script are being run.
- Running. Services are active and being monitored.
- Halting. The halt instructions in the control script are being run.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1436
Doc: 3702

17.435

Packages also have the following switching attributes:

- Package Switching. Enabled means that the package can switch to another node in the event of failure.
- Switching Enabled for a Node. Enabled means that the package can switch to the referenced node. Disabled means that the package cannot switch to the specified node until the node is enabled for the package using the `cmmodpkg` command.

  Every package is marked Enabled or Disabled for each node that is either a primary or adoptive node for the package.

Service Status

Services have only status, as follows:

- Up. The service is being monitored.
- Down. The service is not running. It may have halted or failed.
- Unknown.

Network Status

The network interfaces have only status, as follows:

- Up.
- Down.
- Unknown. We cannot determine whether the interface is up or down. This can happen when the cluster is down. A standby interface has this status.

Serial Line Status

The serial line has only status, as follows:

- Up. Heartbeats are received over the serial line.
- Down. Heartbeat has not been received over the serial line within 2 times the NODE_TIMEOUT value.
- Unknown. We cannot determine whether the serial line is up or down. This can happen when the remote node is down.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1437
3702

Examples of Cluster and Package States

The following sample output from the `cmviewcl -v` command shows status for the cluster in the sample configuration.

Normal Running Status. Everything is running normally; both nodes in the cluster are running, and the packages are in their primary locations.

```
CLUSTER       STATUS
example       up
  NODE          STATUS       STATE
  ftsys9        up           running

    Network_Parameters:
    INTERFACE     STATUS       PATH         NAME
    PRIMARY       up           56/36.1      lan0
    STANDBY       up           60/6         lan1

    PACKAGE       STATUS       STATE        PKG_SWITCH    NODE
    pkg1          up           running      enabled       ftsys9

      Script_Parameters:
      ITEM          STATUS       MAX_RESTARTS   RESTARTS        NAME
      Service       up                      0          0        servicel
      Subnet        up                      0          0        15.13.168.0

      Node_Switching_Parameters:
      NODE_TYPE     STATUS       SWITCHING    NAME
      Primary       up           enabled      ftsys9       (current)
      Alternate     up           enabled      ftsys10

NODE          STATUS       STATE
ftsys10       up           running

    Network_Parameters:
    INTERFACE     STATUS       PATH         NAME
    PRIMARY       up           28.1         lan0
    STANDBY       up           32.1         lan1

    PACKAGE       STATUS       STATE        PKG_SWITCH    NODE
    pkg2          up           running      enabled       ftsys10

      Script_Parameters:
      ITEM          STATUS       MAX_RESTARTS   RESTARTS          NAME
      Service       up                      0          0          service2
      Subnet        up                      0          0          15.13.168.0

      Node_Switching_Parameters:
      NODE_TYPE     STATUS       SWITCHING    NAME
      Primary       up           enabled      ftsys10      (current)
      Alternate     up           enabled      ftsys9
```

Status After Halting a Package. After halting pkg2 with the `cmhaltpkg` command, the output of `cmviewcl -v` is as follows:

RQS nº 03/2005 - CN - CPMI - CORREIOS
1438
Fls Nº
3702
Doc:

```
CLUSTER       STATUS
example       up

  NODE          STATUS       STATE
  ftsys9        up           running

    Network_Parameters:
    INTERFACE     STATUS       PATH         NAME
    PRIMARY       up           56/36.1      lan0
    STANDBY       up           60/6         lan1

    PACKAGE       STATUS       STATE        PKG_SWITCH    NODE
    pkg1          up           running      enabled       ftsys9

      Script_Parameters:
      ITEM          STATUS   MAX_RESTARTS    RESTARTS       NAME
      Service       up                  0           0       service1
      Subnet        up                  0           0       15.13.168.0
      Resource      up                                      /example/float

      Node_Switching_Parameters:
      NODE_TYPE     STATUS       SWITCHING     NAME
      Primary       up           enabled       ftsys9       (current)
      Alternate     up           enabled       ftsys10


  NODE          STATUS       STATE
  ftsys10       up           running

    Network_Parameters:
    INTERFACE     STATUS       PATH         NAME
    PRIMARY       up           28.1         lan0
    STANDBY       up           32.1         lan1

UNOWNED_PACKAGES

    PACKAGE       STATUS       STATE        PKG_SWITCH    NODE
    pkg2          down         unowned      disabled      unowned

      Script_Parameters:
      ITEM          STATUS   MAX_RESTARTS    RESTARTS       NAME
      Service       up                  0           0       service1
      Subnet        up                  0           0       15.13.168.0
      Resource      down                                    /example/float

      Node_Switching_Parameters:
      NODE_TYPE     STATUS       SWITCHING     NAME
      Primary       up           enabled       ftsys10
      Alternate     up           enabled       ftsys9
```

Pkg2 now has the status "down", and it is shown as in the unowned state, with package switching disabled. Resource "/example/float," which is configured as a dependency of pkg2, is down. Note that switching is enabled for both nodes, however. This means that once global switching is re-enabled for the package, it will attempt to start up on the primary node.

Status After Moving the Package to Another Node. After issuing the following command:

```
# cmrunpkg -n ftsys9 pkg2
```

the output of the `cmviewcl -v` command is as follows:

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1439
Nº 3702
Doc:

17432


```
CLUSTER      STATUS
example      up

  NODE         STATUS       STATE
  ftsys9       up           running

    Network_Parameters:
    INTERFACE    STATUS       PATH         NAME
    PRIMARY      up           56/36.1      lan0
    STANDBY      up           60/6         lan1

    PACKAGE      STATUS       STATE        PKG_SWITCH   NODE
    pkg1         up           running      enabled      ftsys9

      Script_Parameters:
      ITEM         STATUS   MAX_RESTARTS   RESTARTS      NAME
      Service      up                0          0       service1
      Subnet       up                0          0       15.13.168.0
      Resource     up                                   /example/float

      Node_Switching_Parameters:
      NODE_TYPE    STATUS       SWITCHING    NAME
      Primary      up           enabled      ftsys9       (current)
      Alternate    up           enabled      ftsys10

    PACKAGE      STATUS       STATE        PKG_SWITCH   NODE
    pkg2         up           running      disabled     ftsys9

      Script_Parameters:
      ITEM         STATUS       NAME          MAX_RESTARTS    RESTARTS
      Service      up           service2.1               0           0
      Subnet       up           15.13.168.0              0           0
      Node_Switching_Parameters:
      NODE_TYPE    STATUS       SWITCHING    NAME
      Primary      up           enabled      ftsys10
      Alternate    up           enabled      ftsys9       (current)

  NODE         STATUS       STATE
  ftsys10      up           running

    Network_Parameters:
    INTERFACE    STATUS       PATH         NAME
    PRIMARY      up           28.1         lan0
    STANDBY      up           32.1         lan1
```

Now pkg2 is running on node ftsys9. Note that it is still disabled from switching.

Status After Package Switching is Enabled. The following command changes package status back to Package Switching Enabled:

```
# cmmodpkg -e pkg2
```

The result is now as follows:

```
CLUSTER      STATUS
example      up

  NODE         STATUS       STATE
  ftsys9       up           running

    PACKAGE      STATUS       STATE        PKG_SWITCH   NODE
    pkg1         up           running      enabled      ftsys9
    pkg2         up           running      enabled      ftsys9

  NODE         STATUS       STATE
  ftsys10      up           running
```


RQS nº 03/2005 - CN - CPMI - CORREIOS
1440
Fls Nº
3702
Doc:

Both packages are now running on ftsys9 and pkg2 is enabled for switching. Ftsys10 is running the daemon and no packages are running on ftsys10.

Status After Halting a Node. After halting *ftsys10*, with the following command:

```
# cmhaltnode  ftsys10
```

the output of `cmviewcl` is as follows on *ftsys9*:

```
CLUSTER       STATUS
example       up

  NODE          STATUS       STATE
  ftsys9        up           running

    PACKAGE       STATUS        STATE         PKG_SWITCH    NODE
    pkg1          up            running       enabled       ftsys9
    pkg2          up            running       enabled       ftsys9

  NODE          STATUS       STATE
  ftsys10       down         halted
```

This output is seen on both *ftsys9* and *ftsys10*.

Viewing RS232 Status

If you are using a serial (RS232) line as a heartbeat connection, you will see a list of configured RS232 device files in the output of the `cmviewcl -v` command. The following shows normal running status:

```
CLUSTER       STATUS
example       up
  NODE          STATUS       STATE
  ftsys9        up           running

    Network_Parameters:
    INTERFACE     STATUS       PATH         NAME
    PRIMARY       up           56/36.1      lan0

    Serial_Heartbeat:
    DEVICE_FILE_NAME       STATUS       CONNECTED_TO:
    /dev/tty0p0              up           ftsys10      /dev/tty0p0


  NODE          STATUS       STATE
  ftsys10       up           running

    Network_Parameters:
    INTERFACE     STATUS       PATH         NAME
    PRIMARY       up           28.1         lan0

    Serial_Heartbeat:
    DEVICE_FILE_NAME       STATUS       CONNECTED_TO:
    /dev/tty0p0              up           ftsys9       /dev/tty0p0
```


RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1441
3702
Doc:

The following display shows status after node *ftsys10* has halted:

```
CLUSTER       STATUS
example       up
  NODE          STATUS       STATE
  ftsys9        up           running

    Network_Parameters:
    INTERFACE     STATUS       PATH         NAME
    PRIMARY       up           56/36.1      lan0

    Serial_Heartbeat:
    DEVICE_FILE_NAME       STATUS       CONNECTED_TO:
    /dev/tty0p0            unknown          ftsys10    /dev/tty0p0


  NODE          STATUS       STATE
  ftsys10       down         running

    Network_Parameters:
    INTERFACE     STATUS       PATH         NAME
    PRIMARY       up           28.1         lan0

    Serial_Heartbeat:
    DEVICE_FILE_NAME       STATUS       CONNECTED_TO:
    /dev/tty0p0            unknown          ftsys9     /dev/tty0p0
```

The following shows status when the serial line is not working:

```
CLUSTER       STATUS
example       up
  NODE          STATUS       STATE
  ftsys9        up           running

    Network_Parameters:
    INTERFACE     STATUS       PATH         NAME
    PRIMARY       up           56/36.1      lan0

    Serial_Heartbeat:
    DEVICE_FILE_NAME       STATUS       CONNECTED_TO:
    /dev/tty0p0              down           ftsys10   /dev/tty0p0


  NODE          STATUS       STATE
  ftsys10        up           running

    Network_Parameters:
    INTERFACE     STATUS       PATH         NAME
    PRIMARY       up           28.1         lan0

    Serial_Heartbeat:
    DEVICE_FILE_NAME       STATUS       CONNECTED_TO:
    /dev/tty0p0              down           ftsys9       /dev/tty0p0
```


RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1442
Nº 3702
Doc:

Reviewing Package IP Addresses

The `netstat -in` command can be used to examine the LAN configuration. The command, if executed on *ftsys9* after the halting of node *ftsys10*, shows that the package IP addresses are assigned to lan0 on *ftsys9* along with the heartbeat IP address.

```
Name  Mtu   Network     Address          Ipkts Ierrs   Opkts Oerrs  Coll
ni0*  0     none        none                 0     0       0     0     0
ni1*  0     none        none                 0     0       0     0     0
lo0   4608  127         127.0.0.1        10114     0   10114     0     0
lan0  1500  15.13.168   15.13.171.14    959269     2  305189    47 30538
lan0  1500  15.13.168   15.13.171.23    959269     2  305189    47 30538
lan0  1500  15.13.168   15.13.171.20    959269     2  305189    47 30538
lan1* 1500  none        none            418623    27   41716     3  5149
```

Reviewing the System Log File

Messages from the Cluster Manager and Package Manager are written to the system log file. The default location of the log file is `/var/adm/syslog/syslog.log`. You can use a text editor, such as `vi`, or the `more` command to view the log file for historical information on your cluster.

This log provides information on the following:

- Commands executed and their outcome.
- Major cluster events which may, or may not, be errors.
- Cluster status information.

NOTE Many other products running on HP-UX in addition to MC/ServiceGuard use the syslog.log file to save messages. The *HP-UX System Administration Tasks* manual provides additional information on using the system log.

Sample System Log Entries

The following entries from the file */var/adm/syslog/syslog.log* show a package that failed to run due to a problem in the pkg5_run script. You would look at the pkg5_run.log for details.

```
Dec 14 14:33:48 star04 cmcld[2048]: Starting cluster management protocols.
Dec 14 14:33:48 star04 cmcld[2048]: Attempting to form a new cluster
Dec 14 14:33:53 star04 cmcld[2048]: 3 nodes have formed a new cluster
Dec 14 14:33:53 star04 cmcld[2048]: The new active cluster membership is:
    star04(id=1) , star05(id=2), star06(id=3)
Dec 14 17:33:53 star04 cmlvmd[2049]: Clvmd initialized successfully.
Dec 14 14:34:44 star04 CM-CMD[2054]: cmrunpkg -v pkg5
Dec 14 14:34:44 star04 cmcld[2048]: Request from node star04 to start
```


RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1443
Doc 3702

```
    package pkg5 on node star04.
Dec 14 14:34:44 star04 cmcld[2048]: Executing '/etc/cmcluster/pkg5/pkg5_run
    start' for package pkg5.
Dec 14 14:34:45 star04 LVM[2066]: vgchange -a n /dev/vg02
Dec 14 14:34:45 star04 cmcld[2048]: Package pkg5 run script exited with
    NO_RESTART.
Dec 14 14:34:45 star04 cmcld[2048]: Examine the file
    /etc/cmcluster/pkg5/pkg5_run.log for more details.
```

The following is an example of a successful package starting:

```
Dec 14 14:39:27 star04 CM-CMD[2096]: cmruncl
Dec 14 14:39:27 star04 cmcld[2098]: Starting cluster management protocols.
Dec 14 14:39:27 star04 cmcld[2098]: Attempting to form a new cluster
Dec 14 14:39:27 star04 cmclconfd[2097]: Command execution message
Dec 14 14:39:33 star04 cmcld[2098]: 3 nodes have formed a new cluster
Dec 14 14:39:33 star04 cmcld[2098]: The new active cluster membership is:
   star04(id=1), star05(id=2), star06(id=3)
Dec 14 17:39:33 star04 cmlvmd[2099]: Clvmd initialized successfully.
Dec 14 14:39:34 star04 cmcld[2098]: Executing '/etc/cmcluster/pkg4/pkg4_run
   start' for package pkg4.
Dec 14 14:39:34 star04 LVM[2107]: vgchange /dev/vg01
Dec 14 14:39:35 star04 CM-pkg4[2124]: cmmodnet -a -i 15.13.168.0 15.13.168.4
Dec 14 14:39:36 star04 CM-pkg4[2127]: cmrunserv Service4 /vg01/MyPing 127.0.0.1
    >>/dev/null
Dec 14 14:39:36 star04 cmcld[2098]: Started package pkg4 on node star04.
```

Reviewing Configuration Files

Review the following ASCII configuration files:

- Cluster configuration file.
- Package configuration files.

Ensure that the files are complete and correct according to your configuration planning worksheets.

Reviewing the Package Control Script

Ensure that the package control script is found on all nodes where the package can run and that the file is identical on all nodes. Ensure that the script is executable on all nodes. Ensure that the name of the control script appears in the package configuration file, and ensure that all services named in the package configuration file also appear in the package control script.

Information about the starting and halting of each package is found in the package's control script log. This log provides the history of the operation of the package control script. It is found at `/etc/cmcluster/`*`package_name`*`/`*`control_script`*`.log`. This log

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1444
Doc: 3702

documents all package run and halt activities. If you have written a separate run and halt script script for a package, each script will have its own log.

Using the cmquerycl and cmcheckconf Commands

In addition, cmquerycl and cmcheckconf can be used to troubleshoot your cluster just as they were used to verify its configuration. The following example shows the commands used to verify the existing cluster configuration on *ftsys9* and *ftsys10*:

```
# cmquerycl -v -C /etc/cmcluster/verify.ascii -n ftsys9 -n ftsys10
# cmcheckconf -v -C /etc/cmcluster/verify.ascii
```

The cmcheckconf command checks:

- The network addresses and connections.
- The cluster lock connectivity.
- The validity of configuration parameters of the cluster and packages for:
  - The uniqueness of names.
  - The existence and permission of scripts.

It doesn't check:

- The correct setup of the power circuits.
- The correctness of the package configuration script.

Using the cmscancl Command

The command cmscancl displays information about all the nodes in a cluster in a structured report that allows you to compare such items as IP addresses or subnets, physical volume names for disks, and other node-specific items for all nodes in the cluster. cmscancl actually runs several different HP-UX commands on all nodes and gathers the output into a report on the node where you run the command.

The following are the types of configuration data that cmscancl displays for each node:

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1445
3702

17,426

Table 8-1 Data Displayed by the `cmscancl` Command

Description	Source of Data
LAN device configuration and status	`lanscan` command
network status and interfaces	`netstat` command
file systems	`mount` command
LVM configuration	`/etc/lvmtab` file
LVM physical volume group data	`/etc/lvmpvg` file
link level connectivity for all links	`linkloop` command
binary configuration file	`cmviewconf` command

Using the `cmviewconf` Command

`cmviewconf` allows you to examine the binary cluster configuration file, even when the cluster is not running. The command displays the content of this file on the node where you run the command.

Reviewing the LAN Configuration

The following networking commands can be used to diagnose problems:

- `netstat -in` can be used to examine the LAN configuration. This command lists all IP addresses assigned to each LAN interface card.
- `lanscan` can also be used to examine the LAN configuration. This command lists the MAC addresses and status of all LAN interface cards on the node.
- `arp -a` can be used to check the arp tables.
- `landiag` is useful to display, diagnose, and reset LAN card information.
- `linkloop` verifies the communication between LAN cards at MAC address levels. For example, if you enter

```
# linkloop -i4 0x08000993AB72
```


RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1446
Doc 3702

you should see displayed the following message:

```
Link Connectivity to LAN station: 0x08000993AB72  OK
```

- `cmscancl` can be used to verify that primary and standby LANs are on the same bridged net.
- `cmviewcl -v` shows the status of primary and standby LANs.

Use these commands on all nodes.

ROS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1447
Doc 3702

Solving Problems

Problems with MC/ServiceGuard may be of several types. The following is a list of common categories of problem:

- Cluster Re-formations.
- System Administration Errors.
- Package Control Script Hangs.
- Package Movement Errors.
- Node and Network Failures.

The first two categories of problems occur with the incorrect configuration of MC/ServiceGuard. The last category contains "normal" failures to which MC/ServiceGuard is designed to react and ensure the availability of your applications.

Cluster Re-formations

Cluster re-formations may occur from time to time due to current cluster conditions. Some of the causes are as follows:

- local switch on an Ethernet LAN if the switch takes longer than the cluster `NODE_TIMEOUT` value. To prevent this problem, you can increase the cluster `NODE_TIMEOUT` value, or you can use a different LAN type.
- excessive network traffic on heartbeat LANs. To prevent this, you can use dedicated heartbeat LANs, or LANs with less traffic on them.
- an overloaded system, with too much total I/O and network traffic.
- an improperly configured network, for example, one with a very large routing table.

In these cases, applications continue running, though they might experience a small performance impact during cluster re-formation.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1448
Doc: 3702

System Administration Errors

There are a number of errors you can make when configuring MC/ServiceGuard that will not show up when you start the cluster. Your cluster can be running, and everything appears to be fine, until there is a hardware or software failure and control of your packages are not transferred to another node as you would have expected.

These are errors caused specifically by errors in the cluster configuration file and package configuration scripts. Examples of these errors include:

- Volume groups not defined on adoptive node.
- Mount point does not exist on adoptive node.
- Network errors on adoptive node (configuration errors).
- User information not correct on adoptive node.

You can use the following commands to check the status of your disks:

- `bdf` - to see if your package's volume group is mounted.
- `vgdisplay -v` - to see if all volumes are present.
- `lvdisplay -v` - to see if the mirrors are synchronized.
- `strings /etc/lvmtab` - to ensure that the configuration is correct.
- `ioscan -fnC disk` - to see physical disks.
- `diskinfo -v /dev/rdsk/cxtydz` - to display information about a disk.
- `lssf /dev/dsk/*d0` - to check LV and paths.

Package Control Script Hangs or Failures

When a `RUN_SCRIPT_TIMEOUT` or `HALT_SCRIPT_TIMEOUT` value is set, and the control script hangs, causing the timeout to be exceeded, MC/Serviceguard kills the script and marks the package "Halted." Similarly, when a package control script fails, MC/ServiceGuard kills the script and marks the package "Halted." In both cases, the following also take place:

- Control of the package will not be transferred.
- The run or halt instructions may not run to completion.
- Global switching will be disabled.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
1449
Fls Nº
3702
Doc:

- The current node will be disabled from running the package.

Following such a failure, since the control script is terminated, some of the package's resources may be left activated. Specifically:

- Volume groups may be left active.
- File systems may still be mounted.
- IP addresses may still be installed.
- Services may still be running.

In this kind of situation, MC/Serviceguard will not restart the package without manual intervention. You must clean up manually before restarting the package. Use the following steps as guidelines:

1. Perform application specific cleanup. Any application specific actions the control script might have taken should be undone to ensure successfully starting the package on an alternate node. This might include such things as shutting down application processes, removing lock files, and removing temporary files.
2. Ensure that package IP addresses are removed from the system. This step is accomplished via the `cmmodnet(1m)` command. First determine which package IP addresses are installed by inspecting the output resulting from running the command `netstat -in`. If any of the IP addresses specified in the package control script appear in the netstat output under the "Address" column, use `cmmodnet` to remove them:

   ```
   # cmmodnet -r -i <ip-address> <subnet>
   ```

   where <ip-address> is the address in the "Address" column and <subnet> is the corresponding entry in the "Network" column.
3. Ensure that package volume groups are deactivated. First unmount any package logical volumes which are being used for filesystems. This is determined by inspecting the output resulting from running the command `bdf -l`. If any package logical volumes, as specified by the `LV[]` array variables in the package control script, appear under the "Filesystem" column, use `umount` to unmount them:

   ```
   # fuser -ku <logical-volume>
   # umount <logical-volume>
   ```

   Next, deactivate the package volume groups. These are specified by the `VG[]` array entries in the package control script.

   ```
   # vgchange -a n <volume-group>
   ```


RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1450
3702

17.421

4. Finally, re-enable the package for switching.

   ```
   # cmmodpkg -e <package-name>
   ```

   If after cleaning up the node on which the timeout occured it is desirable to have that node as an alternate for running the package, remember to re-enable the package to run on the node:

   ```
   # cmmodpkg -e -n <node-name> <package-name>
   ```

The default ServiceGuard control scripts are designed to take the straightforward steps needed to get an application running or stopped. If the package administrator specifies a time limit within which these steps need to occur and that limit is subsequently exceeded for any reason, ServiceGuard takes the conservative approach that the control script logic must either be hung or defective in some way. At that point the control script cannot be trusted to perform cleanup actions correctly, thus the script is terminated and the package administrator is given the opportunity to assess what cleanup steps must be taken.

If you want the package to switch automatically in the event of a control script timeout, set the NODE_FAIL_FAST_ENABLED parameter to YES. (If you are using SAM, set *Package Failfast* to *Enabled.*) In this case, ServiceGuard will cause a TOC on the node where the control script timed out. This effectively cleans up any side effects of the package's run or halt attempt. In this case the package will be automatically restarted on any available alternate node for which it is configured.

Package Movement Errors

These errors are similar to the system administration errors except they are caused specifically by errors in the package control script. The best way to prevent these errors is to test your package control script before putting your high availability application on line.

Running your script with the -x shell option will give you details on where your script may be failing.

Node and Network Failures

These failures cause MC/ServiceGuard to transfer control of a package to another node. This is the normal action of MC/ServiceGuard, but you have to be able to recognize when a transfer has taken place and decide to leave the cluster is its current condition or to restore it to its original condition.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls 'Nº 1451
Doc: 3702

Possible node failures can be caused by the following conditions:

- HPMC
- TOC
- Panics
- Hangs
- Power failures

In the event of a TOC, a system dump is performed on the failed node and numerous messages are also displayed on the console.

You can use the following commands to check the status of your network and subnets:

- `netstat -in` - to display LAN status and check to see if the package IP is stacked on the LAN card.
- `lanscan` - to see if the LAN is on the primary interface or has switched to the standby interface.
- `arp -a` - to check the arp tables.
- `landiag` - to display, test, and reset the LAN cards.

Since your cluster is unique, there are no cookbook solutions to possible problems. But if you apply these checks and commands and work your way through the log files, you will be successful in identifying and solving problems.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1452
3702

A MC/ServiceGuard Commands

The following is a list of commands used for MC/ServiceGuard configuration and maintenance. Man pages for these commands are available on your system *after installation*.

ROS nº 03/2005 - CN - CORREIOS
Fls Nº 1453
Doc 3702

man page	description
cmapplyconf	Verify and apply MC/ServiceGuard and MC/LockManager cluster configuration and package configuration files. cmapplyconf verifies the cluster configuration and package configuration specified in the cluster_ascii_file and the associated pkg_ascii_file(s) , creates or updates the binary configuration file, called cmclconfig, and distributes it to all nodes. This binary configuration file contains the cluster configuration information as well as package configuration information for all packages specified. This file, which is used by the cluster daemons to manage the entire cluster and package environment, is kept in the /etc/cmcluster directory. If changes to either the cluster configuration or to any of the package configuration files are needed, first update the appropriate ASCII ile(s) (cluster or package), then validate the changes using the cmcheckconf command and then use cmapplyconf again to verify and redistribute the binary file to all nodes. The cluster and package configuration can be modified whether the cluster is up or down, although some configuration requires either the cluster or the package be halted. Please refer to the manual for more detail. The cluster ASCII file only needs to be specified if configuring the cluster for he first time, or if adding or deleting nodes to the cluster. The package ASCII file only needs to be specified if the package is being added, or if the package configuration is being modified.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1454
Nº 3702
Doc:

man page	description
cmapplyconf (continued)	It is recommended that the user run the cmgetconf command to get either the cluster ASCII configuration file or package ASCII configuration file whenever changes to the existing configuration are required. Note that cmapplyconf will verify and distribute cluster configuration or package files. It will not cause the cluster daemon to start or removed from the cluster configuration. The same kind of processing will apply to the package configuration to determine whether to add or delete package nodes, package subnet, etc. Not all package configuration changes require the package to be halted.
cmcheckconf	Check high availability cluster configuration and/or package configuration files. cmcheckconf verifies the cluster configuration as specified by the cluster_ascii_file and/or the package configuration files specified by each pkg_ascii_file in the command. If the cluster has already been configured previously, the cmcheckconf command will compare the configuration in the cluster_ascii_file against the previously configuration information stored in the binary configuration file and validates the changes. The same rules apply to the pkg_ascii_file. It is not necessary to halt either the cluster or any of the packages to run the cmcheckconf command.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1455
Doc: 3702

man page	description
cmdeleteconf	Delete either the cluster or the package configuration. cmdeleteconf deletes either the entire cluster configuration, including all its packages, or only the specified package configuration. If neither cluster_name nor package_name is specified, cmdeleteconf will delete the local cluster's configuration and all its packages. If only the package_name is specified, the configuration of package_name in the local cluster is deleted. If both cluster_name and package_name are specified, the package must be configured in the cluster_name, and only the package package_name will be deleted. The local cluster is the cluster that the node running the cmdeleteconf command belongs to.
cmgetconf	Get cluster or package configuration information. Cmgetconf obtains either the cluster configuration, not including the package configuration, or the specified package's configuration information, and writes to either the output_filename file, or to stdout. This command can be run whether the cluster is up or down. If neither cluster_name nor package_name is specified, cmgetconf will obtain the local cluster's configuration. If both cluster_name and package_name are specified, the package must be configured in the cluster_name, and only the package configuration for package_name will be written to output_filename or to stdout.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1456
Nº Doc: 3702

17.415

man page	description
cmhaltcl	Halt a high availability cluster. cmhaltcl causes all nodes in a configured cluster to stop their cluster daemons, optionally halting all packages or applications in the process. This command will halt all the daemons on all currently running systems. If the user only wants to shutdown a subset of daemons, the cmhaltnode command should be used instead.
cmhaltnode	Halt a node in a high availability cluster. cmhaltnode causes a node to halt its cluster daemon and remove itself from the existing cluster. When cmhaltnode is run on a node, the cluster daemon is halted and, optionally, all packages that were running on that node are moved to other nodes if possible.
cmhaltpkg	Halt a high availability package. cmhaltpkg performs a manual halt of high availability package(s) running on MC/ServiceGuard or MC/LockManager clusters. This command may be run on any node within the cluster and may operate on any package within the cluster.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1457
Doc: 3702

3413

man page	description
cmmodpkg	Enable or disable switching attributes for a high availability package. cmmodpkg enables or disables the ability of a package to switch to another node upon failure of the package, and it enables or disables a particular node from running specific packages.Switching for a package can be enabled or disabled globally. For example, if a globally disabled package fails, it will not switch to any other node, and if a globally enabled package fails, it will attempt to switch to the first available node on which it is configured to run.
cmquerycl	Query cluster or node configuration information. cmquerycl searches all specified nodes for cluster configuration and Logical Volume Manager (LVM) information. Cluster configuration information includes network information such as LAN interface, IP addresses, bridged networks and possible heartbeat networks. LVM information includes volume group (VG) interconnection and file systemmount point information. This command should be run as the first step in preparing for cluster configuration. It may also be used as a troubleshooting tool to identify the current configuration of a cluster.
cmruncl	Run a high availability cluster. cmruncl causes all nodes in a configured cluster or all nodes specified to start their cluster daemons and form a new cluster.This command should only be run when the cluster is not active on any of the configured nodes. If a cluster is already running on a subset of the nodes, the cmrunnode command should be used to start the remaining nodes and force them to join the existing cluster.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls_Nº 1458
Nº 3702 Doc:

man page	description
cmrunnode	Run a node in a high availability cluster. cmrunnode causes a node to start its cluster daemon to join the existing cluster. Starting a node will not cause any active packages to be moved to the new node. However, if a package is DOWN, has its switching enabled, and is able to run on the new node, that package will automatically run there.
cmrunpkg	Run a high availability package. cmrunpkg runs a high availability package(s) that was previously halted.This command may be run on any node within the cluster and may operate on any package within the cluster. If a node is not specified, the node on which the command is run will be used. This will result in an error if the current node is not able to run the package or is not in the list of possible owners of the package. When a package is started on a new node, the package's run script is executed.

RQS nº 03/2005 - CN - CPMI - CORREIOS
1459
Fls Nº
3702

17.419

man page	description
cmscancl	Gather system configuration information from nodes with MC/ServiceGuard or MC/LockManager installed. cmscancl is a configuration report and diagnostic tool which gathers system software and hardware configuration information from a list of nodes, or from all the nodes in a cluster. The information that this command displays includes LAN device configuration, network status and interfaces, file systems, LVM configuration, link-level connectivity, and the data from the binary cluster configuration file. This command can be used as a troubleshooting tool or as a data collection tool.
cmviewcl	View information about the current high availability cluster. cmviewcl displays the current status information of a cluster. Output can be displayed for the whole cluster or it may be limited to particular nodes or packages.
cmviewconf	View MC/ServiceGuard or MC/LockManager cluster configuration information. cmviewconf collects and displays the cluster configuration information, in ASCII format, from the binary configuration file for an existing cluster. Optionally, the output can be written to a file. This command can be used as a troubleshooting tool to identify the configuration of a cluster.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1460
3702

B Enterprise Cluster Master Toolkit

The Enterprise Cluster Master Toolkit (HP Product Number B5121) provides a group of example scripts and package configuration files for creating MC/ServiceGuard packages for several major database and internet software products. Each toolkit contains a README file that explains how to customize the package for your needs.

Toolkits are included for the following HP Domain server components:

- FastTrack Server
- Enterprise Server
- Enterprise Server Pro
- Proxy Server
- Directory Server
- Messaging Server
- Collabra Server
- Calendar Server

Toolkits are included for the following database products:

- Informix
- Oracle
- Progress
- Sybase

A separate NFS toolkit is available. Refer to *Managing Highly Available NFS* (HP Part Number B5125-90001) for more information.

Numerous other application integration scripts are available from your HP representative.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1461
3702

RQS nº 03/2005 - CN
CPMI - CORREIOS
1462
Fls Nº
3702

17409

C Designing Highly Available Cluster Applications

This appendix describes how to create or port applications for high availability, with emphasis on the following topics:

- Automating Application Operation
- Controlling the Speed of Application Failover
- Designing Applications to Run on Multiple Systems
- Restoring Client Connections
- Handling Application Failures
- Minimizing Planned Downtime

Designing for high availability means reducing the amount of unplanned and planned downtime that users will experience. Unplanned downtime includes unscheduled events such as power outages, system failures, network failures, disk crashes, or application failures. Planned downtime includes scheduled events such as scheduled backups, system upgrades to new OS revisions, or hardware replacements.

Two key strategies should be kept in mind:

1. Design the application to handle a system reboot or panic. If you are modifying an existing application for a highly available environment, determine what happens currently with the application after a system panic. In a highly available environment there should be defined (and scripted) procedures for restarting the application. Procedures for starting and stopping the application should be automatic, with no user intervention required.
2. The application should not use any system-specific information such as the following if such use would prevent it from failing over to another system and running properly:
   - The application should not refer to `uname()` or `gethostname()`.
   - The application should not refer to the SPU ID.
   - The application should not refer to the MAC (link-level) address.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1463
3702

Fl. 408

Automating Application Operation

Can the application be started and stopped automatically or does it require operator intervention?

This section describes how to automate application operations to avoid the need for user intervention. One of the first rules of high availability is to avoid manual intervention. If it takes a user at a terminal, console or GUI interface to enter commands to bring up a subsystem, the user becomes a key part of the system. It may take hours before a user can get to a system console to do the work necessary. The hardware in question may be located in a far-off area where no trained users are available, the systems may be located in a secure datacenter, or in off hours someone may have to connect via modem.

There are two principles to keep in mind for automating application relocation:

- Insulate users from outages.
- Applications must have defined startup and shutdown procedures.

You need to be aware of what happens currently when the system your application is running on is rebooted, and whether changes need to be made in the application's response for high availability.

Insulate Users from Outages

Wherever possible, insulate your end users from outages. Issues include the following:

- Do not require user intervention to reconnect when a connection is lost due to a failed server.
- Where possible, warn users of slight delays due to a failover in progress.
- Minimize the reentry of data.
- Engineer the system for reserve capacity to minimize the performance degradation experienced by users.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1464
Doc. 3702

17.407

Define Application Startup and Shutdown

Applications must be restartable without manual intervention. If the application requires a switch to be flipped on a piece of hardware, then automated restart is impossible. Procedures for application startup, shutdown and monitoring must be created so that the HA software can perform these functions automatically.

To ensure automated response, there should be defined procedures for starting up the application and stopping the application. In MC/ServiceGuard these procedures are placed in the package control script. These procedures must check for errors and return status to the HA control software. The startup and shutdown should be command-line driven and not interactive unless all of the answers can be predetermined and scripted.

In an HA failover environment, HA software restarts the application on a surviving system in the cluster that has the necessary resources, like access to the necessary disk drives. The application must be restartable in two aspects:

- It must be able to restart and recover on the backup system (or on the same system if the application restart option is chosen).
- It must be able to restart if it fails during the startup and the cause of the failure is resolved.

Application administrators need to learn to startup and shutdown applications using the appropriate HA commands. Inadvertently shutting down the application directly will initiate an unwanted failover. Application administrators also need to be careful that they don't accidently shut down a production instance of an application rather than a test instance in a development environment.

A mechanism to monitor whether the application is active is necessary so that the HA software knows when the application has failed. This may be as simple as a script that issues the command `ps -ef | grep xxx` for all the processes belonging to the application.

To reduce the impact on users, the application should not simply abort in case of error, since aborting would cause an unneeded failover to a backup system. Applications should determine the exact error and take specific action to recover from the error rather than, for example, aborting upon receipt of any error.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1465
3702

17.406

Controlling the Speed of Application Failover

What steps can be taken to ensure the fastest failover?

If a failure does occur causing the application to be moved (failed over) to another node, there are many things the application can do to reduce the amount of time it takes to get the application back up and running. The topics covered are as follows:

- Replicate Non-Data File Systems
- Use Raw Volumes
- Evaluate the Use of JFS
- Minimize Data Loss
- Use Restartable Transactions
- Use Checkpoints
- Design for Multiple Servers
- Design for Replicated Data Sites

Replicate Non-Data File Systems

Non-data file systems should be replicated rather than shared. There can only be one copy of the application data itself. It will be located on a set of disks that is accessed by the system that is running the application. After failover, if these data disks are filesystems, they must go through filesystems recovery (`fsck`) before the data can be accessed. To help reduce this recovery time, the smaller these filesystems are, the faster the recovery will be. Therefore, it is best to keep anything that can be replicated off the data filesystem. For example, there should be a copy of the application executables on each system rather than having one copy of the executables on a shared filesystem. Additionally, replicating the application executables makes them subject to a rolling upgrade if this is desired.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1466
3702
Doc:

Use Raw Volumes

If your application uses data, use raw volumes rather than filesystems. Raw volumes do not require an `fsck` of the filesystem, thus eliminating one of the potentially lengthy steps during a failover.

Evaluate the Use of JFS

If a file system must be used, a JFS offers significantly faster file system recovery as compared to an HFS. However, performance of the JFS may vary with the application.

Minimize Data Loss

Minimize the amount of data that might be lost at the time of an unplanned outage. It is impossible to prevent some data from being lost when a failure occurs. However, it is advisable to take certain actions to minimize the amount of data that will be lost, as explained in the following discussion.

Minimize the Use and Amount of Memory-Based Data

Any in-memory data (the in-memory context) will be lost when a failure occurs. The application should be designed to minimize the amount of in-memory data that exists unless this data can be easily recalculated. When the application restarts on the standby node, it must recalculate or reread from disk any information it needs to have in memory.

One way to measure the speed of failover is to calculate how long it takes the application to start up on a normal system after a reboot. Does the application start up immediately? Or are there a number of steps the application must go through before an end-user can connect to it? Ideally, the application can start up quickly without having to reinitialize in-memory data structures or tables.

Performance concerns might dictate that data be kept in memory rather than written to the disk. However, the risk associated with the loss of this data should be weighed against the performance impact of posting the data to the disk.

Data that is read from a shared disk into memory, and then used as read-only data can be kept in memory without concern.

RQS nº 03/2005 - CN - CPMI - CORREIOS
1467
Fls Nº
3702
Doc:

17404

Keep Logs Small

Some databases permit logs to be buffered in memory to increase online performance. Of course, when a failure occurs, any in-flight transaction will be lost. However, minimizing the size of this in-memory log will reduce the amount of completed transaction data that would be lost in case of failure.

Keeping the size of the on-disk log small allows the log to be archived or replicated more frequently, reducing the risk of data loss if a disaster were to occur. There is, of course, a trade-off between online performance and the size of the log.

Eliminate Need for Local Data

When possible, eliminate the need for local data. In a three-tier, client/server environment, the middle tier can often be dataless (i.e., there is no local data that is client specific or needs to be modified). This "application server" tier can then provide additional levels of availability, load-balancing, and failover. However, this scenario requires that all data be stored either on the client (tier 1) or on the database server (tier 3).

Use Restartable Transactions

Transactions need to be restartable so that the client does not need to re-enter or back out of the transaction when a server fails, and the application is restarted on another system. In other words, if a failure occurs in the middle of a transaction, there should be no need to start over again from the beginning. This capability makes the application more robust and reduces the visibility of a failover to the user.

A common example is a print job. Printer applications typically schedule jobs. When that job completes, the scheduler goes on to the next job. If, however, the system dies in the middle of a long job (say it is printing paychecks for 3 hours), what happens when the system comes back up again? Does the job restart from the beginning, reprinting all the paychecks, does the job start from where it left off, or does the scheduler assume that the job was done and not print the last hours worth of paychecks? The correct behavior in a highly available environment is to restart where it left off, ensuring that everyone gets one and only one paycheck.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1468
3702
Doc:

17403

Another example is an application where a clerk is entering data about a new employee. Suppose this application requires that employee numbers be unique, and that after the name and number of the new employee is entered, a failure occurs. Since the employee number had been entered before the failure, does the application refuse to allow it to be re-entered? Does it require that the partially entered information be deleted first? More appropriately, in a highly available environment the application will allow the clerk to easily restart the entry or to continue at the next data item.

Use Checkpoints

Design applications to checkpoint complex transactions. A single transaction from the user's perspective may result in several actual database transactions. Although this issue is related to restartable transactions, here it is advisable to record progress locally on the client so that a transaction that was interrupted by a system failure can be completed after the failover occurs.

For example, suppose the application being used is calculating PI. On the original system, the application has gotten to the 1,000th decimal point, but the application has not yet written anything to disk. At that moment in time, the node crashes. The application is restarted on the second node, but the application is started up from scratch. The application must recalculate those 1,000 decimal points. However, if the application had written to disk the decimal points on a regular basis, the application could have restarted from where it left off.

Balance Checkpoint Frequency with Performance

It is important to balance checkpoint frequency with performance. The trade-off with checkpointing to disk is the impact of this checkpointing on performance. Obviously if you checkpoint too often the application slows; if you don't checkpoint often enough, it will take longer to get the application back to its current state after a failover. Ideally, the end-user should be able to decide how often to checkpoint. Applications should provide customizable parameters so the end-user can tune the checkpoint frequency.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1469
Doc: 3702

17.402

Design for Multiple Servers

If you use multiple active servers, multiple service points can provide relatively transparent service to a client. However, this capability requires that the client be smart enough to have knowledge about the multiple servers and the priority for addressing them. It also requires access to the data of the failed server or replicated data.

For example, rather than having a single application which fails over to a second system, consider having both systems running the application. After a failure of the first system, the second system simply takes over the load of the first system. This eliminates the start up time of the application. There are many ways to design this sort of architecture, and there are also many issues with this sort of design. This discussion will not go into details other than to give a few examples.

The simplest method is to have two applications running in a master/slave relationship where the slave is simply a hot standby application for the master. When the master fails, the slave on the second system would still need to figure out what state the data was in (i.e., data recovery would still take place). However, the time to fork the application and do the initial startup is saved.

Another possibility is having two applications that are both active. An example might be two application servers which feed a database. Half of the clients connect to one application server and half of the clients connect to the second application server. If one server fails, then all the clients connect to the remaining application server.

Design for Replicated Data Sites

Replicated data sites are a benefit for both fast failover and disaster recovery. With replicated data, data disks are *not* shared between systems. There is no data recovery that has to take place. This makes the recovery time faster. However, there may be performance trade-offs associated with replicating data. There are a number of ways to perform data replication, which should be fully investigated by the application designer.

Many of the standard database products provide for data replication transparent to the client application. By designing your application to use a standard database, the end-user can determine if data replication is desired.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1470
Nº 3702
Doc:

17. 403

Designing Applications to Run on Multiple Systems

If an application can be failed to a backup node, how will it work on that different system?

The previous sections discussed methods to ensure that an application can be automatically restarted. This section will discuss some ways to ensure the application can run on multiple systems. Topics are as follows:

- Avoid Node Specific Information
- Assign Unique Names to Applications
- Use `Uname(2)` With Care
- Bind to a Fixed Port
- Bind to a Relocatable IP Addresses
- Give Each Application its Own Volume Group
- Use Multiple Destinations for SNA Applications
- Avoid File Locking

Avoid Node Specific Information

Typically, when a new system is installed, an IP address must be assigned to each active network interface. This IP address is always associated with the node and is called a **stationary** IP address.

The use of packages containing highly available applications adds the requirement for an additional set of IP addresses, which are assigned to the applications themselves. These are known as **relocatable** application IP addresses. MC/ServiceGuard's network sensor monitors the node's access to the subnet on which these relocatable application IP addresses reside. When packages are configured in MC/ServiceGuard, the associated subnetwork address is specified as a package dependency, and a list of nodes on which the package can run is also provided. When failing a package over to a remote node, the subnetwork must already be active on the target node.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1471
3702

17. 400

Each application or package should be given a unique name as well as a relocatable IP address. Following this rule separates the application from the system on which it runs, thus removing the need for user knowledge of which system the application runs on. It also makes it easier to move the application among different systems in a cluster for for load balancing or other reasons. If two applications share a single IP address, they must move together. Instead, using independent names and addresses allows them to move separately.

For external access to the cluster, clients must know how to refer to the application. One option is to tell the client which relocatable IP address is associated with the application. Another option is to think of the application name as a host, and configure a name-to-address mapping in the Domain Name System (DNS). In either case, the client will ultimately be communicating via the application's relocatable IP address. If the application moves to another node, the IP address will move with it, allowing the client to use the application without knowing its current location. Remember that each network interface must have a stationary IP address associated with it. This IP address does *not* move to a remote system in the event of a network failure.

Obtain Enough IP Addresses

Each application receives a *relocatable* IP address that is separate from the stationary IP address assigned to the system itself. Therefore, a single system might have many IP addresses, one for itself and one for each of the applications that it normally runs. Therefore, IP addresses in a given subnet range will be consumed faster than without high availablity. It might be necessary to acquire additional IP addresses.

Multiple IP addresses on the same network interface are supported only if they are on the same subnetwork.

Allow Multiple Instances on Same System

Applications should be written so that multiple instances, each with its own application name and IP address, can run on a single system. It might be necessary to invoke the application with a parameter showing which instance is running. This allows distributing the users among several systems under normal circumstances, but it also allows all of the users to be serviced in the case of a failure on a single system.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1472
3702
Doc:

17.399

Avoid Using SPU IDs or MAC Addresses

Design the application so that it does not rely on the SPU ID or MAC (link-level) addresses. The SPU ID is a unique hardware ID contained in non-volatile memory, which cannot be changed. A MAC address (also known as a LANIC id) is a link-specific address associated with the LAN hardware. The use of these addresses is a common problem for license servers, since for security reasons they want to use hardware-specific identification to ensure the license isn't copied to multiple nodes. One workaround is to have multiple licenses; one for each node the application will run on. Another way is to have a cluster-wide mechanism that lists a set of SPU IDs or node names. If your application is running on a system in the specified set, then the license is approved.

Previous generation HA software would move the MAC address of the network card along with the IP address when services were moved to a backup system. This is no longer allowed in MC/ServiceGuard.

There were a couple of reasons for using a MAC address, which have been addressed below:

- Old network devices between the source and the destination such as routers had to be manually programmed with MAC and IP address pairs. The solution to this problem is to move the MAC address along with the IP address in case of failover.
- Up to 20 minute delays could occur while network device caches were updated due to timeouts associated with systems going down. This is dealt with in current HA software by broadcasting a new ARP translation of the old IP address with the new MAC address.

Assign Unique Names to Applications

A unique name should be assigned to each application. This name should then be configured in DNS so that the name can be used as input to `gethostbyname()`, as described in the following discussion.

Use DNS

DNS provides an API which can be used to map hostnames to IP addresses and vice versa. This is useful for BSD socket applications such as telnet which are first told the target system name. The application must then map the name to an IP address in order to establish a connection. However, some calls should be used with caution.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1473
3702

17.398
3

Applications should *not* reference official hostnames or IP addresses. The official hostname and corresponding IP address for the hostname refer to the primary LAN card and the *stationary IP address* for that card. Therefore, any application that refers to, or requires the hostname or primary IP address may not work in an HA environment where the network identity of the system that supports a given application moves from one system to another, but the hostname does not move.

One way to look for problems in this area is to look for calls to `gethostname(2)` in the application. HA services should use `gethostname()` with caution, since the response may change over time if the application migrates. Applications that use `gethostname()` to determine the name for a call to `gethostbyname(2)` should also be avoided for the same reason. Also, the `gethostbyaddr()` call may return different answers over time if called with a relocatable IP addresses.

Instead, the application should always refer to the application name and relocatable IP address rather than the hostname and stationary IP address. It is appropriate for the application to call `gethostbyname(2)`, specifying the application name rather than the hostname. `gethostbyname(2)` will pass in the IP address of the application. This IP address will move with the application to the new node.

However, `gethostbyname(2)` should be used to locate the IP address of an application only if the application name is configured in DNS. It is probably best to associate a different application name with each independent HA service. This allows each application and its IP address to be moved to another node without affecting other applications. Only the stationary IP addresses should be associated with the hostname in DNS.

Use uname(2) With Care

Related to the hostname issue discussed in the previous section is the application's use of `uname(2)`, which returns the official system name. The system name is unique to a given system whatever the number of LAN cards in the system. By convention, the `uname` and `hostname` are the same, but they do not have to be. Some applications, after connection to a system, might call `uname(2)` to validate for security purposes that they are really on the correct system. This is not appropriate in an HA environment, since the service is moved from one system to another, and neither the `uname` nor the `hostname` are moved. Applications should

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1474
Doc: 3702

17.397

develop alternate means of verifying where they are running. For example, an application might check a list of hostnames that have been provided in a configuration file.

Bind to a Fixed Port

When binding a socket, a port address can be specified or one can be assigned dynamically. One issue with binding to random ports is that a different port may be assigned if the application is later restarted on another cluster node. This may be confusing to clients accessing the application.

The recommended method is using fixed ports that are the same on all nodes where the application will run, instead of assigning port numbers dynamically. The application will then always return the same port number regardless of which node is currently running the application. Application port assignments should be put in `/etc/services` to keep track of them and to help ensure that someone will not choose the same port number.

Bind to Relocatable IP Addresses

When sockets are bound, an IP address is specified in addition to the port number. This indicates the IP address to use for communication and is meant to allow applications to limit which interfaces can communicate with clients. An application can bind to INADDR_ANY as an indication that messages can arrive on any interface.

Network applications can bind to a stationary IP address, a relocatable IP address, or INADDR_ANY. If the stationary IP address is specified, then the application may fail when restarted on another node, because the stationary IP address is not moved to the new system. If an application binds to the relocatable IP address, then the application will behave correctly when moved to another system.

Many server-style applications will bind to INADDR_ANY, meaning that they will receive requests on any interface. This allows clients to send to the stationary or relocatable IP addresses. However, in this case the networking code cannot determine which source IP address is most appropriate for responses, so it will always pick the stationary IP address.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1475
Nº Doc: 3702

17.396

For TCP stream sockets, the TCP level of the protocol stack resolves this problem for the client since it is a connection-based protocol. On the client, TCP ignores the stationary IP address and continues to use the previously bound relocatable IP address originally used by the client.

With UDP datagram sockets, however, there is a problem. The client may connect to multiple servers utilizing the relocatable IP address and sort out the replies based on the source IP address in the server's response message. However, the source IP address given in this response will be the stationary IP address rather than the relocatable application IP address. Therefore, when creating a UDP socket for listening, the application must always call `bind(2)` with the appropriate relocatable application IP address rather than `INADDR_ANY`.

If the application cannot be modified as recommended above, a workaround to this problem is to not use the stationary IP address at all, and only use a single relocatable application IP address on a given LAN card. Limitations with this workaround are as follows:

- Local LAN failover will not work.
- There has to be an idle LAN card on each backup node that is used to relocate the relocatable application IP address in case of a failure.

Call bind() before connect()

When an application initiates its own connection, it should first call `bind(2)`, specifying the application IP address before calling `connect(2)`. Otherwise the connect request will be sent using the stationary IP address of the system's outbound LAN interface rather than the desired relocatable application IP address. The client will receive this IP address from the `accept(2)` call, possibly confusing the client software and preventing it from working correctly.

Give Each Application its Own Volume Group

Use separate volume groups for each application that uses data. If the application doesn't use disk, it is not necessary to assign it a separate volume group. A volume group (group of disks) is the unit of storage that can move between nodes. The greatest flexibility for load balancing exists when each application is confined to its own volume group, i.e., two applications do not share the same set of disk drives. If two applications do use the same volume group to store their data, then the

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1476
Nº Doc: 3702

17. 395

applications must move together. If the applications' data stores are in separate volume groups, they can switch to different nodes in the event of a failover.

The application data should be set up on different disk drives and if applicable, different mount points. The application should be designed to allow for different disks and separate mount points. If possible, the application should not assume a specific mount point.

To prevent one node from inadvertently accessing disks being used by the application on another node, HA software uses an exclusive access mechanism to enforce access by only one node at a time. This exclusive access applies to a volume group as a whole.

Use Multiple Destinations for SNA Applications

SNA is point-to-point link-oriented; that is, the *services* cannot simply be moved to another system, since that system has a different point-to-point link which originates in the mainframe. Therefore, backup links in a node and/or backup links in other nodes should be configured so that SNA does not become a single point of failure. Note that only one configuration for an SNA link can be active at a time. Therefore, backup links that are used for other purposes should be reconfigured for the primary mission-critical purpose upon failover.

Avoid File Locking

In an NFS environment, applications should avoid using file-locking mechanisms, where the file to be locked is on an NFS Server. File locking should be avoided in an application both on local and remote systems. If local file locking is employed and the system fails, the system acting as the backup system will not have any knowledge of the locks maintained by the failed system. This may or may not cause problems when the application restarts.

Remote file locking is the worst of the two situations, since the system doing the locking may be the system that fails. Then, the lock might never be released, and other parts of the application will be unable to access that data. In an NFS environment, file locking can cause long delays in case of NFS client system failure and might even delay the failover itself.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1477
Doc 3702

Restoring Client Connections

How does a client reconnect to the server after a failure?

It is important to write client applications to specifically differentiate between the loss of a connection to the server and other application-oriented errors that might be returned. The application should take special action in case of connection loss.

One question to consider is how a client knows after a failure when to reconnect to the newly started server. The typical scenario is that the client must simply restart their session, or relog in. However, this method is not very automated. For example, a well-tuned hardware and application system may fail over in 5 minutes. But if users, after experiencing no response during the failure, give up after 2 minutes and go for coffee and don't come back for 28 minutes, the perceived downtime is actually 30 minutes, not 5. Factors to consider are the number of reconnection attempts to make, the frequency of reconnection attempts, and whether or not to notify the user of connection loss.

There are a number of strategies to use for client reconnection:

- Design clients which continue to try to reconnect to their failed server.

  Put the work into the client application rather than relying on the user to reconnect. If the server is back up and running in 5 minutes, and the client is continually retrying, then after 5 minutes, the client application will reestablish the link with the server and either restart or continue the transaction. No intervention from the user is required.

- Design clients to reconnect to a *different* server.

  If you have a server design which includes multiple active servers, the client could connect to the second server, and the user would only experience a brief delay.

  The problem with this design is knowing when the client should switch to the second server. How long does a client retry to the first server before giving up and going to the second server? There are no definitive answers for this. The answer depends on the design of the server application. If the application can be restarted on the same node after a failure (see "Handling Application Failures" following),

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1478
Doc 3702

17.393

the retry to the current server should continue for the amount of time it takes to restart the server locally. This will keep the client from having to switch to the second server in the event of a application failure.

- Use a transaction processing monitor or message queueing software to increase robustness.

  Use transaction processing monitors such as Tuxedo or DCE/Encina, which provide an interface between the server and the client. Transaction processing monitors (TPMs) can be useful in creating a more highly available application. Transactions can be queued such that the client does not detect a server failure. Many TPMs provide for the optional automatic rerouting to alternate servers or for the automatic retry of a transaction. TPMs also provide for ensuring the reliable completion of transactions, although they are not the only mechanism for doing this. After the server is back online, the transaction monitor reconnects to the new server and continues routing it the transactions.

- Queue Up Requests

  As an alternative to using a TPM, queue up requests when the server is unavailable. Rather than notifying the user when a server is unavailable, the user request is queued up and transmitted later when the server becomes available again. Message queueing software ensures that messages of any kind, not necessarily just transactions, are delivered and acknowledged.

  Message queueing is useful only when the user does not need or expect response that the request has been completed (i.e, the application is not interactive).

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1479
Doc: 3702

17.392

Handling Application Failures

What happens if part or all of an application fails?

All of the preceding sections have assumed the failure in question was not a failure of the application, but of another component of the cluster. This section deals specifically with application problems. For instance, software bugs may cause an application to fail or system resource issues (such as low swap/memory space) may cause an application to die. The section deals with how to design your application to recover after these types of failures.

Create Applications to be Failure Tolerant

An application should be tolerant of failures in a single component. Many applications have multiple processes running on a single node. If one process fails, what happens to the other processes? Do they also fail? Can the failed process be restarted on the same node without affecting the remaining pieces of the application?

Ideally, if one process fails, the other processes can wait a period of time for that component to come back online. This is true whether the component is on the same system or a remote system. The failed component can be restarted automatically on the same system and rejoin the waiting processing and continue on. This type of failure can be detected and restarted within a few seconds, so the end user would never know a failure occurred.

Another alternative is for the failure of one component to still allow bringing down the other components cleanly. If a database SQL server fails, the database should still be able to be brought down cleanly so that no database recovery is necessary.

The worse case is for a failure of one component to cause the entire system to fail. If one component fails and all other components need to be restarted, the downtime will be high.

Be Able to Monitor Applications

All components in a system, including applications, should be able to be monitored for their health. A monitor might be as simple as a display command or as complicated as a SQL query. There must be a way to

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1480
Nº Doc. 3702

17.391

ensure that the application is behaving correctly. If the application fails and it is not detected automatically, it might take hours for a user to determine the cause of the downtime and recover from it.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1481
Nº Doc 3702

17390

Minimizing Planned Downtime

Planned downtime (as opposed to unplanned downtime) is scheduled; examples include backups, systems upgrades to new operating system revisions, or hardware replacements. For planned downtime, application designers should consider:

- **Reducing the time needed for application upgrades/patches.**

  Can an administrator install a new version of the application without scheduling downtime? Can different revisions of an application operate within a system? Can different revisions of a client and server operate within a system?

- **Providing for online application reconfiguration.**

  Can the configuration information used by the application be changed without bringing down the application?

- **Documenting maintenance operations.**

  Does an operator know how to handle maintenance operations?

When discussing highly available systems, unplanned failures are often the main point of discussion. However, if it takes 2 weeks to upgrade a system to a new revision of software, there are bound to be a large number of complaints.

The following sections discuss ways of handling the different types of planned downtime.

Reducing Time Needed for Application Upgrades and Patches

Once a year or so, a new revision of an application is released. How long does it take for the end-user to upgrade to this new revision? This answer is the amount of planned downtime a user must take to upgrade their application. The following guidelines reduce this time.

Provide for Rolling Upgrades

Provide for a "rolling upgrade" in a client/server environment. For a system with many components, the typical scenario is to bring down the entire system, upgrade every node to the new version of the software,

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1482
3702
Doc:

17.384

and then restart the application on all the affected nodes. For large systems, this could result in a long downtime. An alternative is to provide for a rolling upgrade. A rolling upgrade rolls out the new software in a phased approach by upgrading only one component at a time. For example, the database server is upgraded on Monday, causing a 15 minute downtime. Then on Tuesday, the application server on two of the nodes is upgraded, which leaves the application servers on the remaining nodes online and causes no downtime. On Wednesday, two more application servers are upgraded, and so on. With this approach, you avoid the problem where everything changes at once, plus you minimize long outages.

The trade-off is that the application software must operate with different revisions of the software. In the above example, the database server might be at revision 5.0 while the some of the application servers are at revision 4.0. The application must be designed to handle this type of situation.

Do Not Change the Data Layout Between Releases

Migration of the data to a new format can be very time intensive. It also almost guarantees that rolling upgrade will not be possible. For example, if a database is running on the first node, ideally, the second node could be upgraded to the new revision of the database. When that upgrade is completed, a brief downtime could be scheduled to move the database server from the first node to the newly upgraded second node. The database server would then be restarted, while the first node is idle and ready to be upgraded itself. However, if the new database revision requires a different database layout, the *old* data will not be readable by the newly updated database. The downtime will be longer as the data is migrated to the new layout.

Providing Online Application Reconfiguration

Most applications have some sort of configuration information that is read when the application is started. If to make a change to the configuration, the application must be halted and a new configuration file read, downtime is incurred.

To avoid this downtime use configuration tools that interact with an application and make dynamic changes online. The ideal solution is to have a configuration tool which interacts with an application. Changes

REG Nº 03/2005 CPMI - CORREIOS
Fls Nº 1483
Nº 3702
Doc

17.385

are made online with little or no interruption to the end-user. This tool must be able to do everything online, such as expanding the size of the data, adding new users to the system, adding new users to the application, etc. Every task that an administrator needs to do to the application system can be made available online.

Documenting Maintenance Operations

Standard procedures are important. An application designer should make every effort to make tasks common for both the highly available environment and the normal environment. If an administrator is accustomed to bringing down the entire system after a failure, he or she will continue to do so even if the application has been redesigned to handle a single failure. It is important that application documentation discuss alternatives with regards to high availability for typical maintenance operations.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1484
Nº 3702
Doc:

17.387

D Integrating HA Applications with MC/ServiceGuard

The following is a summary of the steps you should follow to integrate an application into the MC/ServiceGuard environment:

1. Read the rest of this book, including the chapters on cluster and package configuration, and the appendix "Designing Highly Available Cluster Applications."
2. Define the cluster's behavior for normal operations:
   - What should the cluster look like during normal operation?
   - What is the standard configuration most people will use? (Is there any data available about user requirements?)
   - Can you separate out functions such as database or application server onto separate machines, or does everything run on one machine?
3. Define the cluster's behavior for failover operations:
   - Does everything fail over together to the adoptive node?
   - Can separate applications fail over to the same node?
   - Is there already a high availability mechanism within the application other than the features provided by MC/ServiceGuard?
4. Identify problem areas
   - What does the application do today to handle a system reboot or panic?
   - Does the application use any system-specific information such as uname() or gethostname(), SPU_ID or MAC address which would prevent it from failing over to another system?

RQS nº 03/2005 - CN - CPMI - CORREIOS
1485
Fls Nº
3702

17. 386

Checklist for Integrating HA Applications

This section contains a checklist for integrating HA applications in both single and multiple systems.

Defining Baseline Application Behavior on a Single System

1. Define a baseline behavior for the application on a standalone system:
   - Install the application, database, and other required resources on one of the systems. Be sure to follow MC/ServiceGuard rules in doing this:
     - Install all shared data on separate external volume groups.
     - Use JFS filesystems as appropriate.
   - Perform some sort of standard test to ensure the application is running correctly. This test can be used later in testing with MC/ServiceGuard. If possible, try to connect to the application through a client.
   - Crash the standalone system, reboot it, and test how the application starts up again. Note the following:
     - Are there any manual procedures? if so, document them.
     - Can everything start up from rc scripts?
   - Try to write a simple script which brings everything up without having to do any keyboard typing. Figure out what the administrator would do at the keyboard, then put that into the script.
   - Try to write a simple script to bring down the application. Again, figure out what the administrator would do at the keyboard, then put that into the script.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1486
Nº 3702
Doc.

17.385
J

Integrating HA Applications in Multiple Systems

1. Install the application on a second system.
   - Create the LVM infrastructure on the second system.
   - Add the appropriate users to the system.
   - Install the appropriate executables.
   - With the application *not* running on the first system, try to bring it up on the second system. You might use the script you created in the step above. Is there anything different that you must do? Does it run?
   - Repeat this process until you can get the application to run on the second system.
2. Configure the MC/ServiceGuard cluster:
   - Create the cluster configuration.
   - Create a package.
   - Create the package script.
   - Use the simple scripts you created in earlier steps as the customer defined functions in the package control script.
3. Start the cluster and verify that applications run as planned.

Testing the Cluster

1. Test the cluster:
   - Have clients connect.
   - Provide a normal system load.
   - Halt the package on the first node and move it to the second node:

     ```
     # cmhaltpkg pkg1
     # cmrunpkg -n node2 pkg1
     # cmmodpkg -e pkg1
     ```

   - Move it back.

     ```
     # cmhaltpkg pkg1
     # cmrunpkg -n node1 pkg1
     # cmmodpkg -e pkg1
     ```


RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1487
Doc: 3702

17.384
1

- Fail one of the systems. For example, turn off the power on node 1. Make sure the package starts up on node 2.
- Repeat failover from node 2 back to node 1.

2. Be sure to test all combinations of application load during the testing. Repeat the failover processes under different application states such as heavy user load versus no user load, batch jobs vs online transactions, etc.
3. Record timelines of the amount of time spent during the failover for each application state. A sample timeline might be 45 seconds to reconfigure the cluster, 15 seconds to run `fsck` on the filesystems, 30 seconds to start the application and 3 minutes to recover the database.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1488
Nº Doc: 3702

17.383

E Rolling Software Upgrades

You can upgrade the HP-UX operating system and the MC/ServiceGuard software one node at a time without bringing down your clusters. This process can also be used any time one system needs to be taken offline for hardware maintenance or patch installations. Until the process of upgrade is complete on all nodes, you cannot change the cluster configuration files, and you will not be able to use any of the features of the new MC/ServiceGuard release.

Refer also to the section on hardware maintenance in the "Troubleshooting" chapter.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
1489
Fls Nº
3702
Doc:

Steps for Rolling Upgrades

Use the following steps:

1. Use cmhaltnode to halt the node you wish to upgrade. This will cause the node's packages to start up on an adoptive node.
2. Edit the /etc/rc.config.d/cmcluster file to include the following line:

   AUTOSTART_CMCLD = 0
3. Upgrade the node to the available HP-UX release, including MC/ServiceGuard. You can perform other software or hardware upgrades if you wish, provided you do not detach any SCSI cabling.
4. Edit the /etc/rc.config.d/cmcluster file to include the following line:

   AUTOSTART_CMCLD = 1
5. Restart the cluster on the upgraded node via the cmrunnode command.
6. Repeat this process for each node in the cluster.

NOTE Be sure to plan sufficient system capacity to allow moving the packages from node to node during the process without an unacceptable loss of performance.

If a cluster were to fail before the rolling upgrade was complete (perhaps due to a catastrophic power failure), the cluster can be restarted by entering the cmruncl command from a node which has been upgraded to the latest revision of the software.

Performing a Cold Install During Rolling Upgrade

If you are doing a cold install when rolling HP-UX to a new release, you should use the following procedure on each node:

1. Use cmhaltnode to halt the node you wish to upgrade. This will cause the node's packages to start up on an adoptive node.
2. Perform the cold install of the operating system.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1490
Nº 3702

17.381

3. Create a directory named /etc/cmcluster on the freshly installed node, and copy into it the /etc/cmcluster/cmclconfig file from a node that is running the earlier release.
4. Install the new version of MC/ServiceGuard.
5. Edit the /etc/rc.config.d/cmcluster file to include the following line:

   AUTOSTART_CMCLD = 1
6. Restart the cluster on the upgraded node via the cmrunnode command.
7. Repeat this process for each node in the cluster.

Using SAM to Perform a Rolling Upgrade

A rolling upgrade can be carried out using SAM instead of HP-UX commands. However, SAM must be invoked on a node containing the latest revision of the software. Performing tasks on a node containing an earlier revision of the software will not work or will cause inconsistent results.

To perform a rolling upgrade using SAM, from the SAM main menu, choose Clusters, then High Availability Clusters, and then select the appropriate type of administration — cluster or package administration. Perform the tasks as explained in the steps in the following section, using SAM instead of HP-UX commands.

Keeping Kernels Consistent

If you change kernel parameters as a part of doing a rolling upgrade, be sure to change the parameters similarly on all nodes that can run the same packages in a failover scenario.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1491
Doc: 3702

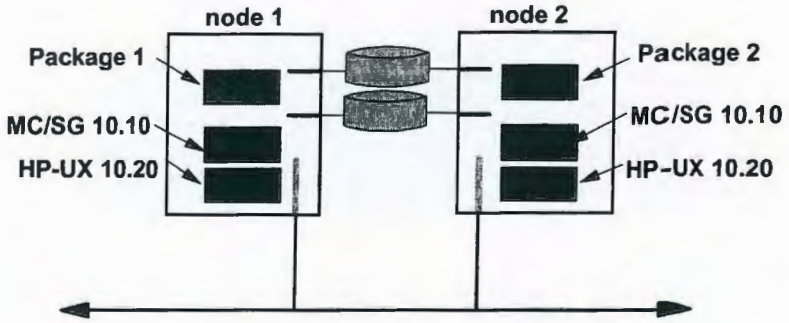
17.380

Example of Rolling Upgrade

While you are performing a rolling upgrade warning messages may appear while the node is determining what version of software is running. This is a normal occurrence and not a cause for concern.

The following example shows a simple rolling upgrade on two nodes running one package each, as shown in Figure E-1. (This and the following figures show the starting point of the upgrade as MC/ServiceGuard 10.10 and HP-UX 10.20 for illustration only. A roll to MC/ServiceGuard 11.01 and HP-UX 11.00 is shown. For your systems, substitute the actual release numbers of your rolling upgrade path.)

Figure E-1 **Running Cluster Before Rolling Update**



Step 1.

Halt the first node, as follows

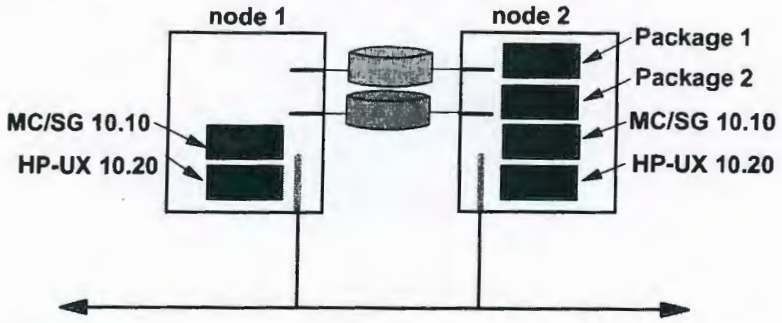
```
# cmhaltnode -f node1
```

This will cause PKG1 to be halted cleanly and moved to node 2. The MC/ServiceGuard daemon on node 1 is halted, and the result is shown in Figure E-2.

RQS nº 03/2005 - CN - CPMI - CORREIOS
1492
Fls Nº
Doc: 3702

17.379

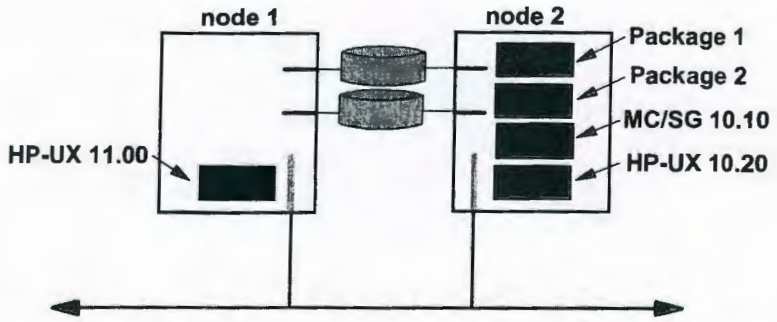
Figure E-2 **Running Cluster with Packages Moved to Node 2**



Step 2.

Upgrade node 1 to the next operating system release (in this example, HP-UX 11.00), and install the next version of MC/ServiceGuard (11.01).

Figure E-3 **Node 1 Upgraded to HP-UX 11.00**



Step 3.

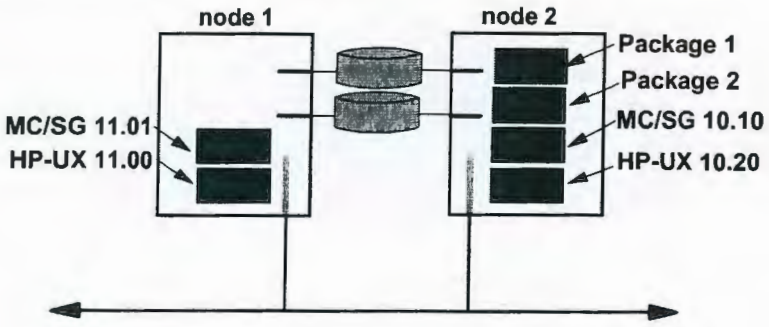
When upgrading is finished, enter the following command on node 1 to restart the cluster on node 1.

```
# cmrunnode -n node1
```

At this point, different versions of the MC/ServiceGuard daemon (*cmcld*) are running on the two nodes, as shown in Figure E-4.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1493
3702

Figure E-4 **Node 1 Rejoining the Cluster**



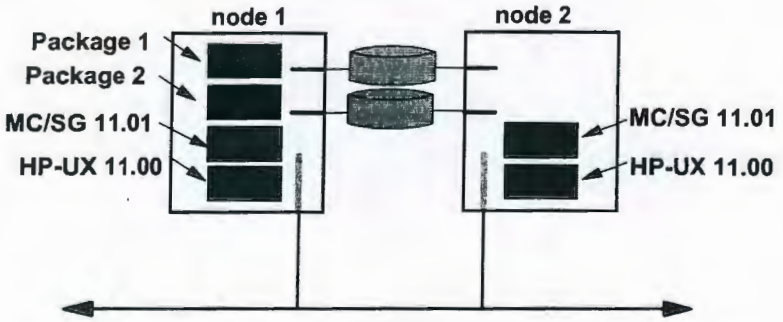
Step 4.

Repeat the process on node 2. Halt the node, as follows:

```
# cmhaltnode -f node2
```

This causes both packages to move to node 1. Then upgrade node 2 to HP-UX 11.00 and MC/ServiceGuard 11.01.

Figure E-5 **Running Cluster with Packages Moved to Node 1**



Step 5.

Move PKG2 back to its original node. Use the following commands:

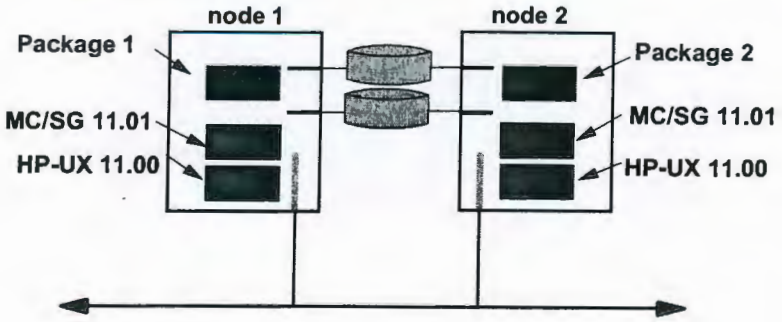
```
# cmhaltpkg pkg2
# cmrunpkg -n node2 pkg2
# cmmodpkg -e pkg2
```


RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1494
Doc: 3702

1377

The `cmmodpkg` command re-enables switching of the package, which is disabled by the `cmhaltpkg` command. The final running cluster is shown in Figure E-6.

Figure E-6 Running Cluster After Upgrades



RQS nº 03/2005 - CN -
CPMI - CORREIOS
1495
Fls Nº
Doc 702

17.376

Limitations of Rolling Upgrades

The following limitations apply to rolling upgrades:

- During rolling upgrade, HP-UX commands and SAM interactive screens must be invoked on a node containing the latest revision of the software. Performing tasks on a node containing an earlier revision of the software will not work or will cause inconsistent results.
- You cannot modify the cluster or package configuration until the upgrade is complete. You *cannot* modfy the hardware configuration--including the cluster's network configuration--during rolling upgrade. This means that you must upgrade all nodes to the new release before you can modify the configuration file and copy it to all nodes.
- None of the features of the newer release of MC/ServiceGuard are allowed until all nodes have been upgraded.
- Binary configuration files may be incompatible between releases of MC/ServiceGuard. Do *not* manually copy configuration files between nodes except as part of a cold install process (see "Performing a Cold Install During Rolling Upgrade," above).
- Rolling upgrades are only supported from the previous two releases. For more information, see the *MC/ServiceGuard Release Notes* for your particular release.
- You can perform a rolling upgrade only on a configuration that has not been modified since the last time the cluster was started.
- Rolling upgrades are not intended as a means of using mixed releases of MC/ServiceGuard or HP-UX within the cluster. It is highly recommended that you upgrade all cluster nodes as quickly as possible to the new release level.
- You cannot delete MC/ServiceGuard software (via **swremove**) from a node while the cluster is in the process of rolling upgrade.

RQS nº 03/2005 - CN - CPMI - CORREIOS
1496
Fls Nº
3702
Doc:

17.375

F Using OTS/9000 on the LAN

MC/ServiceGuard supports OTS/9000, Hewlett-Packard's implementation of OSI Transport Services and related protocols. To configure OTS/9000 with MC/ServiceGuard, perform the following steps:

1. Configure OTS/9000 on all cluster nodes. See your OTS/9000 documentation for complete information.
2. Configure an IP subnet for each LAN card that has OTS on it. This is needed because MC/ServiceGuard actually monitors the LANICS (LAN interface cards) through configured IP subnets. See Chapter 3 for information on specifying IP subnets in MC/ServiceGuard.

When the cluster is running, MC/ServiceGuard will detect network failures by sensing an IP subnet failure.

NOTE In the MC/ServiceGuard environment, OTS/9000 protocol can only be used to transmit data, not heartbeats. However, you can configure a TCP/IP network for heartbeats on the same LAN that is running OTS/9000.

You can configure an OTS monitor as a package dependency within MC/ServiceGuard. Use the SAM interface, and choose "Additional Package Dependencies" in the "Package Configuration" subarea.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1497
Nº 3702 Doc:

17.374

RQS nº 03/2005 - CN -
CPMI - CORREIOS
1498
Fls Nº
3702
Doc

47.373

G Blank Planning Worksheets

This appendix reprints blank versions of the planning worksheets described in the "Planning" chapter. You can duplicate any of these worksheets that you find useful and fill them in as a part of the planning process.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1499
3702

17.372

Blank Hardware Worksheet

```
==========================================================================
SPU Information:

S800 Host Name _____________________   S800 Series No _____________________

Memory Capacity _____________________   Number of I/O Slots _____________
==========================================================================
LAN Information:

Name of          Name of            Node IP            Traffic
Subnet _________ Interface _________ Addr_____________ Type _____________

Name of          Name of            Node IP            Traffic
Subnet _________ Interface _________ Addr_____________ Type _____________

Name of          Name of            Node IP            Traffic
Subnet _________ Interface _________ Addr_____________ Type _____________
==========================================================================
Serial (RS232) Heartbeat Interface Information:

Node Name _____________________ RS232 Device File _______________

Node Name _____________________ RS232 Device File _______________
==========================================================================
X.25 Information

OTS subnet _____________________ OTS subnet _____________________

==========================================================================
Disk I/O Information for Shared Disks:

Bus Type _____ Slot Number ___ Address ___ Disk Device File _____________

Bus Type _____ Slot Number ___ Address ___ Disk Device File _____________

Bus Type _____ Slot Number ___ Address ___ Disk Device File _____________

Bus Type _____ Slot Number ___ Address ___ Disk Device File _____________

Attach a printout of the output from ioscan -fnC disk command
after installing disk hardware and rebooting the system.  Mark this
printout to indicate which physical volume group each disk belongs to.
```


RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1500
Nº Doc: 3702

17.371

Blank Power Supply Worksheet

SPU Power:

S800 Host Name _____ Power Supply _____

S800 Host Name _____ Power Supply _____

Disk Power:

Disk Unit _____ Power Supply _____

Disk Unit _____ Power Supply _____

Disk Unit _____ Power Supply _____

Disk Unit _____ Power Supply _____

Disk Unit _____ Power Supply _____

Disk Unit _____ Power Supply _____

Tape Backup Power:

Tape Unit _____ Power Supply _____

Tape Unit _____ Power Supply _____

Other Power:

Unit Name _____ Power Supply _____

Unit Name _____ Power Supply _____

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1501
Doc 3702

17.370

Blank Volume Group and Physical Volume Worksheet

Volume Group Name: _____

Name of First Physical Volume Group: _____

Physical Volume Name: _____

Physical Volume Name: _____

Physical Volume Name: _____

Physical Volume Name: _____

Physical Volume Name: _____

Physical Volume Name: _____

Physical Volume Name: _____

Name of Second Physical Volume Group: _____

Physical Volume Name: _____

Physical Volume Name: _____

Physical Volume Name: _____

Physical Volume Name: _____

Physical Volume Name: _____

Physical Volume Name: _____

Physical Volume Name: _____

Physical Volume Name: _____

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1502
Nº 3702

87369

Cluster Configuration Worksheet

```
=====================================================================
Name and Nodes:
=====================================================================

Cluster Name: _____

Node Names: _____

Maximum Configured Packages: _____

Cluster Volume Groups: _____

=====================================================================
Subnets:
=====================================================================
Heartbeat IP Addresses: _____

Non-Heartbeat IP Addresses: _____

=====================================================================
Cluster Lock Volume Groups and Volumes:
=====================================================================
First Lock VG:    |    First Lock Physical Volume:
                  |
 _____            |Name (Node 1): _____Disk Unit No: _____Power Unit:____
                  |
                  |Name (Node 2): _____Disk Unit No: _____Power Unit:____
                  |
Second Lock VG:   |  Second Lock Physical Volume:
                  |
 _____            |Name (Node 1): _____Disk Unit No: _____Power Unit:____
                  |
                  |Name (Node 2): _____Disk Unit No: _____Power Unit:____

=====================================================================
Timing Parameters:
=====================================================================

Heartbeat Interval: _____
=====================================================================

Node Timeout: _____
=====================================================================

Network Polling Interval: _____
=====================================================================

Autostart Delay: _____
```


RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1503
Nº 3702
Doc:

Package Configuration Worksheet

```
================================================================================
Package Configuration File Data:
================================================================================

Package Name: _____

Primary Node: _____

First Failover Node:_____

Second Failover Node:_____

Package Run Script: _____Timeout: _____

Package Halt Script: _____Timeout: _____

Package Switching Enabled? _____ Local Switching Enabled? _____

Node Failfast Enabled? _____

Additional Package Resource:

Resource Name:_____ Polling Interval_____ Resource UP Value_____

================================================================================

Package Control Script Data:
================================================================================

VG[0]_____LV[0]_____FS[0]_____FS_MOUNT_OPT[0]_____

VG[1]_____LV[1]_____FS[1]_____FS_MOUNT_OPT[1]_____

VG[2]_____LV[2]_____FS[2]_____FS_MOUNT_OPT[2]_____

IP[0] _____ SUBNET[0]_____

IP[1] _____ SUBNET[1]_____

X.25 Resource Name _____

Service Name: _____ Run Command: _____Retries: _____

Service Fail Fast Enabled? _____Service Halt Timeout _____

Service Name: _____ Run Command: _____ Retries: _____

Service Fail Fast Enabled? _____Service Halt Timeout _____
```


RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1504
Doc: 3702

17.367
L

Index

A

active node, 17
adding a package to a running cluster, 162
adding cluster nodes
  advance planning, 104
adding nodes to a running cluster, 149
adding nodes while the cluster is running, 155
adding packages on a running cluster, 143
additional package resource
  parameter in package configuration, 95
additional package resources
  monitoring, 53
addressing, SCSI, 72
administration
  adding nodes to a ruuning cluster, 149
  cluster and package states, 179
  halting a package, 160
  halting the entire cluster, 151
  moving a package, 160
  of cluster and packages, 147
  of packages and services, 159
  of the cluster, 148
  reconfiguring a package while the cluster is running, 162
  reconfiguring a package with the cluster offline, 161
  reconfiguring the cluster, 152
  removing nodes from operation in a ruuning cluster, 150
  responding to cluster events, 166
  reviewing configuration files, 188
  starting a cluster when all nodes are down, 148
  starting a package, 159
  troubleshooting, 179
adoptive node, 17
alternate Links
  creating volume groups with, 111
applications
  automating, 208
  checklist of steps for integrating with MC/ServiceGuard, 229
  handling failures, 224
  writing HA services for networks, 209
ARP messages
  after switching, 61
array
  replacing a faulty mechanism, 175
arrays
  disk arrays for data protection, 33
ASCII cluster configuration file template, 118
ASCII package configuration file template, 134
AUTO_START_TIMEOUT
  parameter in the cluster configuration file, 86
AUTO_START_TIMEOUT (autostart delay)
  in sample configuration file, 118
  parameter in cluster manager configuration, 86
automatic restart of cluster, 47
automatic switching
  parameter in package configuration, 96
automatically restarting the cluster, 153
automating application operation, 208
autostart delay
  parameter in the cluster configuration file, 86
autostart for clusters
  setting up, 128

B

backing up cluster lock information, 50
binding
  in network applications, 219
bridged net
  defined, 26
  for redundancy in network interfaces, 26
building a cluster
  ASCII cluster configuration file template, 118
  cluster configuration steps, 117
  identifying cluster lock volume group, 120
  identifying cluster-aware volume groups, 120
  logical volume infrastructure, 107
  verifying the cluster configuration, 122
building an ha cluster configuration, 101
bus type
  hardware planning, 73

C

changes in cluster membership, 47
changes to cluster allowed while the cluster is running, 154
changes to packages allowed while the cluster is running, 164

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1505
3702
Doc:

17.366
2

Index

changing the volume group configuration while the cluster is running, 157
checkpoints, 213
client connections
restoring in applications, 222
cluster
configuring with commands, 118
configuring with SAM, 117
MC/ServiceGuard, 16
redundancy of components, 24
typical configuration, 16
understanding components, 24
cluster administration, 148
solving problems, 192
cluster and package maintenance, 147
cluster configuration
creating with SAM or Commands, 117
file on all nodes, 45
identifying cluster lock volume group, 120
identifying cluster-aware volume groups, 120
planning, 81
planning worksheet, 87
sample diagram, 69
step by step, 101
verifying the cluster configuration, 122
cluster configuration file, 118
Autostart Delay parameter (AUTO_START_TIMEOUT), 86
cluster coordinator
defined, 45
cluster lock
4 or more nodes, 48, 49
and cluster re-formation time, 82
backup up lock data, 50
choosing the lock volume group, 81
dual locks, 49
identifying in configuration file, 120
no locks, 49
single lock, 49
storing configuration data, 125
two nodes, 48
use in re-forming a cluster, 48
cluster manager
automatic restart of cluster, 47
blank planning worksheet, 247
cluster name parameter, 83
cluster node parameter, 83
cluster volume group parameter, 83
defined, 45
dynamic re-formation, 47
heartbeat interval parameter, 85
heartbeat subnet parameter, 83
initial configuration of the cluster, 45
main functions, 45
maximum configured packages parameter, 85
monitored non-heartbeat subnet, 84
network polling interval parameter, 86
node timeout parameter, 85
physical lock volume parameter, 84
planning the configuration, 83
serial device file parameter, 84
testing, 171
cluster node
parameter in cluster manager configuration, 83
cluster parameters
initial configuration, 45
cluster re-formation time, 82
cluster startup
manual, 45
cluster volume group
creating physical volumes, 110
parameter in cluster manager configuration, 83
cluster with high availability disk array
figure, 36
CLUSTER_NAME (cluster name)
in sample configuration file, 118
parameter in cluster manager configuration, 83
clusters
active/standby type, 39
larger size, 39
cmapplyconf, 124, 144
cmcheckconf, 122
troubleshooting, 189
cmdeleteconf
deleting a package configuration, 163
deleting the cluster configuration, 130
cmmodnet
assigning IP addresses in control scripts, 55
cmquerycl
troubleshooting, 189
configuration
ASCII cluster configuration file template, 118
ASCII package configuration file template, 134
basic tasks and steps, 20
cluster, 101
cluster planning, 81
of the cluster, 45
package, 131
package planning, 88

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1506
3702
Doc:

17.365
2

Index

service, 131
configuration file
for cluster manager, 45
troubleshooting, 188
configuration with dual attach FDDI stations
figure, 29
configuring packages and their services, 131
control script
adding customer defined functions, 142
creating with commands, 138
creating with SAM, 138
in package configuration, 138
pathname parameter in package configuration, 93
troubleshooting, 188
controlling the speed of application failover, 210
creating the package configuration, 132
customer defined functions
adding to the control script, 142

D

data
disks, 32
data congestion, 46
databases
toolkits, 205
deactivating volume groups, 113
deciding when and where to run packages, 51
deleting a package configuration
using cmdeleteconf, 163
deleting a package from a running cluster, 163
deleting nodes while the cluster is running, 156
deleting the cluster configuration
using cmdeleteconf, 130
designing applications to run on multiple systems, 215
detecting failures
in network manager, 56
disk
choosing for volume groups, 110
data, 32
interfaces, 32
mirroring, 33
root, 32
sample configurations, 34
disk arrays
creating volume groups with PV links, 111
disk arrays, highly available, 33
disk enclosures
high availability, 33
disk failure
protection through mirroring, 17
disk I/O
hardware planning, 73
disk layout
planning, 78
disk logical units
hardware planning, 73
disk monitor, 34
disk monitor (EMS), 53
disks
in MC/ServiceGuard, 32
replacing, 175
supported types in MC/ServiceGuard, 32
distributing the cluster and package configuration, 144
down time
minimizing planned, 226
DTC
using with MC/ServiceGuard, 99
dual attach FDDI stations, 28
dual cluster locks
choosing, 49
dynamic cluster re-formation, 47

E

eight-node active/standby cluster
figure, 40
eight-node cluster with disk array
figure, 41
EMS
for disk monitoring, 34
for preventive monitoring, 173
monitoring package resources with, 53
using the EMS HA monitors, 53
enclosure for disks
replacing a faulty mechanism, 175
enclosures
high availability, 33
Ethernet
redundant configuration, 26
Event Monitoring Service
for disk monitoring, 34
in troubleshooting, 173
event monitoring service
using, 53
expanding the cluster
planning ahead, 67
expansion
planning for, 92

F

failover
controlling the speed in applications, 210

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1507
Doc: 3702

17.364
2

Index

defined, 17
failover behavior
in packages, 91
failure
kinds of responses, 62
network communication, 64
response to hardware failures, 62
responses to package and service failures, 63
restarting a service after failure, 64
failures
of applications, 224
fibrechannel interconnect in a four-node cluster
figure, 30
fibrechannel switched configurations, 29
figures
cluster with high availability disk array, 36
configuration with dual attach FDDI stations, 29
eight-node active/standby cluster, 40
eight-node cluster with EMC disk array, 41
fibrechannel interconnect in a four-node cluster, 30
MC/ServiceGuard software components, 44
mirrored disks connected for high availability, 35
node 1 rejoining the cluster, 238
node 1 upgraded to HP-UX 10.01, 237
primary disk and mirrors on different buses, 38
redundant FDDI configuration, 28
redundant LANs, 27
root disks on different shared buses, 37
running cluster after upgrades, 239
running cluster before rolling upgrade, 236
running cluster with packages moved to node 1, 238
running cluster with packages moved to node 2, 237
sample cluster configuration, 69
serial (RS232) heartbeat line, 31
tasks in configuring an MC/ServiceGuard cluster, 20
typical cluster after failover, 18
typical cluster configuration, 16
file locking, 221
file systems
array variable in package control script, 97
creating for a cluster, 111
planning, 78
FIRST_CLUSTER_LOCK_PV
in sample configuration file, 118
parameter in cluster manager configuration, 84
FIRST_CLUSTER_LOCK_VG
in sample configuration file, 118
floating IP address
defined, 55
floating IP addresses
in MC/ServiceGuard packages, 55
FS
array variable in package control script, 97
in sample package control script, 139
FS_MOUNT_OPT
array variable in package control script, 97
in sample package control script, 139

G

general planning, 67
gethostbyname
and package IP addresses, 55
gethostbyname(), 217

H

HA
disk enclosures, 33
HA monitors (EMS), 53
HALT_SCRIPT
in sample ASCII package configuration file, 134
parameter in package configuration, 93
HALT_SCRIPT_TIMEOUT (halt script timeout)
in sample ASCII package configuration file, 134
parameter in package configuration, 94
halting a cluster, 151
halting a package, 54, 160
halting the entire cluster, 151
handling application failures, 224
hardware
monitoring, 173
hardware failures
response to, 62
hardware planning
blank planning worksheet, 243
Disk I/O Bus Type, 73
disk I/O information for shared disks, 73
host IP address, 71

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1508
Nº 3702
Doc:

17.363
L

Index

host name, 70
I/O bus addresses, 73
I/O slot numbers, 73
LAN information, 70
LAN interface name, 70
LAN traffic type, 71
memory capacity, 70
number of I/O slots, 70
planning the configuration, 69
RS232 heartbeat line, 71
S800 series number, 70
SPU information, 70
subnet, 70
worksheet, 75
heartbeat
RS232 line, 72
heartbeat interval
parameter in cluster manager configuration, 85
heartbeat line
configuring RS232, 71
heartbeat lines, serial, 31
heartbeat messages, 17
defined, 46
heartbeat subnet address
parameter in cluster manager configuration, 83
HEARTBEAT_INTERVAL
in sample configuration file, 118
parameter in cluster manager configuration, 85
HEARTBEAT_INTERVAL (heartbeat timeout)
parameter in cluster manager configuration, 85
HEARTBEAT_IP
in sample configuration file, 118
parameter in cluster manager configuration, 83
high availability, 16
HA cluster defined, 24
objectives in planning, 67
highly available disk arrays, 33
host IP address
hardware planning, 71
host name
hardware planning, 70
how the cluster manager works, 45
how the network manager works, 55
how the package manager works, 51
HP Predictive monitoring
in troubleshooting, 173

I

I/O bus addresses
hardware planning, 73
I/O slots
hardware planning, 70, 73
identifying cluster-aware volume groups, 120
in-line terminator
permitting online hardware maintenance, 176
installing software
MC/LockManager, 106
integrating HA applications with MC/ServiceGuard, 229
internet
toolkits, 205
introduction
MC/ServiceGuard at a glance, 16
understanding MC/ServiceGuard hardware, 23
understanding MC/ServiceGuard software, 43
IP
in sample package control script, 139
IP address array variable in package control script, 98
IP address
adding and deleting in packages, 56
for nodes and packages, 55
hardware planning, 71
portable, 55
reviewing for packages, 187
switching, 59, 60

J

JFS, 211

K

kernel consistency
in cluster configuration, 104

L

LAN
heartbeat, 46
interface name, 70
planning information, 70
LAN failure
MC/ServiceGuard behavior, 24
LAN interfaces
monitoring with network manager, 56
primary and secondary, 26
LAN planning
host IP address, 71
traffic type, 71
larger clusters, 39
link-level addresses, 217
load sharing with IP addresses, 56
local switching, 57
parameter in package configuration, 97
lock
use of the cluster lock, 48
lock disk

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1509
3702
Doc:

17.367

Index

replacing a faulty mechanism, 176
lock volume group
identifying in configuration file, 120
planning, 81, 82
lock volume group, reconfiguring, 152
logical volumes
array variable in package control script, 97
creating for a cluster, 113
creating the infrastructure, 107
planning, 78
worksheet, 78, 80
lssf
using to obtain a list of disks, 110
LV
array variable in package control script, 97
in sample package control script, 139
lvextend
creating a root mirror with, 108
LVM
commands for cluster use, 107
creating a root mirror, 107
creating file systems, 88
creating logical volumes, 88
creating volume groups, 88
disks, 32
planning, 78
setting up volume groups on another node, 114
LVM configuration
worksheet, 78, 80

M

MAC addresses, 217
man pages, 197
list of pages available for MC/ServiceGuard, 197
managing the cluster and nodes, 148
manual cluster startup, 45
MAX_CONFIGURED_PACKAGES
parameter in cluster manager configuration, 85
maximum number of nodes, 24
MC/LockManager
installing, 106
MC/ServiceGuard
at a glance, 15
introduction, 16
MC/ServiceGuard behavior
in LAN failure, 24
in monitored resource failure, 24
in software failure, 24
MC/ServiceGuard commands
using to configure package, 133
MC/ServiceGuard software components
figure, 44
membership change
reasons for, 47
memory capacity
hardware planning, 70
minimizing planned down time, 226
mirror copies of data
protection against disk failure, 17
MirrorDisk/UX, 33
mirrored disks connected for high availability
figure, 35
mirroring
disks, 33
mkboot
creating a root mirror with, 107
monitored non-heartbeat subnet
parameter in cluster manager configuration, 84
monitored resource failure
MC/ServiceGuard behavior, 24
monitoring hardware, 173
monitoring LAN interfaces
in network manager, 56
moving a package, 160
multiple systems
designing applications for, 215

N

NET_SWITCHING_ENABLED
in sample ASCII package configuration file, 134
parameter in package configuration, 97
network
adding and deleting package IP addresses, 56
failure, 58
load sharing with IP addresses, 56
local interface switching, 57
local switching, 57
OTS/9000 support, 241
redundancy, 26, 31
remote system switching, 59
network communication failure, 64
network components
in MC/ServiceGuard, 26
network manager
adding and deleting package IP addresses, 56
main functions, 55
monitoring LAN interfaces, 56
testing, 172
network planning

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1510
Nº Doc 3702

17.361

Index

subnet, 70
network polling interval (NETWORK_POLLING_INTERVAL)
parameter in cluster manager configuration, 86
network time protocol (NTP)
for clusters, 104
NETWORK_INTERFACE
in sample configuration file, 118
NETWORK_POLLING_INTERVAL (network polling interval)
in sample configuration file, 118
networking
redundant subnets, 70
networks
binding to IP addresses, 219
binding to port addresses, 219
IP addresses and naming, 215
node and package IP addresses, 55
packages using IP addresses, 217
supported types in MC/ServiceGuard, 26
writing network applications as HA services, 209
no cluster locks
choosing, 49
node
basic concepts, 24
in MC/ServiceGuard cluster, 16
IP addresses, 55
node types
active, 17
primary, 17
NODE_FAIL_FAST_ENABLED
in sample ASCII package configuration file, 134
parameter in package configuration, 97
NODE_NAME
in sample ASCII package configuration file, 134
parameter in cluster manager configuration, 83
NODE_TIMEOUT (heartbeat timeout)
in sample configuration file, 118
NODE_TIMEOUT (node timeout)
parameter in cluster manager configuration, 85
nodetypes
primary, 17
NTP
time protocol for clusters, 104

O

online hardware maintenance
by means of in-line SCSI terminators, 176
OTS/9000 support, 241
outages
insulating users from, 208

P

package
adding and deleting package IP addresses, 56
basic concepts, 24
blank planning worksheet, 248
changes allowed while the cluster is running, 164
halting, 54, 160
in MC/ServiceGuard cluster, 16
local interface switching, 57
moving, 160
reconfiguring while the cluster is running, 162
reconfiguring with the cluster offline, 161
remote switching, 59
running, 51
starting, 159
toolkits for databases, 205
package administration, 159
solving problems, 192
package and cluster maintenance, 147
package configuration
additional package resource parameter, 95
automatic switching parameter, 96
control script pathname parameter, 93
distributing the configuration file, 144
in SAM, 132
local switching parameter, 97
package failfast parameter, 97
package name parameter, 93
planning, 88
resource polling interval parameter, 96
resource up parameter, 96
run and halt script timeout parameters, 94
service fail fast parameter, 95
service halt timeout parameter, 95
service name parameter, 95
step by step, 131
subnet parameter, 95
using HP-UX commands, 133
verifying the configuration, 144
writing the package control script, 138
package configuration file, 134

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1511
Nº 3102
Doc:

17.360

Index

package control script
  file systems, 97
  generating with commands, 138
  IP addresses, 98
  logical volumes, 97
  service command, 99
  service name, 98
  service restart variable, 99
  subnets, 98
  volume groups, 97
  worksheet, 100
package coordinator
  defined, 46
package failfast
  parameter in package configuration, 97
package failover behavior, 91
package failures
  responses, 63
package IP address
  defined, 55
package IP addresses
  defined, 55
  reviewing, 187
package manager
  blank planning worksheet, 248
  main functions, 51
  testing, 170
package name
  parameter in package configuration, 93
package switching behavior
  changing, 163
PACKAGE_NAME
  in sample ASCII package configuration file, 134
packages
  deciding where and when to run, 51
parameters
  for failover, 91
parameters for cluster manager
  initial configuration, 45
physical volume
  for cluster lock, 48
  parameter in cluster lock configuration, 84
physical volumes
  blank planning worksheet, 246
  creating for clusters, 110
  planning, 78
  worksheet, 78, 80
PKG_SWITCHING ENABLED
  parameter in package configuration, 96
PKG_SWITCHING_ENABLED
  in sample ASCII package configuration file, 134
planning
  cluster configuration, 81
  cluster lock, 81
  cluster lock and cluster expansion, 82
  cluster manager configuration, 83
  disk I/O information, 73
  for expansion, 92
  hardware configuration, 69
  high availability objectives, 67
  LAN information, 70
  overview, 65
  package configuration, 88
  power, 76
  resource monitoring, 89
  SCSI addresses, 72
  SPU information, 70
  volume groups and physical volumes, 78
  worksheets, 75
planning and documenting an HA cluster, 65
planning for cluster expansion, 67
planning worksheets
  blanks, 243
point of failure
  in networking, 26, 31
point to point connections to storage devices, 40
power planning
  power sources, 76
  worksheet, 77
power supplies
  blank planning worksheet, 245
Predictive monitoring, 173
primary disks and mirrors on different buses
  figure, 38
primary LAN interfaces
  defined, 26
primary network interface, 26
primary node, 17
PV Links, 33
  creating volume groups with, 111
pvcreate
  creating a root mirror with, 107
PVG-strict mirroring
  creating volume groups with, 110

Q

quorum
  in re-formation of cluster, 48

R

RAID
  for data protection, 33
RAID disks, 33
raw volumes, 211
README
  for database toolkits, 205
reconfiguring a package
  while the cluster is running, 162

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1512
Doc 3702

17.359
2

Index

reconfiguring a package with the cluster offline, 161
reconfiguring a running cluster, 154
reconfiguring the entire cluster, 152
reconfiguring the lock volume group, 152
recovery time, 81
redundancy
in networking, 26, 31
of cluster components, 24
redundancy in network interfaces, 26
redundant Ethernet configuration, 26
redundant FDDI configuration
figure, 28
redundant FDDI connections, 28
redundant LANS
figure, 27
redundant networks
for heartbeat, 17
re-formation
of cluster, 47
re-formation time, 82
relocatable IP address
defined, 55
relocatable IP addresses
in MC/ServiceGuard packages, 55
remote switching, 59
removing MC/ServiceGuard from a system, 168
removing nodes from operation in a running cluster, 150
removing packages on a running cluster, 143
replacing disks, 175
resource monitoring
planning, 89
Resource Name
parameter in package configuration, 95
resource polling interval
parameter in package configuration, 96
resource up interval
parameter in package configuration, 96
RESOURCE_NAME
in sample ASCII package configuration file, 134
parameter in package configuration, 95
RESOURCE_POLLING_INTERVAL
in sample ASCII package configuration file, 134
parameter in package configuration, 96
RESOURCE_UP_VALUE
in sample ASCII package configuration file, 134
parameter in package configuration, 96
resources
disks, 32
responses
to cluster events, 166
to package and service failures, 63
responses to failures, 62
responses to hardware failures, 62
restart
automatic restart of cluster, 47
following failure, 64
SERVICE_RESTART variable in package control script, 99
restartable transactions, 212
restarting the cluster automatically, 153
restoring client connections in applications, 222
rhosts file
for security, 103
rolling software upgrades, 233
example, 236
steps, 234
rolling upgrade
limitations, 240
root disk limitations on shared buses, 36
root disks on different shared buses
figure, 37
root mirror
creating with LVM, 107
RS232 connection
for heartbeats, 72
RS232 heartbeat line, configuring, 71
RS232 serial heartbeat line, 31
RS232 status, viewing, 185
RUN_SCRIPT
in sample ASCII package configuration file, 134
parameter in package configuration, 93
RUN_SCRIPT_TIMEOUT
in sample ASCII package configuration file, 134
RUN_SCRIPT_TIMEOUT (run script timeout)
parameter in package configuration, 94
running cluster
adding or removing packages, 143
running packages, 51

S

S800 series number
hardware planning, 70

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1513
3702

17.358

Index

SAM
  for cluster and package administration, 147
  using to configure cluster, 117
  using to configure packages, 132
sample cluster configuration
  figure, 69
sample disk configurations, 34
SCSI addressing, 72
SECOND_CLUSTER_LOCK_PV
  parameter in cluster manager configuration, 84
security
  editing files, 103
serial (RS232) heartbeat line, 30, 31
  figure, 31
serial heartbeat connections
  identifying, 121
serial port
  using for heartbeats, 72
SERIAL_DEVICE_FILE(RS232)
  parameter in cluster manager configuration, 84
service administration, 159
service command
  variable in package control script, 99
service configuration
  step by step, 131
service fail fast
  parameter in package configuration, 95
service failures
  responses, 63
service halt timeout
  parameter in package configuration, 95
service monitor
  how it works, 52
service name
  parameter in package configuration, 95
  variable in package control script, 98
service restart parameter
  variable in package control script, 99
service restarts, 64
SERVICE_CMD
  array variable in package control script, 99
  in sample package control script, 139
SERVICE_FAIL_FAST_ENABLED
  in sample ASCII package configuration file, 134
  parameter in package configuration, 95
SERVICE_HALT_TIMEOUT
  in sample ASCII package configuration file, 134
  parameter in package configuration, 95
SERVICE_NAME
  array variable in package control script, 98
  in sample ASCII package configuration file, 134
  in sample package control script, 139
  parameter in package configuration, 95
SERVICE_RESTART
  array variable in package control script, 99
  in sample package control script, 139
shared disks
  planning, 73
shutdown and startup
  defined for applications, 209
single cluster lock
  choosing, 49
single point of failure
  avoiding, 16
single-node operation, 167
size of cluster
  preparing for changes, 104
SNA applications, 221
software failure
  MC/ServiceGuard behavior, 24
software planning
  LVM, 78
solving problems, 192
SPU information
  planning, 70
standby LAN interfaces
  defined, 26
standby network interface, 26
starting a package, 159
startup and shutdown
  defined for applications, 209
startup of cluster
  manual, 45
  when all nodes are down, 148
state
  of cluster and package, 179
stationary IP addresses, 55
STATIONARY_IP
  parameter in cluster manager configuration, 84
status
  of cluster and package, 179
  package IP address, 187
  system log file, 187
stopping a cluster, 151
stopping a package, 54
SUBNET
  array variable in package control script, 98
  in sample ASCII package configuration file, 134
  in sample package control script, 139

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1514
Nº 3102 Doc:

17.357
2

Index

parameter in package configuration, 95
subnet
hardware planning, 70
parameter in package configuration, 95
supported configurations
S800, 70
supported disks in MC/ServiceGuard, 32
supported networks in MC/ServiceGuard, 26
switching
ARP messages after switching, 61
local interface switching, 57
remote system switching, 59
switching IP addresses, 59, 60
system log file
troubleshooting, 187
system message
changing for clusters, 129

T

tasks in MC/ServiceGuard configuration
figure, 20
template
ASCII cluster configuration file, 118
ASCII package configuration file, 134
testing
cluster manager, 171
network manager, 172
package manager, 170
testing cluster operation, 170
time protocol (NTP)
for clusters, 104
TOC
when a node fails, 62
toolkits
for databases, 205
traffic type
LAN hardware planning, 71
troubleshooting
approaches, 179
monitoring hardware, 173
replacing disks, 175
reviewing control scripts, 188
reviewing package IP addresses, 187
reviewing system log file, 187
using cmquerycl and cmcheckconf, 189
troubleshooting your cluster, 169
typical cluster after failover
figure, 18
typical cluster configuration
figure, 16

U

uname(2), 218
understanding network components in MC/ServiceGuard, 26
UPS
in power planning, 76
use of the cluster lock, 48

V

verifying cluster configuration, 122
verifying the cluster and package configuration, 144
VG
array variable in package control script, 97
in sample package control script, 139
vgcfgbackup
and cluster lock data, 125
vgextend
creating a root mirror with, 107
vgimport
using to set up volume groups on another node, 115
viewing RS232 status, 185
volume group
array variable in package control script, 97
creating for a cluster, 110, 111
creating physical volumes for clusters, 110
deactivating before export to another node, 113
for cluster lock, 48
planning, 78
setting up on another node with LVM Commands, 114
setting up on another node with SAM, 114
worksheet, 78, 80
volume group and physical volume planning, 78
VOLUME_GROUP
in sample configuration file, 118
parameter in cluster manager configuration, 83

W

What is MC/ServiceGuard?, 16
worksheet
blanks, 243
cluster configuration, 87, 247
hardware configuration, 75, 243
LVM configuration, 246
package configuration, 248
package control script, 100
power supply configuration, 77, 245
use in planning, 65

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1515
3702
Doc:

17.356

Index

volume group and physical volumes, 78
volume groups and PV links, 80

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1516
Nº 3702
Doc:

17.355
2

ANEXO UNIDADE DE BACKUP ROBOTIZADO
PARTE D/1

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

RQS nº 03/2005 - CN -
CPMI - CORREIOS
1517
Fls Nº
3702
Doc:

17.354
L

HP OpenView Storage Data Protector Administrator's Guide

Manual Edition: May 2003

Manufacturing Part Number: B6960-90078

Release A.05.10

© Copyright Hewlett-Packard Development Company, L.P.2003.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1518
Doc: 5702

17.353

Legal Notices

Hewlett-Packard makes no warranty of any kind with regard to this manual, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Hewlett-Packard shall not be held liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.

Warranty. A copy of the specific warranty terms applicable to your Hewlett-Packard product and replacement parts can be obtained from your local Sales and Service Office.

Restricted Rights Legend. All rights are reserved. No part of this document may be photocopied, reproduced, or translated to another language without the prior written consent of Hewlett-Packard Company. The information contained in this document is subject to change without notice.

Use, duplication or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 for DOD agencies, and subparagraphs (c) (1) and (c) (2) of the Commercial Computer Software Restricted Rights clause at FAR 52.227-19 for other agencies.

Hewlett-Packard Company
United States of America

Copyright Notices. ©Copyright 1983-2003 Hewlett-Packard Development Company, L.P. all rights reserved.

Reproduction, adaptation, or translation of this document without prior written permission is prohibited, except as allowed under the copyright laws.

©Copyright 1979, 1980, 1983, 1985-93 Regents of the University of California

This software is based in part on the Fourth Berkeley Software Distribution under license from the Regents of the University of California.

©Copyright 1986-1992 Sun Microsystems, Inc.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1519
Nº 3702
Doc:

17.352
2

©Copyright 1985-86, 1988 Massachusetts Institute of Technology

©Copyright 1989-93 The Open Software Foundation, Inc.

©Copyright 1986-1997 FTP Software, Inc. All rights reserved

©Copyright 1986 Digital Equipment Corporation

©Copyright 1990 Motorola, Inc.

©Copyright 1990, 1991, 1992 Cornell University

©Copyright 1989-1991 The University of Maryland

©Copyright 1988 Carnegie Mellon University

©Copyright 1991-1995 by Stichting Mathematisch Centrum, Amsterdam, The Netherlands

©Copyright 1999, 2000 Bo Branten

Trademark Notices. UNIX® is a registered trademark in the United States and other countries, licensed exclusively through X/Open Company Limited.

X Window System is a trademark of the Massachusetts Institute of Technology.

Motif is a trademark of the Open Software Foundation, Inc. in the U.S. and other countries.

Windows NT™ is a U.S. trademark of Microsoft Corporation. Microsoft®, MS-DOS®, Windows® and MS Windows® are U.S. registered trademarks of Microsoft Corporation.

Oracle®, SQL*Net®, and Net8® are registered U.S. trademarks of Oracle Corporation, Redwood City, California. Oracle Reports™, Oracle8™, Oracle8 Server Manager™ and Oracle8 Recovery Manager™ are trademarks of Oracle Corporation, Redwood City, California.

Java™ is a U.S. trademark of Sun Microsystems, Inc.

Adobe® and Acrobat® are trademarks of Adobe Systems Incorporated.

ARM® is a registered trademark of ARM Limited.

X/Open® is a registered trademark, and the X device is a trademark of X/Open Company Ltd. in the UK and other countries.

VisiCalc® is a U.S. registered trademark of Lotus Development Corp.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
1520
Fls Nº
3702
Doc:

17.351
2

HP-UX Release 11.00 and later (in both 32- and 64-bit configurations) on all HP 9000 computers are Open Group UNIX 95 branded products.

Netscape and Netscape Navigator are U.S. trademarks of Netscape Communications Corporation.

OpenView® is a registered U.S. trademark of Hewlett-Packard Company.

© 2003 Bristol Technology, Inc., Bristol Technology, Wind/U, HyperHelp and Xprinter are registered trademarks of Bristol Technology Inc.

Other reserved names are trademarks of the respective companies.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1521
Doc: 3702

17.350
L

Contents

1. Introducing Data Protector

In This Chapter 2
The Data Protector Cell Environment 3
How a Backup Session Works 4
How a Restore Session Works 4
Using the Data Protector User Interface 6
Graphical User Interface 7
The Command-Line Interface 11
Data Protector Online Resources 12
Using Microsoft Management Console (MMC) 13
Overview of Tasks to Set Up Data Protector 15

2. Configuring and Using Backup Devices

In This Chapter 18
Configuring Backup Devices 20
Configuring Standalone Devices 23
Configuring File Devices 26
Configuring Library Devices 29
Configuring Libraries with Multiple Systems 32
Configuring Magazine Devices 34
Configuring Stacker Devices 35
Configuring a Library for Mixed Media 37
Configuring Devices for Direct Backup 38
Configuration Procedure 39
Support of New Devices 41
Using Several Drive Types in a Library 42
Shared Devices in the SAN Environment 44
Locking Devices Used Exclusively by Data Protector 46
Locking Devices Used by Multiple Applications 46
Direct Library Access Concept 47
Indirect Library Access Concept 47
Configuration Overview 47
Shared Devices and MC/ServiceGuard 58
Drive Cleaning 61
Configuring Automatic Drive Cleaning 62
Testing the Drive Cleaning Configuration 63
Busy Drive Handling 65
Activating Barcode Support 66

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1522
Nº 3702
Doc:

347.349
L

Contents

Activating Cartridge Memory Support 68
Disabling a Backup Device 70
Removing a Backup Device 72
Renaming a Backup Device 73
Device Locking 74
Device Concurrency, Segment Size, and Block Size 76

3. Configuring Users and User Groups

In This Chapter 82
Data Protector User Rights 83
Predefined Data Protector User Groups 86
Adding or Deleting a User Group 88
Adding a User Group 88
Deleting a User Group 89
Adding or Deleting a User 90
Modifying a User 92
Changing User Properties 92
Moving a User to Another User Group 92
Changing User Group Rights 93
Example User Configurations 94
Allowing Users to Restore Their Own Files 94
Enabling Users to Back Up Their Systems 94

4. Managing Media

In This Chapter 98
Overview of Data Protector Media Management 99
Media Life Cycle 100
Creating a Media Pool 102
Properties of a Media Pool 103
Adding Media to a Media Pool 107
Formatting Media 108
Formatting Media in a Magazine 110
Recognizing Other Data Formats 111
Importing Media 113
Importing the Catalog from Media 114
Importing Media in a Magazine Device 115
Appending Backups to Media 117
Using a Pre-Allocation List of Media for Backup 119

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1523
3702
Doc

17.348
2

Contents

Selecting Media for Backup 120
Media Selection 120
Setting Data Protection for Media 122
Recycling Media 123
Moving Media to Another Pool 124
Exporting Media from Data Protector 125
Modifying Media Locations 126
Modifying Media Descriptions 127
Verifying Data on a Medium 128
Scanning Media in a Device 129
Checking the Condition of a Medium 131
Factors Influencing the Condition of Media 132
Changing How Media Condition Is Calculated 134
Searching for and Selecting a Medium 135
Entering a Medium into a Device 136
Ejecting a Medium from a Device 137
Scheduled Eject of Media 138
Vaulting Media 140
Configuring Vaults 141
Moving Media to a Vault 141
Restoring from Media in a Vault 141
Copying Media 143
Automated Media Copying 145
Detection of Write-Protected Media 147
Using Different Media Format Types 148
Modifying Views in the Media Management Window 149

5. Backup

In This Chapter 152
Configuring a Backup 153
Creating a Backup Specification 154
Backing Up UNIX Systems 161
Backing Up UNIX Filesystems 161
Backing Up Clients Using Disk Discovery 163
Backing Up Disks Using NFS 164
Backing Up UNIX Disks as Disk Image Objects 166
Backing Up Windows Systems 168
Backing Up Filesystems (Logical Disk Drives) 168

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1524
3702

17.347
L

Contents

Backing Up CONFIGURATION 173
Backing Up Windows Clients Using Disk Discovery 183
Backing Up Windows Shared Disks 185
Backing Up Windows Disks as Disk Image Objects 190
Backing Up Novell NetWare Systems 194
Backing Up Novell NetWare Filesystems (Volumes) 194
Client Backup with Disk Discovery 198
Backing Up NetWare Directory Services (NDS) 199
Backing Up OpenVMS Systems 201
Backing Up OpenVMS Filesystems 201
Backing Up in a Direct Backup Environment 204
Backup Specification Configuration Procedure 205
Starting Direct Backup Using the CLI 206
Scheduling Unattended Backups 207
Starting Backups on Specific Dates 209
Starting Periodic Backups 209
Editing Your Backup Schedule 210
Skipping Backups During Holidays 211
Configuring Backup Options When Scheduling Backups 211
Running Consecutive Backups 212
Selecting a Backup Type: Full or Incremental 213
Using Backup Templates 216
Data Protector Default Backup Templates 216
Options Offered by Templates 216
Using a Backup Template When Creating a New Backup Specification 218
Applying a Backup Template 218
Creating a New Template 220
Modifying an Existing Template 220
Groups of Backup Specifications 222
Using Backup Options 225
Most Frequently Used Backup Options 227
List of Data Protector Backup Options 236
Device Backup Options 249
Pre- and Post-Exec Commands 250
Pre- and Post- Exec Commands on Windows Systems 251
Pre- and Post- Exec Commands on UNIX Systems 257
Managing Failed Backups 263
Warnings When Backing Up System Disks 263

RQS nº 03/2005 - CN - CPMI - CORREIOS
1525
Fls Nº 3702
Doc:

17.346
L

Preventing Backup Failure 264
Restarting Failed Backups 266

6. Restore

In This Chapter 268
Restoring Your Data. 269
Standard Restore Procedure 269
Restoring Disk Images 273
Restoring Your Data to a Shared Disk 275
Restoring UNIX Systems. 276
Restoring Windows Systems 277
Restoring the Windows CONFIGURATION 280
Restoring the Windows 2000/XP/Server 2003 System State 281
Restoring the Windows Registry 282
Restoring Windows 2000/XP/Server 2003 Services 283
Restoring DFS. 285
Restoring Windows User Profiles and Event Logs 285
Restoring Windows TCP/ IP Services 286
Restoring Novell Netware Filesystems. 287
Restoring Namespace Information and Volume Space Restrictions 287
Restoring File Ownerships and Trustees 288
Restoring the Novell NetWare CONFIGURATION 288
Restoring Novell NDS. 289
Restoring OpenVMS Filesystems 291
What is Restored?. 291
Restore Options 294
List of Restore Options 294
Restore Techniques 299
Restoring Files to Different Paths 299
Restoring Files in Parallel 300
Viewing Files Not in the IDB 301
Restoring Files in Use 302
Restoring by Query 302
Skipping Files for Restore 304
Selecting Only Specific Files (Matching) for Restore 304
Restoring Files and Directories Manually. 305

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1526
Doc. 3702

17.345
2

Contents

7. Monitoring, Reporting, Notifications, and the Event Log

In This Chapter 308
Monitoring Sessions 309
Viewing Currently Running Sessions 309
Viewing Finished Sessions 310
Responding to Mount Requests 310
Restarting Failed Backups 311
Aborting Running Sessions 312
Changing the Amount of Messages Shown 312
Monitoring Several Cells Simultaneously 314
Data Protector Reporting 315
Report Types 317
Backup Specification Reports 317
Configuration Reports 320
IDB Reports 321
Pools and Media Reports 324
Sessions in Timeframe Reports 326
Single Session Report 328
Report Formats 329
Report Send Methods 331
Email Send Method 331
Broadcast Message Send Method 332
Log to File Send Method 332
SNMP Send Method 332
External Send Method 334
Configuring Reports Using the Data Protector GUI 335
Configuring Report Groups and Adding Reports 335
Running Reports and Report Groups Using the Data Protector GUI 338
Running Individual Reports 338
Running Report Groups 338
Running Reports and Report Groups Using the Command-Line Interface 339
Data Protector Notifications 342
Notification Types 342
Notification Send Methods 347
Configuring Notifications 351
Configuring Reports and Notifications on the Web 353
Copying Data Protector Java Programs to the Web Server 354
Restricting Access to Web Reporting 354

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1527
Doc: 3702

17.344
L

Contents

Generating the Reports 355
Configuring Notifications 355
Configuring Report Groups 355
Data Protector Event Log 356

8. Manager-of-Managers Environment

In This Chapter 360
Manager-of-Managers 361
Configuring the Manager-of-Managers 362
Setting Up MoM Manager 363
Importing Data Protector Cells 363
Adding a MoM Administrator 364
Restarting Data Protector Services 364
Centralized Media Management Database (CMMDB) 366
Configuring a Centralized Media Management Database 368
Configuring the CMMDB on the MoM Manager 369
Configuring the CMMDB on the Client Cell 370
Centralized Licensing 372
Setting Up Centralized Licensing 372
Moving Licenses in the MoM Environment 375
Deactivating Centralized Licensing 376
Working with a MoM Environment 377
Importing and Exporting Data Protector Cells 377
Moving Client Systems Among Cells 378
Distributing the MoM Configuration 378
Configuring Data Protector Users 379
Managing Devices and Media for a Specific Cell 379
Restoring, Monitoring, and Reporting in an Enterprise Environment 380

9. Managing the Data Protector Internal Database

In This Chapter 382
About the Data Protector Internal Database 383
The IDB Architecture 384
Configuring the IDB 388
Allocating Disk Space for Future Use 388
Preparing for IDB Recovery 390
Configuring the Database Reports and Notifications 400
Maintaining the IDB 402

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1528
Nº - Doc: 3702

17.343
2

Contents

Reducing the IDB Growth 405
Reducing the IDB Size 406
Purging Obsolete Filenames 408
Extending the Database Size 408
Checking the Database Size 410
Checking the Consistency of the Database 411
Moving the Database to a Different Cell Manager 412
Restoring the IDB 414
Restoring the IDB to a Temporary Directory 414
Moving the IDB to the Original Location 415
Recovering the IDB 417
Overview of IDB Recovery Methods 417
Identifying the Level of Database Corruption 419
Performing Guided Autorecovery 421
Handling Minor Database Corruption in the DCBF Part 422
Handling Major Database Corruption in the Filenames Part 423
Recovering the IDB Using IDB Recovery File and Changed Device 424
Recovering the IDB Without the IDB Recovery File 426
Recovering the IDB from a Specific IDB Session 428
Replaying IDB Transaction Logs 430
Recovering the IDB to a Different Disk Layout 431
Updating the IDB by Importing Media 433

10. Disaster Recovery

In This Chapter 436
Introduction 437
Preparing for a Disaster Recovery 443
Planning 443
Consistent and Relevant Backup 444
Updating the System Recovery Data (SRD) 445
Assisted Manual Disaster Recovery of a Windows System 450
Requirements 451
Limitation 451
Preparation 451
Recovery 456
Disk Delivery Disaster Recovery of a Windows Client 459
Requirements 459
Limitations 460

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1529
Doc: 3702

17.342
2

Contents

Preparation 460
Recovery 461
Enhanced Automated Disaster Recovery of a Windows System 463
Requirements 464
Limitations 465
Preparation 466
Recovery 470
One Button Disaster Recovery of a Windows System 472
Requirements 473
Limitations 474
Preparation 475
Recovery 477
Automated System Recovery 480
Requirements 481
Limitations 482
Preparation 483
Recovery 486
Restoring the Data Protector Cell Manager Specifics 487
Making IDB consistent (all methods) 487
Enhanced Automated Disaster Recovery Specifics 487
One Button Disaster Recovery Specifics 488
Automated System Recovery Specifics 489
Advanced Recovery Tasks 490
Restoring the Microsoft Cluster Server Specifics 490
Restoring Internet Information Server (IIS) Specifics 496
Manual Disaster Recovery of an HP-UX Client 498
Concept 498
Using Custom Installation Medium 499
Using System Recovery Tools 503
Disk Delivery Disaster Recovery of an UNIX Client 507
Limitations 507
Preparation 507
Recovery 510
Manual Disaster Recovery of an UNIX Cell Manager 512
Limitation 512
Preparation 512
Recovery 512
Troubleshooting Disaster Recovery on Windows 514

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1530
Nº Doc: 3702

17.341
L

Contents

General Troubleshooting 514
Troubleshooting Assisted Manual Disaster Recovery 515
Troubleshooting Disk Delivery Disaster Recovery 515
Troubleshooting EADR and OBDR 516

11. Customizing the Data Protector Environment

In This Chapter 522
Global Options File 523
Most Often Used Variables 523
Using Omnirc Options 525
Firewall Support 528
Limiting the Range of Port Numbers 528
Port Usage in Data Protector 531
Examples of Configuring Data Protector in Firewall Environments 535

12. Troubleshooting

In This Chapter 548
Before Calling Your Support Representative 549
Data Protector Log Files 550
Location of Data Protector Log Files 550
Format of Data Protector Log Files 550
Log Files and Their Contents 551
Debugging 553
Limiting the Maximum Size of Debugs 553
Ways of Debugging 554
Debug Syntax 555
Trace File Name 556
INET Debug on UNIX 557
INET Debug on Windows 557
CRS Debug on Windows 557
CRS Debug in the Microsoft Cluster Environment 558
Sample Debugging 558
Browsing Troubleshooting Messages 561
When You Cannot Access Online Troubleshooting 562
Description of Common Problems 564
Troubleshooting Networking and Communication 565
Hostname Resolution Problems 565
Client Fails with "Connection Reset by Peer" 567

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1531
Doc: 3702

17.340
C

Contents

Troubleshooting Data Protector Services and Daemons 569
Problems Starting Data Protector Services on Windows 569
Problems Starting Data Protector Daemons on UNIX 571
Data Protector Processes 573
Troubleshooting Devices and Media 574
Cannot Access Exchanger Control Device on Windows 2000/XP/Server 2003 574
Device Open Problem 575
Using Unsupported SCSI Adapters on Windows 575
Medium Quality Statistics 575
Medium Header Sanity Check 577
Cannot Use Devices After Upgrading to Data Protector A.05.10 578
Other Common Problems 579
Troubleshooting Backup and Restore Sessions 580
Filenames Are Not Displayed Correctly in GUI 580
Full Backups Are Performed Instead of Incrementals 580
Unexpected Mount Request for a Standalone Device 581
Unexpected Mount Request for a Library Device 582
Unexpected Mounted Filesystems Detected 583
Data Protector Fails to Start a Scheduled Session 584
Data Protector Fails to Start an Interactive Session 585
Poor Backup Performance on Novell NetWare Server 585
Data Protector Fails to Start Parallel Restore Media Agent on Novell NetWare Clients 585
Backup Protection Expiration 586
Troubleshooting Application Database Restores 586
Problems with non-ASCII Characters in Filenames 587
Troubleshooting Data Protector Installation 588
Problems with Remote Installation of Windows Clients 588
Name Resolution Problems when Installing the Windows Cell Manager 589
Troubleshooting User Interface Startup 590
Inet Is Not Responding on the Cell Manager 590
No Permissions to Access the Cell Manager 590
Connection to a Remote System Refused on Windows or Novell NetWare 591
Connection to Windows 98 Clients Fails 591
Troubleshooting the IDB 592
Problems During the Upgrade of the IDB on Solaris 592
Problems While Running the User Interface 595
Libraries (Executables) Missing 595
Data Files (Directories) Missing 596

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1532
3702
Doc:

17.339
L

Contents

Temporary Directory Missing 597
Problems During Backup and Import 598
Performance Problems 599
MMDB and CDB Are Not Synchronized 600
Troubleshooting Reporting and Notifications 602
Troubleshooting Data Protector Online Help 603
Troubleshooting Online Help on Windows 603
Troubleshooting Online Help on UNIX 603
Check Whether Data Protector Functions Properly 605
Data Protector Checking and Maintenance Mechanism 605
The User Check Failed Notification 606
Overview of Items to Be Checked 607

13. Integrations with Other Applications

In This Chapter 612
Cluster Integrations with Data Protector 613
Cluster Concepts and Terminology 613
Cluster-Aware Databases and Applications 616
Microsoft Cluster Server Integration 617
Cell Manager on Microsoft Cluster Server 618
Clients on Microsoft Cluster Server 618
Backing Up Data in a Cluster (MSCS) 619
Managing Cluster-Aware Backups 620
MC/ServiceGuard Integration 627
Cell Manager on MC/ServiceGuard 627
Clients on MC/ServiceGuard 637
Backing Up Data in a Cluster (MC/SG) 638
Veritas Cluster Integration 640
Clients on Veritas Cluster 640
Novell NetWare Cluster Integration 642
Clients on Novell NetWare Cluster 642
Data Source Integration (DSI) 644
Application Response Measurement (ARM) Integration 646
ManageX Integration 648
Access Points for System and Management Applications 649
Introduction 649
Data Protector Access Points 649
Examples 653

RQS nº 03/2005 - CN
CPMI - CORREIOS
1533
Fls Nº 3702
Doc:

17.338
L

Contents

14. ADIC/GRAU DAS and STK ACS Libraries

In This Chapter 656
ADIC/GRAU DAS and STK ACS Integrations 657
Configuration Basics 659
Media Management Basics 659
The ADIC/GRAU DAS Library Device 662
Direct Access to the Library: Installation and Configuration 662
Connecting Library Drives 662
Preparing for Installation 662
Installing the DAS Media Agent 664
Using the Data Protector GUI 669
Indirect Access to the DAS Library: Installation and Configuration 670
Using Data Protector to Access the ADIC/GRAU Library 671
The STK ACS Library Device 680
Direct Access to the Library: Installation and Configuration 680
Media Management Basics 680
Connecting Library Drives 681
Installing the ACS Media Agent to Use the StorageTek Library 681
Using Data Protector to Configure the STK ACS Library 686
Indirect Access to the Library: Installation and Configuration 686
Using Data Protector to Access the STK ACS Library 687
Troubleshooting Library Installation and Configuration 697

A. Further Information

In This Appendix A-2
Backing Up and Restoring UNIX Specifics A-3
VxFS Snapshot A-3
Data Protector Commands A-7
Performance Considerations A-8
The Infrastructure A-8
Configuring Backups and Restores A-10
Example of Scheduled Eject of Media A-14
Schedule the Report Group A-14
Add the Report to the Report Group and Configure It A-14
Copy the Script to the Specified Directory A-15
Examples of Pre-Exec and Post-Exec Commands for UNIX A-20
Disaster Recovery:
Move Kill Links on HP-UX 11.x A-25

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1534
Nº 3702
Doc:

17.337
L

Contents

Creating a libaci.o on AIX A-26
Example of the Package Configuration File A-28
Example of the Package Control File A-38
Data Protector Log Files Example Entries A-44
debug.log A-44
sm.log A-46
inet.log A-46
media.log A-46
upgrade.log A-47
Windows Manual Disaster Recovery Preparation Template A-49
Changing Block Size on Windows Media Agent A-51

Glossary

Index

RQS nº 03/2005 - CN -
CPMI - CORREIOS
1535
Fls
Doc: 3702

17.336

Printing History

The manual printing date and part number indicate its current edition. The printing date will change when a new edition is printed. Minor changes may be made at reprint without changing the printing date. The manual part number will change when extensive changes are made.

Manual updates may be issued between editions to correct errors or document product changes. To ensure that you receive the updated or new editions, you should subscribe to the appropriate product support service. See your HP sales representative for details.

Table 1 **Edition History**

Part Number	Manual Edition	Product
B6960-90057	August 2002	Data Protector Release A.05.00
B6960-90078	May 2003	Data Protector Release A.05.10

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1536
Doc: 3702

17.335
L

xx

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1537
Doc 3702

17.334
L

Conventions

The following typographical conventions are used in this manual.

Table 2

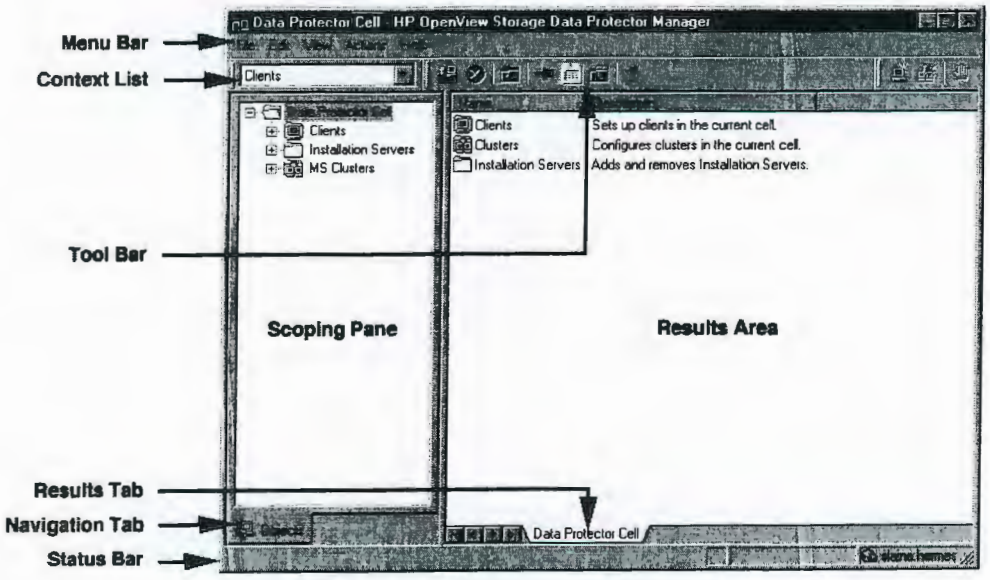
Convention	Meaning	Example
Italic	Book or manual titles, and manual page names	Refer to the *HP OpenView Storage Data Protector Integration Guide* for more information.
	Provides emphasis	You *must* follow these steps.
	Specifies a variable that you must supply when entering a command	At the prompt type: `rlogin` *your_name* where you supply your login name.
Bold	New terms	The Data Protector **Cell Manager** is the main ...
`Computer`	Text and items on the computer screen	The system replies: `Press Enter`
	Command names	Use the `grep` command ...
	File and directory names	`/usr/bin/X11`
	Process names	Check to see if `Data Protector Inet` is running.
	Window/dialog box names	In the `Backup Options` dialog box...
	Text that you must enter	At the prompt, type: `ls -l`
Keycap	Keyboard keys	Press **Return**.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1538
Doc: 3702

17.383
2

Data Protector provides a cross-platform (Windows and UNIX) graphical user interface.

Figure 1 Data Protector Graphical User Interface



RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1539
Doc: 3702

17.332
2

Contact Information

General Information

General information about Data Protector can be found at

http://www.hp.com/go/dataprotector

Technical Support

Technical support information can be found at the HP Electronic Support Centers at

http://support.openview.hp.com/support.jsp

Information about the latest Data Protector patches can be found at

http://support.openview.hp.com/patches/patch_index.jsp

For information on the Data Protector required patches, refer to the *HP OpenView Storage Data Protector Software Release Notes*.

HP does not support third-party hardware and software. Contact the respective vendor for support.

Documentation Feedback

Your comments on the documentation help us to understand and meet your needs. You can provide feedback at

http://ovweb.external.hp.com/lpe/doc_serv/

Training Information

For information on currently available HP OpenView training, see the HP OpenView World Wide Web site at

http://www.openview.hp.com/training/

Follow the links to obtain information about scheduled classes, training at customer sites, and class registration.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1540
Doc 3702

E C T
17.331
2
CPL - AC

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1541
Nº Doc: 3702

17.330

Data Protector Documentation

Data Protector documentation comes in the form of manuals and online Help.

Manuals

Data Protector manuals are available in printed format and in PDF format. Install the PDF files during the Data Protector setup procedure by selecting the `User Interface` component on Windows or the `OB2-DOCS` component on UNIX. Once installed, the manuals reside in the `<Data_Protector_home>\docs` directory on Windows and in the `/opt/omni/doc/C/` directory on UNIX. You can also find the manuals in PDF format at http://ovweb.external.hp.com/lpe/doc_serv/

HP OpenView Storage Data Protector Administrator's Guide

This manual describes typical configuration and administration tasks performed by a backup administrator, such as device configuration, media management, configuring a backup, and restoring data.

HP OpenView Storage Data Protector Installation and Licensing Guide

This manual describes how to install the Data Protector software, taking into account the operating system and architecture of your environment. This manual also gives details on how to upgrade Data Protector, as well as how to obtain the proper licenses for your environment.

HP OpenView Storage Data Protector Integration Guide

This manual describes how to configure and use Data Protector to back up and restore various databases and applications. There are two versions of this manual:

- *HP OpenView Storage Data Protector Windows Integration Guide*

  This manual describes integrations running the Windows operating systems, such as Microsoft Exchange, Microsoft SQL, Oracle, SAP R/3, Informix, Sybase, NetApp Filer, HP OpenView Network Node Manager, and Lotus Domino R5 Server.

RQS nº 03/2005 - CN - CPMI - CORREIOS
1542
Fls Nº
Doc: 3702

17.329
2

- *HP OpenView Storage Data Protector UNIX Integration Guide*

  This manual describes integrations running on the UNIX operating system, such as Oracle, SAP R/3, Informix, Sybase, NetApp Filer, IBM DB2 UDB, HP OpenView Network Node Manager, and Lotus Domino R5 Server.

HP OpenView Storage Data Protector Concepts Guide

This manual describes Data Protector concepts and provides background information on how Data Protector works. It is intended to be used with the task-oriented *HP OpenView Storage Data Protector Administrator's Guide*.

HP OpenView Storage Data Protector EMC Symmetrix Integration Guide

This manual describes how to install, configure, and use the EMC Symmetrix integration. It is intended for backup administrators or operators.

It describes the integration of Data Protector with the EMC Symmetrix Remote Data Facility and TimeFinder features for Symmetrix Integrated Cached Disk Arrays. It covers the backup and restore of file systems and disk images, as well as online databases, such as Oracle and SAP R/3.

HP OpenView Storage Data Protector HP StorageWorks Disk Array XP Integration Guide

This manual describes how to install, configure, and use the integration of Data Protector with HP StorageWorks Disk Array XP. It is intended for backup administrators or operators. It covers the backup and restore of Oracle, SAP R/3, Microsoft Exchange, and Microsoft SQL.

HP OpenView Storage Data Protector EVA/VA/MSA Integration Guide

This manual describes how to install, configure, and use the integration of Data Protector with HP StorageWorks Virtual Array, HP StorageWorks Enterprise Virtual Array or HP StorageWorks Modular SAN Array 1000. It is intended for backup administrators or operators. It covers the backup and restore of Oracle, SAP R/3, Microsoft Exchange, and Microsoft SQL.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
1543
Fls Nº
3702
Doc:

17.328
L

HP OpenView Storage Data Protector Integration Guide for HP OpenView

This manual describes how to install, configure, and use the integration of Data Protector with HP OpenView Service Information Portal, HP OpenView Service Desk, and HP OpenView Reporter. It is intended for backup administrators. It discusses how to use the OpenView applications for Data Protector service management.

HP OpenView Storage Data Protector MPE/iX System User Guide

This manual describes how to install and configure MPE/iX clients, and how to back up and restore MPE/iX data.

HP OpenView Storage Data Protector Integration Guide for HP OpenView Operations

This manual describes how to monitor and manage the health and performance of the Data Protector environment with HP OpenView Operations (OVO), HP OpenView Service Navigator, and HP OpenView Performance (OVP).

HP OpenView Storage Data Protector Software Release Notes

This manual gives a description of new features of HP OpenView Storage Data Protector A.05.10. It also provides information on supported configurations (devices, platforms and online database integrations, SAN, and ZDB), required patches, and limitations, as well as known problems and workarounds. An updated version of the supported configurations is available at http://www.openview.hp.com/products/datapro/spec_0001.html.

Online Help

Data Protector provides context-sensitive (F1) help and Help Topics for Windows and UNIX platforms.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1544
Doc. 3702

17.327
2

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1545
Doc 3702

17.326
L

In This Book

The *HP OpenView Storage Data Protector Administrator's Guide* describes how to configure and use the Data Protector network backup product. You must properly install Data Protector before you can configure it.

NOTE

This manual describes Data Protector functionality without specific information on particular licensing requirements. Some Data Protector functionality is subject to specific licenses. The related information is covered in the *HP OpenView Storage Data Protector Installation and Licensing Guide*.

Audience

This manual is intended for network administrators responsible for maintaining and backing up systems on the network.

Conceptual information can be found in the *HP OpenView Storage Data Protector Concepts Guide*, which is recommended in order to fully understand the fundamentals and the model of Data Protector.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1546
3702

E C T
17.325
L
CPL - A

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1547
Doc 3702

17.324
2

Organization

The manual is organized as follows:

Chapter 1	"Introducing Data Protector" on page 1.
Chapter 2	"Configuring and Using Backup Devices" on page 17.
Chapter 3	"Configuring Users and User Groups" on page 81.
Chapter 4	"Managing Media" on page 97.
Chapter 5	"Backup" on page 151.
Chapter 6	"Restore" on page 267.
Chapter 7	"Monitoring, Reporting, Notifications, and the Event Log" on page 307.
Chapter 8	"Manager-of-Managers Environment" on page 359.
Chapter 9	"Managing the Data Protector Internal Database" on page 381.
Chapter 10	"Disaster Recovery" on page 435.
Chapter 11	"Customizing the Data Protector Environment" on page 521.
Chapter 12	"Troubleshooting" on page 547.
Chapter 13	"Integrations with Other Applications" on page 611.
Chapter 14	"ADIC/GRAU DAS and STK ACS Libraries" on page 655.
Appendix A	"Further Information" on page A-1.
Glossary	Definition of terms used in this manual.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1548
3702
Doc:

ECT
17.323
CPL-AC

1 Introducing Data Protector

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1549
3702

17.322
2

In This Chapter

This chapter contains some general principles on how Data Protector works, covered in these sections:

"The Data Protector Cell Environment" on page 3

"Using the Data Protector User Interface" on page 6

"Overview of Tasks to Set Up Data Protector" on page 15

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1550
Nº 3702

17321
2

The Data Protector Cell Environment

The Data Protector **cell** is a network environment containing a **Cell Manager**, **clients**, and **backup devices**. The Cell Manager has the main Data Protector control software installed and is the central point from which the cell is administered and backup and restore operations are controlled. Systems that are to be backed up can be added to the cell and set up as Data Protector clients. When Data Protector performs a backup of data from these clients, it saves the data to media (such as magnetic tapes, or hard disks) contained within backup devices.

The **Data Protector Internal Database (IDB)** keeps track of the files backed up, making it is easy to browse and restore them, either singly or collectively.

The **Cell Manager** is the main control center for the cell and contains the IDB. It runs the core Data Protector software and the Session Manager, which starts and stops backup and restore sessions and writes session information to the IDB.

Any system within a chosen cell environment can be set up as a Data Protector **client**. Essentially, a client is a system that can be backed up, a system connected to a backup device with which the backup data can be saved, or both. The role of the client depends on whether it has a Disk Agent or a Media Agent installed.

A client that will be backed up using Data Protector must have a **Disk Agent** installed. Data Protector controls the access to the disk. The Disk Agent lets you back up information from, or restore information to, the client system.

A client system with connected backup devices must have a **Media Agent** installed. This software controls the access to the backup device. The Media Agent controls reading from and writing to a backup device's media.

A **backup device** performs the actual recording of backup data to a recording medium, and the retrieval of restore data from a medium.

The physical object upon which the data is recorded, such as a DAT tape or a hard disk, is called the backup **medium**.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1551
Nº Doc: 3702

17.320
C

NOTE For further information on these terms, or on the principles of Data Protector operation, see the *HP OpenView Storage Data Protector Concepts Guide*.

How a Backup Session Works

A backup session starts either when a backup is requested through the user interface, or when a scheduled backup is initiated. During this session, Data Protector backs up the requested filesystems and disks to the specified media.

1. The Cell Manager determines the type of session that has been requested (backup) and starts the appropriate Session Manager.
2. The Session Manager reads the backup specification and determines what needs to be backed up and which devices to use.
3. The Session Manager then starts a Media Agent for each media drive that will be used and a Disk Agent for each disk that will be read.
4. The Monitor window appears. This window lets you respond to mount requests and view the progress of a backup session.
5. The Disk Agents start sending data to the Media Agent.
6. If more than one Disk Agent is used, the Disk Agents send data to the Media Agent concurrently and the Media Agent places the data on the medium.
7. As each block of data is written to the medium, the Media Agent sends information to the Session Manager about what has been backed up. The Session Manager uses this information to update the catalog of backed-up files in the IDB.

How a Restore Session Works

A restore session starts when a restore is requested. During this session, Data Protector performs a restore of requested files and disks from the media.

1. You specify which filesystems to restore and how to restore them, using the Data Protector user interface.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
1552
Fls Nº
3702
Doc:

17.319

2. The Cell Manager determines the type of session that has been requested (restore), and starts the appropriate Session Manager.
3. The Session Manager then determines which filesystems or directories to restore, which devices to use, and what restore options have been specified.
4. The Session Manager starts the appropriate Disk Agent and Media Agent. For example, a Media Agent is started for the media (tape) drive that will be used and a Disk Agent is started for the disk to which the data will be restored.
5. The `Monitor` window appears. This window lets you respond to mount requests and view the progress of a restore session.
6. The Media Agent starts sending data to the Disk Agent.
7. The Session Manager then updates the IDB and the Disk Agent writes the data to the disk.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1553
Doc 3702

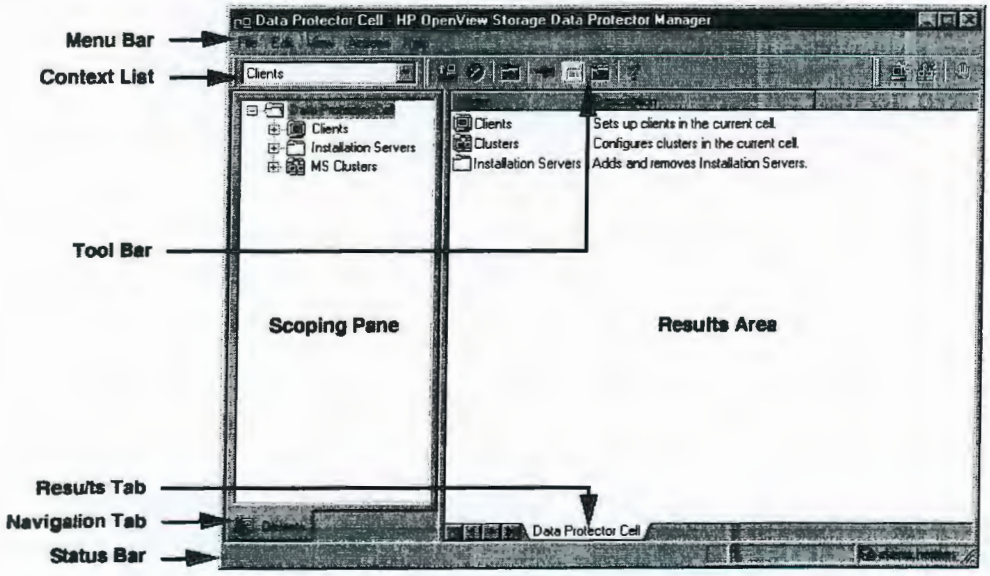
17.318
L

Using the Data Protector User Interface

There is one Data Protector user interface, available on Windows and UNIX platforms. It consists of the Data Protector graphical user interface (GUI) and the command-line interface.

Using the Data Protector user interface, you can perform all Data Protector tasks.

Figure 1-1 HP OpenView Storage Data Protector Graphical User Interface



RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1554
Doc: 3702

17.317

Graphical User Interface

The Data Protector graphical user interface (GUI) uses features such as buttons and text boxes to enhance usability. Whenever possible, drop-down lists are provided to allow you to select from a list instead of typing in your selection. In addition, a comprehensive online Help system provides information about each window and each task.

Depending on the user rights, you can either use the GUI to access the complete Data Protector functionality or to access only specific contexts.

For more information on user rights, refer to "Data Protector User Rights" on page 83.

For more information on Data Protector contexts, refer to "Context List" on page 9.

Starting GUI on Windows Platforms

To start the Data Protector GUI on Windows platforms, do one of the following:

- Click `Start` on the Windows desktop and click `Data Protector Manager` from the `HP OpenView Storage Data Protector` program group to start the GUI for the complete Data Protector functionality.
- Use the `manager` command to start the GUI for the complete Data Protector functionality.

  Context-specific options for this command enable you to start one or more Data Protector contexts. For example, the command
  `manager -backup -restore`
  starts the Data Protector `Backup` and `Restore` contexts.

  To specify the Cell Manager you want to connect to, use the following command: `manager -server` *`<Cell Manager_name>`*.

  For more information on these commands, refer to the *`omnigui`* man page.

Starting GUI on UNIX Platforms

To use the Data Protector GUI on UNIX platforms, enter:

`xomni`	to start the GUI with the complete Data Protector functionality
`xomniadmin`	to start the administration (configuration) of clients, users, reports, and the IDB GUI
`xomnibackup`	to start the backup GUI

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1555
Doc: 3702

17.310
C

`xomnicellmon`	to start the MoM cell monitoring GUI
`xomnimm`	to start the media and devices management GUI
`xomnimonitor`	to start the monitoring a single cell GUI
`xomnirestore`	to start the restore GUI
`xomniinstrec`	To start the instant recovery GUI. A special license is needed to start this GUI. Refer to the *HP OpenView Storage Data Protector HP StorageWorks Disk Array XP Integration Guide* for more information on the instant recovery functionality and to the *HP OpenView Storage Data Protector Installation and Licensing Guide* for more information on Data Protector licenses.
`xomnimom`	to start the Manager-of-Managers GUI

For more information on these commands, refer to the `omnigui` man page.

Printing from the Data Protector Graphical User Interface

Data Protector lets you print from the GUI. You can print session messages, reports, event logs, and various lists (for example, lists of configured clients and devices). Generally, you can print anything displayed as a list in the Results Area, and the online Help topics. However, you are not able to print any of the `Properties`. Instead, you can use the Data Protector reporting functionality to configure various reports about your backup environment. For more information on reporting, refer to "Data Protector Reporting" on page 315.

Prerequisite

You must have a printer already configured on your system.

When you click `Print` on HP-UX, you can choose among predefined printers. Note that if you do not have a proper printer driver installed, you are not able to print. In that case, choose a PS printer and select the `Print to file` option. You can then send the generated file to the PS printer using the UNIX `lp` command from the UNIX terminal.

On Windows, however, a displayed printer in the `Select Printer` window means that the printer is already configured on your system and you are able to print.

For detailed steps on printing, refer to online Help, index keyword "printing from GUI".

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1556
Doc: 3702

17.315
L

Elements of the Data Protector Graphical User Interface

For the visual representation of the GUI elements, refer to Figure 1-1 on page 6.

Context List

The **Context List** is a drop-down list, from which you can select the management contexts described below:

`Clients`	Controls all of the client systems in the current Data Protector cell. You can add, delete, and monitor any client within the cell.
`Users`	Adds and removes users, user groups and their rights.
`Devices & Media`	Controls device and media maintenance and access to media which store the data.
`Backup`	Controls which data is to be backed up, where, and how.
`Restore`	Controls which data is to be restored, where, and how.
`Instant Recovery`	Controls the split mirror instant recovery processes. A special license is needed to display this context. Refer to the *HP OpenView Storage Data Protector HP StorageWorks Disk Array XP Integration Guide* for more information on the instant recovery functionality and to the *HP OpenView Storage Data Protector Installation and Licensing Guide* for more information on Data Protector licenses.
`Reporting`	Allows you to get information on your cell configuration, backup specifications, media and media pools, as well as on specific sessions and objects.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1557
Doc 3702

17 314
2

`Internal Database`	Allows you to get information on the IDB storage capacity, database objects, and sessions.
`Monitor`	Allows you to monitor sessions that are in progress.

Scoping Pane

The **Scoping Pane** provides a tree of items that can be selected to open a view. Selecting an item in the Scoping Pane displays information in the **Results Area**.

Results Area

Selecting an item in the Scoping Pane displays corresponding information in the **Results Area**. If you click `Clients` in the Scoping Pane, the Results Area displays a list of all the clients within your cell.

Navigation Tabs

Navigation Tabs appear at the bottom of the Scoping Pane. These tabs allow you to switch between the two possible item list views in the Scoping Pane: **Objects** and **Tasks**. Not every Scoping Pane has these views.

Tab Name	*What the Tab Displays in the Scoping Pane*
`Objects`	A hierarchical presentation of data, similar to the directory tree in Windows Explorer. For example, in the Devices & Media context, the Scoping Pane will display the list of devices and media configured with Data Protector.
`Tasks`	A list of tasks that you can perform. Clicking a task displays a wizard that will walk you through an entire task, such as backing up a file.

Results Tab

The name on the **Results Tab** corresponds to the name of the item currently selected in the Scoping Pane. You can click the Pin icon on the toolbar to make this view "stick" and keep it available for the future. For example, if you need to use the GUI to look up some other information, but you want to continue with the previous view later, you can access this view by selecting the "pinned" tab.

You can remove one or more tabs by right-clicking the area and selecting `Remove Tab` or `Remove Other Tabs`.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1558
Nº 3702
Doc:

17.313
2

The Command-Line Interface

The command-line interface (CLI) follows the standard UNIX format for commands and options and provides complete Data Protector functionality. You can use these commands in scripts to speed up your commonly performed tasks.

The `omniintro` man page lists all supported Data Protector commands, as well as differences between commands on the UNIX and Windows platforms.

See also "Data Protector Commands" on page A-7.

RQS nº 03/2005 - CN
CPMI – CORREIOS
Fls Nº 1559
Doc 3702

17.512
2

Data Protector Online Resources

Information about Data Protector is available in this manual and in the online Help system. This manual contains the information you need to plan and administer your Data Protector network, and information on some more commonly performed tasks. The online Help system contains the information you need to perform all available tasks.

The following Data Protector online resources are available:

Help Topics	Online Help with task instructions and reference information. You can select topics by using the contents list, index, or search facility.
Help Navigator	Context-sensitive Help that provides detailed help on the current task.
Online Documentation	Online manuals in PDF format that can be read with the Adobe Acrobat Reader.
Data Protector on the Web	Opens your Web browser to the Data Protector homepage, where more information about Data Protector can be found.
Online Support	Opens your Web browser to the HP OpenView interactive Online Support service page.
About	Displays version and copyright information for Data Protector, as well as licensing information.

You can access the online resources by either using the `Help` drop-down menu or the `Help` buttons provided on the Data Protector windows.

Hyperlinks (cross-references) to additional information and definitions help you navigate through online Help. You click the hyperlinked word or phrase to jump to the new topic. Hyperlinked words and phrases are marked with either solid underlining or different color.

Starting and Using the Help Navigator

The Help Navigator provides context-sensitive online Help, which can be used to find information about the current GUI panel or task.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1560
3702

17311
L

If the GUI concerned is running on Windows, the Help Navigator is dynamic: Once it is started, its contents automatically change as you go to the next page of the wizard or to another view in the Data Protector user interface.

To start the Help Navigator, either:

- Press **F1**
- Click `Help Navigator` from the Help menu, or
- Click the Help Navigator icon (the question mark) on the button bar

Using the Online Manuals

Data Protector provides online manuals in PDF format that can be read using the Adobe Acrobat Reader. Once installed, the online manuals reside in the *<Data_Protector_home>*`\docs` directory (Windows) or the `/opt/omni/doc/C` directory (HP-UX or Solaris) on the Cell Manager system.

Using Microsoft Management Console (MMC)

On Windows systems, it is possible to integrate the Data Protector GUI with the Microsoft Management Console.

The `Microsoft Management Console (MMC)` is a Graphical User Interface (GUI) that lets you manage and run your administrative tools within a common interface environment. You can add already installed software, hardware, or network management applications to the console, where the primary type of tool that can be added to the console is called a **snap-in**.

The Data Protector snap-in, known as **OB2_Snap,** provides a basic integration of Data Protector and the MMC. Using OB2_Snap, you can go to the Data Protector home page or to Data Protector Web/Java Reporting. You can also start the Data Protector GUI on Windows from the MMC.

Proceed as follows to add **OB2_Snap** to the MMC.

1. Download the MMC software from http://www.microsoft.com/downloads/.
2. From the Windows desktop, click `Start`, and then select `Run`.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1561
Doc 3702

17310

3. In the Open text box, enter mmc to open the Microsoft Management Console window.
4. From the Console menu, select Add/Remove Snap-in. In the Standalone property page of the Add/Remove Snap-in window, click Add.
5. In the Add Standalone Snap-in window, select HP OpenView Storage Data Protector. Click Close to exit the window, then click OK to get back to the Microsoft Management Console window.

   The HP OpenView Storage Data Protector item will be displayed under Console Root. Once you have added the applications to MMC, save the file as *<Console_Name>*.msc.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1562
Nº 3702 Doc

17.309
L

Overview of Tasks to Set Up Data Protector

Although configuring Data Protector is easy, some advanced planning will help you configure the environment and optimize your backups. This section provides an overview of the global tasks to set up a backup environment.

Depending on the size and complexity of your environment, you may not need to go through all these steps.

1. Analyze your network and organizational structure. Decide which systems need to be backed up.

   For more information refer to the *HP OpenView Storage Data Protector Concepts Guide*.

2. Check whether there are any special applications and databases which you want to back up, such as Microsoft Exchange, Microsoft SQL, Oracle, SAP R/3, or others. Data Protector provides specific integrations with these products.

   Refer to the *HP OpenView Storage Data Protector Integration Guide* for instructions on how to configure the integrations.

3. Decide on the configuration of your Data Protector cell, such as the following:

   - System to be your Cell Manager
   - Systems on which you want to install the user interface
   - Type of backup - local backup versus network backup
   - Systems to control backup devices

4. Purchase the required Data Protector licenses for your setup. This way you obtain the passwords you need to have installed. Alternatively, you can operate Data Protector using an instant-on password. However, this is valid only for 60 days from the date of installation. Refer to the *HP OpenView Storage Data Protector Installation and Licensing Guide* for details.

5. Decide how you want to structure your backups:

   - Which media pools would you like to have, and how will they be used?

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1563
3702
Doc:

17 3C8
2

- Which devices will be used, and how?
- Which user groups do you want to have, and what will they do?
- How many backup specifications do you want to have, and how should they be grouped?

6. Install the Data Protector Cell Manager and Installation Server(s). Then use the Data Protector GUI to distribute Data Protector agents to other systems. Also, connect the devices (tape drives) to the systems that will control them. See the *HP OpenView Storage Data Protector Installation and Licensing Guide* for detailed instructions.
7. Configure the device(s). See Chapter 2, "Configuring and Using Backup Devices," on page 17.
8. Configure the pools and optionally prepare the media. See Chapter 4, "Managing Media," on page 97.
9. Set up the backup specifications, including scheduling. See Chapter 5, "Backup," on page 151.
10. Configure the IDB. See Chapter 9, "Managing the Data Protector Internal Database," on page 381.
11. Configure reports, if required. See Chapter 7, "Monitoring, Reporting, Notifications, and the Event Log," on page 307.
12. Consider preparing for disaster recovery if your disk fails. See Chapter 10, "Disaster Recovery," on page 435.
13. Become familiar with tasks such as:
    - How to work with failed backups
    - Performing restores
    - Testing disaster recovery
    - IDB maintenance

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1564
Nº 3702
Doc:

17.307
L

2 Configuring and Using Backup Devices

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1565
Nº Doc: 3702

17.306
2

In This Chapter

This chapter includes information on the following topics:

"Configuring Backup Devices" on page 20
"Configuring Standalone Devices" on page 23
"Configuring File Devices" on page 26
"Configuring Library Devices" on page 29
"Configuring Libraries with Multiple Systems" on page 32
"Configuring Magazine Devices" on page 34
"Configuring Stacker Devices" on page 35
"Configuring a Library for Mixed Media" on page 37
"Configuring Devices for Direct Backup" on page 38
"Support of New Devices" on page 41
"Using Several Drive Types in a Library" on page 42
"Configuring Magazine Devices" on page 34
"Shared Devices in the SAN Environment" on page 44
"Drive Cleaning" on page 61
"Busy Drive Handling" on page 65
"Activating Barcode Support" on page 66
"Activating Cartridge Memory Support" on page 68
"Disabling a Backup Device" on page 70
"Removing a Backup Device" on page 72
"Device Locking" on page 74
"Device Concurrency, Segment Size, and Block Size" on page 76

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1566
Doc: 3702

17305
L

NOTE Backup devices (like tape drives) are subject to specific Data Protector licenses. See the *HP OpenView Storage Data Protector Installation and Licensing Guide* for details.

RQS nº 03/2005 - CPMI - CORREIOS
1567
Fls Nº
3702

17.304
L

Configuring Backup Devices

Preparation of a backup device consists of connecting the device to the system and knowing which of the (working) associated device files (SCSI address) is to be used. To configure a device:

1. Connect the device to a computer. Refer to the documentation that comes with the device.
2. Make sure that you have done the following:

UNIX Systems

Create or find the device filename for a device connected to a UNIX system. For detailed steps, refer to the online Help index keyword "creating device filenames" or "finding device filenames". For further information, refer to Appendix B of the *HP OpenView Storage Data Protector Installation and Licensing Guide*.

Windows Systems

Provide a SCSI II address and load the driver that will be used with a device connected to a Windows system.

For tape drives, the Windows native tape driver can be:

- unloaded (preferred) or
- loaded

  The device filename depends on whether a Windows native tape driver is used with a particular tape drive.

On how to obtain the SCSI II address, refer to the online Help index keyword "creating SCSI addresses". For further information, refer to Appendix B of the *HP OpenView Storage Data Protector Installation and Licensing Guide*.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1568
3702
Doc:

17.303

Windows Robotics Drivers	On Windows, disable the Removable Storage Service or Windows medium changer (robotics) driver before you configure the robotics device with Data Protector. For detailed steps, refer to the online Help index keyword "robotics drivers". For further information, refer to Appendix B of the *HP OpenView Storage Data Protector Installation and Licensing Guide*.
Cartridge Memory	If your backup device is connected to a Windows system and uses media with Cartridge Memory, make sure that your SCSI II card supports execution of 16-byte CDB SCSI II commands. On the UNIX and Novell platforms, you need a tape driver which supports the respective SCSI II commands.

3. Boot the system to have the device recognized by the system.
4. Configure the device, as described in the following sections, so that you can use it with Data Protector.
5. Prepare the media that you want to use with your backups. On how to format media, refer to "Formatting Media" on page 108.

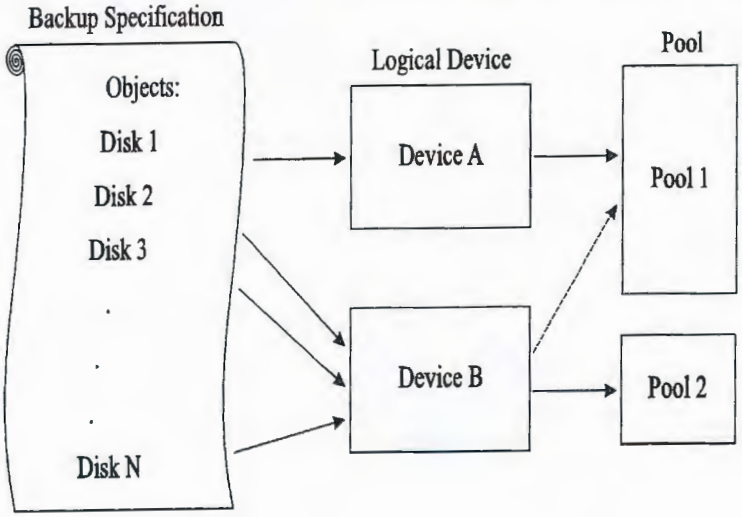
   A default media pool is used with each device so that you do not have to create one. If you want to create your own media pool, refer to "Creating a Media Pool" on page 102.

   Figure 2-1 shows the relationship between the backup specification, devices, and media pools. The devices are referred to in the backup specification, while each device is linked to a default media pool. This media pool can be changed in the backup specification.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1569
3702

17.802
L

Figure 2-1 **How Backup Specifications, Devices, and Media Pools Relate**



RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1570
3702

17 302

Configuring Standalone Devices

What Are Standalone Devices?

Standalone devices are simple backup devices with one drive that reads from or writes to one medium at a time. They are used for small-scale backups. When a medium is full, the operator has to manually replace it with a new medium so that the backup can proceed. Standalone devices are not appropriate for large, unattended backups.

Data Protector provides simple configuration and management of media used in standalone backup devices.

How to Configure a Standalone Device

Once you have prepared the device for configuration as described in "Configuring Backup Devices" on page 20, configure a standalone device so that you can use it with Data Protector. In the `Devices & Media` context, right-click `Devices` and click `Add Device`. In the `Add Device` wizard, specify the `Standalone` device type. Refer to Figure 2-2.

For detailed steps and examples, refer to the online Help index keyword "configuring standalone devices".

Data Protector supports a specific set of backup devices. Refer to the *HP OpenView Storage Data Protector Software Release Notes* for a detailed list of supported devices and their corresponding media types.

In case you want to use a device that is not in the list of supported devices, refer to "Support of New Devices" on page 41.

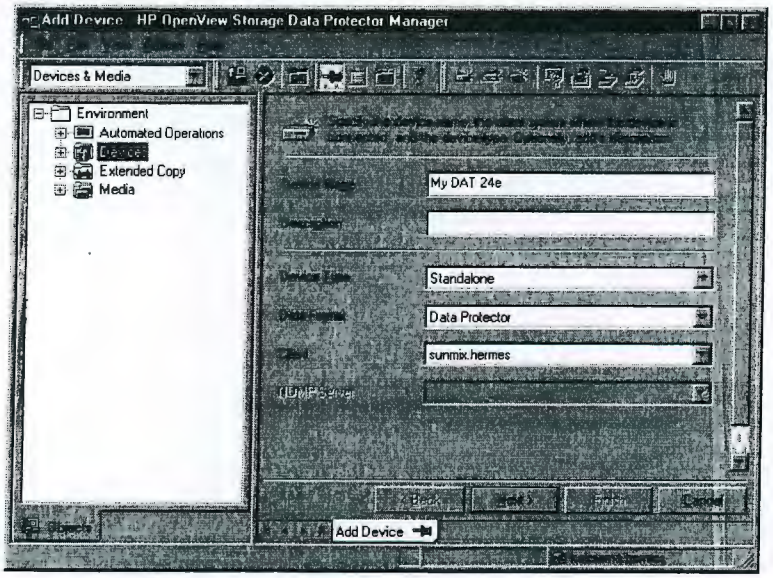
TIP

You can also let Data Protector automatically configure most common devices. You still need to prepare the media for a backup session, but Data Protector determines the name, policy, media type, media policy, and the device's SCSI II address or device file. For detailed steps, refer to the online Help index keyword "autoconfiguring backup devices".

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1571
Nº 3702
Doc:

17.300
2

Figure 2-2 **Specifying Device Type and Name**



Configuring Device Chains

Data Protector allows you to configure standalone devices of the same type into **device chains**. When a medium in one device becomes full, the backup automatically continues on the medium in the next device in the device chain. Device chains are possible for only one Media Agent, that is, you can connect a device chain to only one system.

The configuration is the same as for a standalone device, except that you enter multiple SCSI addresses (on Windows) or device filenames (on UNIX).

NOTE

The order in which the devices are added determines the order in which Data Protector uses them.

When all of the media in a device chain are full, Data Protector issues a mount request. The operator must replace the medium in the *first device* with a new medium, format it, and then confirm the mount request. Data

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1572
Nº 3702
Doc:

17.299
2

Protector can immediately use media that are recognized and unprotected. Data Protector can also use blank media, so that you do not have to format them.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1573
Nº 3702
Doc

17.298
2

Configuring File Devices

What Are File Devices?

A file device is a file in a specified directory to which you back up data instead of writing it to a tape. File devices are available for standalone devices and Jukebox devices simulation. The file device functionality is available on the Windows, HP-UX, Solaris, AIX, and Linux operating systems.

The default capacity of a file device is 100 MB for data and 10 MB for the catalog. The default segment size (for a 100 MB file device) is 30 MB.

The recommended segment sizes for specific file device sizes is:

Table 2-1 The Recommended Segment Sizes for Specific Device File Sizes

File size (GB)	Segment size (MB)
< 10	100
< 100	500
< 200	1000
< 300	1500
< 400	2000
< 500	2500

Data Protector never measures the amount of free space on the filesystem; it takes either the default or the specified capacity as the file size limit. If the disk on which the file device resides runs out of space, the backup will fail. The largest capacity specified for a file is 500 GB on Windows and 4 GB on UNIX systems.

Data Protector does not support using compressed files for file devices. You can change the default file size by changing the `FileMediumCapacity` parameter in the `<Data_Protector_home>\Config\Options\global` file on the Windows Cell Manager or in the `/etc/opt/omni/options/global` file on the HP-UX or Solaris Cell Manager.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1574
3702
Doc:

17.297
2

You specify the capacity of a file device when you first format the medium. When you reformat the medium, you can specify a new size; however, the originally specified size will be used. You can change the capacity of a file device only by deleting the file from the system.

The path to a file device can be anywhere, whether it is an internal drive or an external portable hard drive.

Handling Mount Requests

Media are handled differently from physical devices. When a standalone file device (medium) becomes full, Data Protector tries to write to the same file again. Data Protector does not recognize that any other file exists, so it issues a mount request.

When the mount request occurs, the existing file has to be moved or renamed (for example, by exchanging the ZIP media). The original file should no longer exist after the move. You then need to confirm the mount request. Data Protector will recreate the original file with the default file capacity. After the backup is finished, the file created by Data Protector contains the last part of the backup.

For Jukebox file devices, Data Protector issues a mount request when all media (files) are full.

Prerequisite

Before you configure a file device on a Windows system, disable the file compression option. This can be done using `Windows Explorer`. Right-click the file, select `Properties` and deselect `Compress` under `Attributes`. If `Compress` is selected, Data Protector will not be able to write to the file device.

IMPORTANT

Do not use the name of an existing file for configuring a file device, because the existing file will be overwritten.

Do not use the same filename for configuring several file devices, because every time a file device accesses the file, it will be overwritten.

How to Configure File Devices

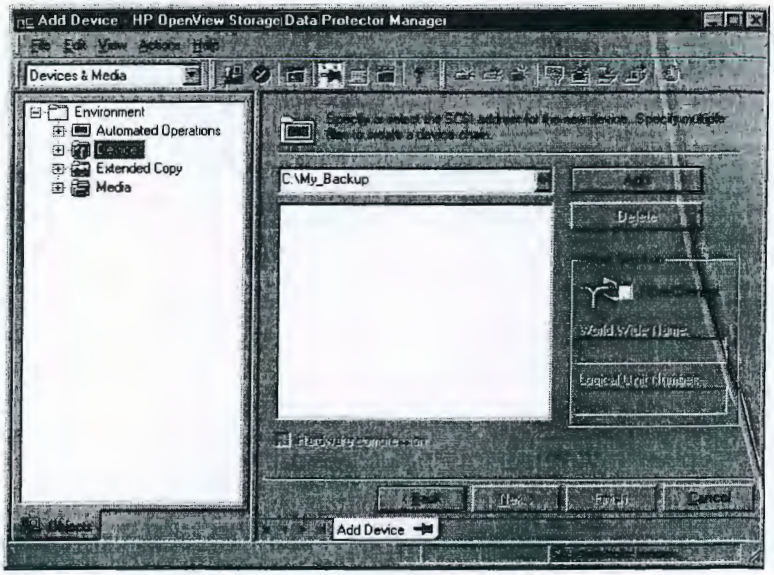
To create a standalone file device, specify the `Standalone` device type in the `Add Device` wizard. Refer to Figure 2-2. As a device address, specify a pathname for the file device, for example, `C:\My_Backup`. Refer to Figure 2-3. For detailed steps, refer to the online Help index keyword "configuring file devices".

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1575
Nº 3702
Doc:

17.296
L

To create a jukebox file device, specify the Jukebox device type in the Add Device wizard. As device addresses, specify different pathnames that will simulate jukebox slots. For detailed steps, refer to the online Help index keyword "configuring file devices".

Figure 2-3 **Specifying a Pathname for a File Device**



RQS nº 03/2005
CPMI - CORREIOS
1576
Fls Nº
3702
Doc:

17.295
L

Configuring Library Devices

What Are Library Devices?

SCSI-II library devices, also called autoloaders, are large backup devices. They contain a number of media cartridges in a device's repository and can have multiple drives handling multiple media at the same time. Most library devices also allow you to configure automatic drive cleaning, which is performed by Data Protector when the drive gets dirty. Refer to "Drive Cleaning" on page 61.

A library device has a SCSI ID for each drive in the device, and one for the library robotic mechanism. This mechanism moves media from slots to drives and back again. For example, a library with four drives has five SCSI IDs, four for the drives and one for the robotic mechanism.

Slot Number

Each slot in the device's repository holds one medium. Data Protector assigns a number to each slot, starting from 1. When managing a library, you refer to the slots using their numbers. For example, a library with 48 repository slots has slot numbers 1, 2, 3, 4, 5, 6...47, 48.

Drive Index

The drive index identifies the mechanical position of the drive in the library. Refer to Figure 2-4.

The index number is relevant for the robotics control. The robot knows only index numbers and has no information about the SCSI address of the drive. The drive index is a sequential integer (starting from 1) which has to be coupled with the SCSI address of this drive. For example, for a four-drive library, the drive indexes are 1,2,3,4.

If you have only one drive in the library, the drive index is 1.

Drive SCSI Address

The drive index must match the corresponding SCSI address. This means that you need to configure the pairs as follows:

SCSI address_A for index 1,
SCSI address_B for index 2, and so on.

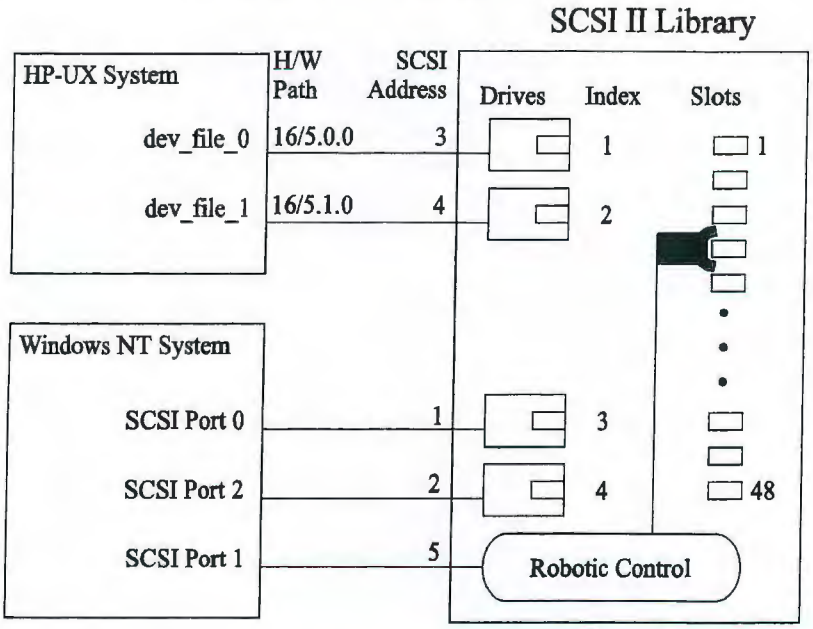
RQS nº 03/2005 - CN -
CPMI - CORREIOS
1577
Fls Nº 3702
Doc:

17.294
2

NOTE

It is not necessary to configure all drives for use with Data Protector. You can configure one media pool for all drives, or have an independent media pool for each drive. It is recommended that you use the default media pool when configuring a device.

Figure 2-4 **Drive Index to SCSI Address Mapping**



How to Configure a Library Device

Once you have prepared the device for configuration as described in "Configuring Backup Devices" on page 20, configure a library device, including its drive(s). The `Add Device` wizard guides you through both configurations. For detailed steps and examples, refer to the online Help index keyword "configuring SCSI libraries".

TIP

You can also have Data Protector automatically configure the library devices for you. You still need to prepare the media for a backup session, but Data Protector determines the name, policy, media type, media

RQS nº 03/2005 - CN -
CPMI - CORREIOS
1578
Fls Nº
3702

17.243
2

policy, and the device file or SCSI address of the device, and also configures the drive and slots. For detailed steps, refer to the online Help index keyword "autoconfiguring backup devices".

To verify the device configuration, right-click the created drive, and choose `Scan Medium`. If the device is configured correctly, Data Protector will be able to load, read, and unload media in the slots.

What's Next?

If you have configured all the backup devices you want to use with Data Protector, do the following:

- Add media to the media pools that you will use with the newly configured device. Refer to "Adding Media to a Media Pool" on page 107.
- If you want to configure a cleaning tape, refer to "Drive Cleaning" on page 61.
- If your device uses barcodes, refer to "Activating Barcode Support" on page 66.
- Configure a backup for your data. Refer to Chapter 5, "Backup," on page 151.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1579
Doc: 3702

17.292
L

Configuring Libraries with Multiple Systems

You can configure a library so that each drive receives data from a different system running a Data Protector Media Agent. The library robotics control is still performed by one system. This improves performance in high-end environments by allowing local backup, instead of having to move the data over the network.

Prerequisites

- Each client system that you want to use with the drives in the library must have the Data Protector Media Agent component installed.
- You need to have connected the backup device to the system, and a working device file (SCSI address) must exist before you can configure the device for use with Data Protector.

For more information on multi-drive support, see the *HP OpenView Storage Data Protector Concepts Guide*.

How to Configure Libraries with Multiple Systems

Configure a library as described in "Configuring Library Devices" on page 29. When you are prompted to configure drives in the library, specify the client system that you want to use with each drive. For detailed steps, refer to the online Help index keyword "configuring libraries for multiple systems".

TIP

To verify the device configuration, select a range of slots from the library and then click `Scan` from the `Actions` menu. If the device is configured correctly, Data Protector will be able to load, read, and unload media back into the slots.

What's Next?

If you have configured all the backup devices you want to use with Data Protector, do the following:

- Add media to the media pools that you will use with the newly configured device. See "Adding Media to a Media Pool" on page 107.
- If you want to configure a cleaning tape, see "Drive Cleaning" on page 61.
- If your device uses barcodes, see "Activating Barcode Support" on page 66.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1580
Doc: 3702

17.289
L

Configuring Stacker Devices

What Are Stacker Devices?

A stacker is a single device with one drive and sequentially accessed media. Using stacker devices requires more human media management than using a small library. Data Protector provides simple configuration and management of media used in stacker backup devices.

How to Configure a Stacker Device?

To create a stacker device, specify the `Stacker` device type in the `Add Device` wizard. For detailed steps, refer to the online Help index keyword "configuring stacker devices".

Stacker Device Media Management

The operations scan, verify, or format have to be run separately on each medium in a stacker device. When performing these operations, use the `Eject medium after operation` option, in order to have each medium loaded automatically (only the first medium should be loaded manually). When all the tapes in the stacker magazine are used, the magazine must be unmounted manually and the next one inserted.

Stackers load media in sequential order, therefore a `Loose` media allocation policy is recommended. A `Strict` policy would require media to be loaded in the same order as they are to be used.

Example

1. Manually load the first medium.
2. Run format/verify/scan (with `Eject after operation` enabled) -- (next tape will be loaded automatically).
3. Repeat step 2 until all tapes are finished.
4. When all the tapes in the stacker magazine are used, unmount the magazine manually and insert the next one.

NOTE

If a medium is not properly loaded, Data Protector will abort the medium session.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1581
Nº Doc: 3702

17.288
2

Backup and Restore with Stacker Devices

Only the first medium has to be manually loaded. When a tape is full, it is ejected and the next tape is loaded automatically. When all the tapes are used in a stacker magazine, the magazine has to be unmounted manually and the next one has to be inserted. Again the first tape has to be loaded manually into the drive.

NOTE

A backup or restore session will not be aborted if media are not present, but a mount request will be issued instead. The whole session will not be aborted if a user does not change stacker magazines within a time out period.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1582
Doc: 3702

17.287
2

Configuring a Library for Mixed Media

A mixed media library contains media of several types, such as DLT and magneto-optical. It uses identical robotics to move all the media (regardless of media type) between slots and drives.

In order to use this library functionality, configure several (sub)libraries: one library definition per media type.

To take full advantage of this feature, perform the following steps:

- Configure at least one media pool (or use the default pool) per media type.
- Configure the library robotics once per media type, including the slot range for that media type. Make sure the robotics control (SCSI path on Windows systems or device file on UNIX systems) for each of the library robotic definitions resides on the same host and that they are identical.
- Configure all the drives for a media type and link them to the related library robotic and media pool. Make sure the drive index is unique for each physical device, regardless of media type.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1583
3702
Doc:

17.286

Configuring Devices for Direct Backup

This section provides the configuration steps for backup devices used in a direct backup environment. Refer to the *HP OpenView Storage Data Protector Concepts Guide* for a more detailed information on direct backup concepts.

Direct backup is a Data Protector backup solution in a SAN environment. Please read the section "Shared Devices in the SAN Environment" on page 44 for general information on SAN environments. Note that the direct backup device configuration steps differ from the configuration steps described in the mentioned section, and are given in this section.

A direct backup environment consists of the following:

- a SAN network
- internal or external Fibre Channel bridge(s) (FC bridge)
- backup device(s) connected to FC bridge(s) (standalone or SCSI-II library)
- physical XCopy engine(s) (present on an FC Bridge)
- disk array(s) assuring point-in-time stability of data (HP StorageWorks Disk Array XP or HP StorageWorks Virtual Array)
- application system(s) connected to the disk array original disk(s)
- backup system(s) connected to the disk array mirror disk(s) and controlling the SCSI-II library robotics and SCSI-II library/standalone device drives

An internal FC bridge is embedded in the backup device, whereas an external FC bridge resides at any point in the SAN.

A backup device used in the direct backup environment is identified by the World Wide Name (WWN) of the Fibre Channel bridge that it is connected to or embedded in the backup device, and by the device (standalone device) or drive (SCSI-II library) Logical Unit Number (LUN) as seen on the SAN. If a SCSI-II library is used, its robotics does not have to be connected to a FC bridge.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1584
3702
Doc:

17.285
2

Backup Device Auto-detection

The XCopy engine must reside on the FC bridge to which the backup device or drive is connected (external FC bridge), or on the internal FC bridge. A backup device that is used with direct backup functionality is auto-detected whenever a direct backup session is started. If auto-detection is not used, the WWN and the LUN parameters must be entered manually; the LUN must be reconfigured every time the LUN changes.

XCopy Engine

There can be more than one physical XCopy engine in a direct backup environment. Each of these physical XCopy engines can have more logical XCopy engines configured and assigned. Which of these logical XCopy engines will be used in a direct backup session is specified in the direct backup specification by specifying the backup device(s) to be used and assigning them a logical XCopy engine. The physical XCopy engine behind the logical XCopy engine specified in the backup specification must be configured for the backup system specified in the backup specification.

The following types of backup devices are supported for a Data Protector direct backup:

- standalone devices
- SCSI-II libraries

Configuration Procedure

Refer to the following online Help index keywords and perform any necessary steps before configuring backup devices as described later in this section:

- online Help index keyword "preparing backup devices"
- online Help index keyword "configuring direct backup environment"

Configuring a backup device for direct backup consists of the following:

1. Configuring a standalone device or SCSI-II library.
2. Configuring XCopy engines.
3. If direct library access will be used, configuring the `libtab` file.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1585
3702
Doc:

17.284
L

Configuring Standalone Devices

Refer to the online Help index keyword "configuring standalone devices for direct backup" for detailed information on how to configure a standalone device for a direct backup.

Configuring SCSI-II Libraries

Refer to the online Help index keyword "configuring SCSI-II libraries for direct backup" for detailed information on how to configure a SCSI-II library for a direct backup.

Configuring XCopy Engines

Refer to the online Help index keyword "configuring XCopy engine" for detailed information on how to configure an XCopy engine.

Configuring the libtab File

Configuration of the `libtab` file is necessary only if direct library access is to be used.

Refer to the "Manually Configuring the libtab Files" on page 56 for detailed information on how to configure the `libtab` file.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1586
Doc: 3702

17.283

Support of New Devices

To use a device that is not listed as supported in the *HP OpenView Storage Data Protector Software Release Notes*, download the latest software package for the `scsitab` file from the HP OpenView World Wide Web site at http://www.hp.com/go/dataprotector.

IMPORTANT Modifying the `scsitab` file is not supported.

After you have downloaded the `scsitab` software package, follow the installation procedure provided with it.

The `scsitab` file must be located on the system to which the device is connected, in the following location:

- *<Data_Protector_home>*`\scsitab` on Windows platforms
- `/opt/omni/scsitab` on HP-UX and Solaris platforms
- `/usr/omni/scsitab` on other UNIX platforms

If you receive an error message while configuring your device, please contact HP Support to get information about when the device will be supported.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1587
3702

17.282
2

Using Several Drive Types in a Library

Using several drive types of a similar technology like DLT 4000/7000/8000 (the same is true within the DDS family) in the same library can lead to problems when you use the media in any drive, but do not ensure a common format on all media.

For example, at restore time, a DLT 4000 cannot read a tape that has been written with a DLT 8000 (highest density). Compressed and non-compressed media cannot be used interchangeably.

To avoid these kind of problems, you can either use a common density setting for all your media, or you can separate your media pools. Both of these solutions are described in the following sections.

Same Density Setting

This method uses a common format on all media, which allows you to use all media interchangeably in any drive.

For devices used on Windows systems, consult the drive documentation for information about using a specific write density.

On UNIX systems, you can set the density for drives by selecting the related device filenames and using them in the device definitions. The density must be set at the same value. For example, in case of DLT 4000 and DLT 7000 drives, the DLT 4000 drive density should be set.

Make sure the block size setting of the devices used is the same. This setting in the device definition must be used at the time the media are formatted.

The free pool concept can be used as desired.

During a restore, any drive can be used with any media.

On HP-UX, you can set the density of a drive when creating the device filename. See Appendix B, "Creating the Device Files on HP-UX", in the *HP OpenView Storage Data Protector Installation and Licensing Guide* for more information.

Different Media Pools (on UNIX and Windows)

This method separates the media used by one group of drives from the media used by another group of drives, allowing you to better optimize drive and media usage.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1588
Doc: 3702

17.281
L

On Windows and UNIX systems, you can configure separate media pools for different groups of drives. This allows you to use different density settings for different drive types. For example, you could create a DLT 4000 pool and a DLT 8000 pool.

The related setting in the device definition must be used at the time the media are formatted. For example, the media in the pool for the DLT 8000 highest density must be formatted by a DLT 8000 in highest density setting.

The free pool concept cannot be used across such pools. This would not identify media from the other pool to the devices correctly; they would be seen as "foreign" media. The free pool concept can at most be used only in a single pool (like the DLT 8000 pool), in case the same media type (DLT) is written in an incompatible way.

Care must be taken during restore, since media from a given pool can only be used with related devices.

To configure new media pools, refer to the online Help index keyword "configuring media pools".

To modify media pool settings for a drive, modify the drive properties. For detailed steps, refer to the online Help index keyword "modifying, media pools".

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1589
Doc 3702

17.280
D

Shared Devices in the SAN Environment

This section describes some of the basic concepts of Storage Area Networks (SANs). For further conceptual information, see the *HP OpenView Storage Data Protector Concepts Guide*.

The concepts and instructions provided here are the following:

- Device locking when the library is accessed exclusively by Data Protector
- Using the Data Protector user interface to configure the library robotics and drives
- Locking library robotics and drives
- Direct versus indirect library access

What Is a SAN?

A Storage Area Network (SAN) is a network dedicated to data storage, based on high-speed Fibre Channel technology. A SAN lets you offload storage operations from application servers to a separate network. Data Protector supports this technology by enabling multiple hosts to share storage devices connected over a SAN, which allows multiple systems to be connected to multiple devices. This is done by defining the same physical device multiple times, for example, once on every system that needs access to the device.

Key Concepts

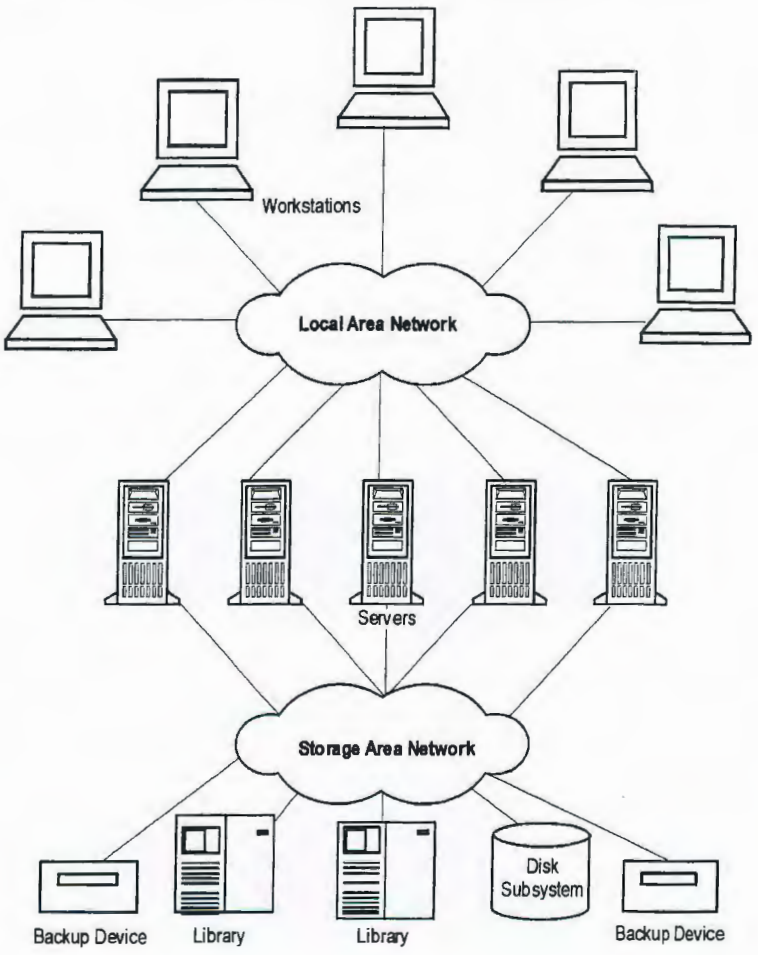
There are some key concepts to consider when using Data Protector in a SAN environment:

- Each system can have its own (pseudo-)local device, although the devices are typically shared among several systems. This applies to individual drives, as well as to the robotics in libraries.
- Take care to prevent several systems from writing to the same device at the same time. Access to devices needs to be synchronized between all systems. This is done using locking mechanisms.
- SAN technology provides an excellent way of managing library robotics from multiple systems. It creates the ability to manage the robotics directly, as long as the requests sent to the robotics are synchronized among all the systems involved.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1590
Doc: 3702

17.279
L

Figure 2-5 **Multiple System to Multiple Device Connectivity in SAN**



RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1591
3702
Doc:

17.277

Direct Library Access Concept

With direct library access, every system sends control commands directly to the library robotics. Therefore, a system does not depend on any other system in order to function.

With direct library access , when multiple systems send commands to the same library, the sequence of such communication has to be coordinated. Therefore, every library definition is associated by default with a host controlling the library robotics. If another host requests that a medium be moved, Data Protector will first access the system specified in the library definition for performing the move. If the system is not available, direct access from the local host to the library robotics is used if the `libtab` file is set. All of this is done in a transparent manner within Data Protector.

Indirect Library Access Concept

With indirect library access, only one system (the default robotics control system) sends robotic control commands that are initiated from Data Protector. Any other system that requests a robotics function forwards the request to the robotics control system, which then sends the actual command to the robotics. This is the default setting, and is done in a transparent manner within Data Protector for all requests from Data Protector.

Configuration Overview

This section provides an overview of the steps involved in configuring your system. It includes the following topics:

- Configuration goals

  This section specifies the mixed SAN environment to be configured.

- Configuration methods

  This section outlines the configuration methods that need to be performed for UNIX, Windows, and mixed SAN environments.

- Autoconfiguring the devices

  This section outlines the device autoconfiguration specifics in a SAN environment.

- Manually configuring the robotics

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1592
Doc. 3702

17.272

Prerequisite

Before configuring Data Protector devices in a SAN environment, the Data Protector Media Agent must be installed on each host that needs to communicate with the shared library. See the *HP OpenView Storage Data Protector Installation and Licensing Guide* for more information on installing a Media Agent.

Configuring the Library Robotics

To create the library itself, refer to "Configuring Library Devices" on page 29 or to the online Help topic "Configuring Devices in a SAN Environment".

For robotics control, you can use any host within the SAN; here the system `dupin.company.com` is used. The library robotics will be controlled by that host, unless the host is unavailable and direct access is enabled as explained in detail in "Enabling Direct Access" on page 55.

Configuring the Library Robotics in a Cluster

If you want the robotic control to be managed by a cluster, you need to make sure that:

- The robotics control exists on each cluster node.
- The virtual cluster name is used in the library robotics configuration.
- The common robotics and device filenames are installed either using the `mksf` command or using the `libtab` file. For information on how to configure the `libtab` file, refer to "Manually Configuring the libtab Files" on page 56.

After you have configured the library robotics, create the drives.

Manually Configuring the Devices (Drives)

You need to configure each device (tape drive) on each host from which you want to use the device.

`Lock Names` must be used to prevent the same device from being used by several hosts at the same time. Optionally, the "direct access" mode can be selected.

Configuring Drives

As will be seen shortly, it helps to follow a drive naming convention similar to the following:

`LibraryLogicalName_DriveIndex_Hostname`, for example `SAN_LIB_2_computer_1`.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1593
Doc 3702

17.271
2

The drive naming convention shows its benefits during backup specification creation. Whenever you configure a backup on any host, all you have to do now is to use the drive that is configured on that host, since the drive includes the host name in its name.

Table 2-2 **Device Locking for Drives**

Environment Conditions	Required Action
The drive is used by only one system and Data Protector only	No locking is necessary. Leave the fields blank, for example, `Lock Name` = blank
The drive is used by several systems (SAN), Data Protector is the only application accessing the drive	Use device locking (define a `Lock Name`) as described in the section "Device Locking" on page 74
The drive is used by several systems and several applications (not only by Data Protector)	Use device locking (define a `Lock Name`) and ensure that operational rules provide exclusive access to all devices from only one application at a time

Defining Lock Names

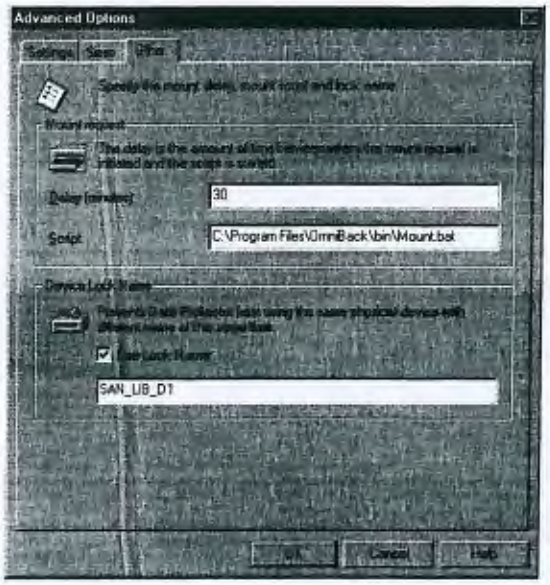
Using `Lock Names` is necessary in a SAN environment. This prevents collisions on the device caused by several systems talking to it at the same time. It is recommended to use the following convention for `Lock Names`:

`LibraryLogicalName_DdriveIndex`, for example `SAN_LIB_D1`.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1594
3702
Doc:

17270

Figure 2-7 **Setting Advanced Options**

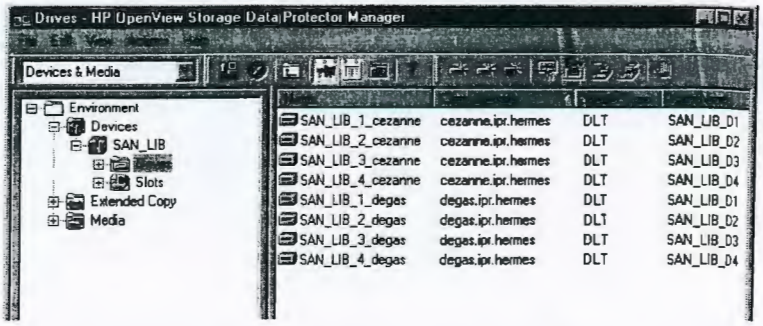


When you are setting the locking name of a drive, use the same lock name for the same physical drive when using it in the device definition on another host.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1595
Doc. 3702

17.269

Figure 2-8 **Summary of Device Definitions Using Lock Names**



Enabling Direct Access

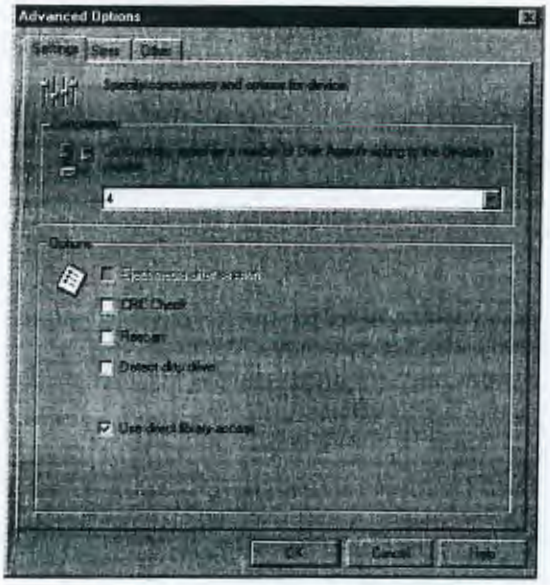
The Direct Access mechanism always uses the default robotics control host first for media movements, but if this fails, Data Protector uses direct access, if enabled.

To enable direct access, select the `Use direct library access` option (see Figure 2-9 on page 56) and configure the `libtab` file on every host on which you want to use direct access.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1596
Doc: 3702

17.268

Figure 2-9 **Selecting Direct Access**



Manually Configuring the libtab Files

The purpose of the `libtab` files is to map the library robotic control access so that it also works on the "direct access requesting system", since here the local control path is likely to be different from the one used on the default library robotic control system.

You need to create a `libtab` file for every Windows and UNIX system client host that needs "direct access" to the library robotics, and is not identical to the system configured as the default library robotics control system.

On each system requesting direct access, a plain text file with the following format must be provided:

<FullyQualifiedHostname> <DeviceFile | SCSIPath> <DeviceName>

- *<FullyQualifiedHostname>* is the name of the client host demanding direct access control for the library robotics. If the host is part of a cluster, the node name should be used.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1597
3702
Doc:

17.267
2

- *<DeviceFile | SCSIPath>* is the control path to the library robotic driver on this client host.
- *<DeviceName>* is the name of the device definition used on this client host.

You need one line per device for which you request direct access.

The `libtab` file is located on:

- *<Data_Protector_home>*`\libtab` on Windows systems
- `/opt/omni/.libtab` on HP-UX and Solaris systems
- `/usr/omni/.libtab` on other UNIX systems

Example files follow for all systems involved. Definitions are separated by blank lines, which are ignored. Since the default library robotics are defined on the host `dupin.company.com`, no `libtab` file is needed on this system.

TIP

It is possible to have only one `libtab` file that includes definitions for all systems involved and is distributed to all such systems. In this case, when a specific system needs "direct access" to the library robotic, the definitions for other systems are ignored and only the definitions for the system are used.

Example `libtab` file on zala

Example of the `libtab` file on host zala.company.com (Windows):

```
zala.company.com  scsi:2:0:2:0  SAN_LIB_1_zala
zala.company.com  scsi:2:0:2:0  SAN_LIB_2_zala
zala.company.com  scsi:2:0:2:0  SAN_LIB_3_zala
zala.company.com  scsi:2:0:2:0  SAN_LIB_4_zala
```

Example `libtab` file on oda

Example of the `libtab` file on host oda.company.com (HP-UX):

```
oda.company.com  /dev/spt/lib  SAN_LIB_1_computer_2
oda.company.com  /dev/spt/lib  SAN_LIB_2_computer_2
oda.company.com  /dev/spt/lib  SAN_LIB_3_computer_2
oda.company.com  /dev/spt/lib  SAN_LIB_4_computer_2
```


RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1598
Doc. 3702

17.266
L

Example `libtab` file on donat

Example of the `libtab` file on host donat.company.com (Solaris):

```
donat.company.com /dev/rsst6 SAN_LIB_1_sample
donat.company.com /dev/rsst6 SAN_LIB_2_sample
donat.company.com /dev/rsst6 SAN_LIB_3_sample
donat.company.com /dev/rsst6 SAN_LIB_4_sample
```

NOTE

If the host is part of a cluster, `<FullyQualifiedHostname>` must be the virtual host name, and `<DeviceFile | SCSIPath>` must refer to the local node.

Shared Devices and MC/ServiceGuard

If you are using Data Protector with MC/ServiceGuard for clustering, you can implement the integration in a SAN environment. Since clustering is based on sharing resources such as network names, disks, and tapes among nodes, Fibre Channel and SAN are well suited as enabling technologies for storage device sharing. ATS (Advanced Tape Services) is an integrated part of HP MC/ServiceGuard 11.05 that manages tape resources and enables the use of Data Protector in a SAN environment.

This section explains how to create the necessary device files, how to configure the virtual host, how to configure static and floating drives, and how to use the Data Protector GUI to configure the integration for use in a SAN environment.

Configuration Basics

Nodes in a cluster can share SAN-connected devices in order to perform a "LAN-free" backup of an application running in a cluster. Cluster-aware applications can, at any time, run on any node in a cluster since they run on the virtual host. In order to perform a LAN-free local backup of such an application, you need to configure the logical device with a virtual hostname instead of a real node name.

You can configure as many logical devices for a single physical device as you need, but you have to use the same `Lock Name` for all devices.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1599
Doc 3702

17.265
L

In order to share a device among multiple systems, configure one logical device for each system on which you want to use the device locally.

NOTE Before the ATS component can be configured, the MC/ServiceGuard configuration has to be completed and a cluster has to exist.

Refer to the following documents for detailed information:

- B3936-90032 *Using Advanced Tape Services* (MC/ServiceGuard documentation)
- B3935-90015 *MC/ServiceGuard Version A.11.05 Release Notes*
- B3936-90026 *Managing MC/ServiceGuard*, Sixth Edition

Creating the ATS Configuration Files

Run the `stquerycl` command to gather the configuration of all attached tape devices and robotic control. This will create the configuration file. The configuration file includes the following new device file names and a usage policy for all devices:

- `dev/rmt/st#m`

  for tape device files
- `dev/rac/sac#`

  for robotic control devices

The configuration files should be the same on all nodes for the same physical device. Both the robotics and drive files should be included.

Configuring Drives

Floating Drives Drives that should be accessible from both hosts, depending on which host the package is running, have to be configured based on the virtual host.

Table 2-3 How to Configure a Floating Drive

Hostname	`node_Appl`
Device Control Path	`/dev/rmt/st3m`

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1600
3702
Doc:

17.264

Table 2-3 **How to Configure a Floating Drive**

Lock Name	`Lib1_Drive_1`

Static Drives

The drives can still be used in the standard way using the static hostname and the local device file. (You can use the local HP-UX or ATS device file.) The local drives should be configured on the node. For example:

Table 2-4 **How to Configure a Static Drive**

Hostname	`Host_A`
Device Control Path	`/dev/rmt/0m`
Lock Name	`Lib1_Drive_1`

The previous examples for floating and static drives show the device identified by `/dev/rmt/0m` and `/dev/rmt/st3m`. Both device files refer to the same physical devices, and therefore the lock name (`Lib1_Drive_1`) is identical.

RQS nº 03/2005 - CN - CPMI - CORREIOS
1601
Fls Nº
3702
Doc:

57.263

Drive Cleaning

There are several methods for cleaning dirty drives:

- Library built-in cleaning mechanism

  Some tape libraries have a functionality for cleaning drives automatically when a drive requests head cleaning. When the library detects a dirty drive, it automatically loads a cleaning tape. However, Data Protector is not notified of this action. This interrupts any active session, causing it to fail.

  This hardware-managed cleaning procedure is not recommended, since it is not compatible with Data Protector. Use automatic drive cleaning managed by Data Protector instead.

- Automatic drive cleaning managed by Data Protector

  Data Protector provides automatic cleaning for most devices using cleaning tapes. For SCSI-II libraries and magazine devices, you can define which slots contain cleaning tapes. A dirty drive sends the cleaning request, and Data Protector uses the cleaning tape to clean the drive.

  This method prevents failed sessions due to dirty drives, provided that suitable media are available for backup. Refer to "Configuring Automatic Drive Cleaning" on page 62.

- Manual cleaning

  If automatic drive cleaning is not configured, you need to clean the dirty drive manually. If Data Protector detects a dirty drive, a cleaning request appears in the session monitor window. You then have to manually insert a cleaning tape into the drive.

A special tape-cleaning cartridge with slightly abrasive tape is used to clean the head. Once loaded, the drive recognizes this special tape cartridge and starts cleaning the head.

Limitations

- Data Protector does not support the diagnostic vendor-unique SCSI command for performing drive cleaning with cleaning tapes stored in one of the special cleaning tape storage slots. These special cleaning tape storage slots are not accessible using the normal SCSI commands, and therefore cannot be used with the automatic drive cleaning managed by Data Protector. Configure the standard slot(s)

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1602
3702
Doc:

to store cleaning tape(s).

- Detection and use of cleaning tapes depends on the system platform where the Media Agent is running. See the *HP OpenView Storage Data Protector Software Release Notes* for further information.
- You should not use another kind of device management application if you configure automatic drive cleaning managed by Data Protector, as this may cause unexpected results. This is due to the "cleanme" request being cleared as it is read, depending on the specific device type and vendor.
- Automatic drive cleaning for logical libraries with a shared cleaning tape is not supported. Each logical library needs to have its specific cleaning tape configured.

Conditions for Automatic Cleaning

Automatic drive cleaning is supported for libraries with barcode support, as well as for those without barcode support.

The following conditions must be met for automatic cleaning:

- In a library without barcode support, a cleaning-tape slot has been configured in the Data Protector device definition and contains a cleaning-tape cartridge. The cleaning-tape slot must be configured together with the other library slots.
- In a library with barcode support, the cleaning tape has a barcode label with "CLN" as its prefix. Further, barcode support must be enabled. Refer to "Activating Barcode Support" on page 66.
- The configured drive has the `Detect Dirty Drive` option enabled.

When Data Protector receives notification that the drive needs cleaning, it automatically loads the cleaning tape, cleans the drive, and then resumes the session.

All cleaning activities are logged in the following file:

- on Windows: `<Data_Protector_home>\log\cleaning.log`
- on UNIX: `/var/opt/omni/log/cleaning.log`

Configuring Automatic Drive Cleaning

The configuration of automatic drive cleaning is performed in two steps:

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1603
3702
Doc:

17.261

1. Enable dirty drive detection. This needs to be done for all device types (standalone and libraries). This enables Data Protector to recognize the event issued by the drive.
2. Configure a slot for the cleaning tape in the library or magazine device.

Enabling Dirty Drive Detection

To enable dirty drive detection, select the `Detect dirty drive` advanced option in the `Settings` property page for the drive. For detailed steps, refer to the online Help index keyword "configuring drive cleaning".

Configuring a Slot for Cleaning Tape

To configure a slot for a cleaning tape in a SCSI-II library, click the `Cleaning Slot` option and select an existing slot in the drop-down list in the `Repository` property page for the device. For detailed steps, refer to the online Help index keyword "configuring drive cleaning".

Testing the Drive Cleaning Configuration

To test if drive cleaning has been successfully configured, do the following:

Preparation

1. Log on to the system where the Media Agent for the drive is installed.
2. Change to the Data Protector `tmp` directory:
   - on HP-UX and Solaris systems: `/var/opt/omni/tmp/`
   - on other UNIX systems: `/usr/omni/tmp/`
   - on Windows systems: *<Data_Protector_home>*`\tmp\`
   - on Novell NetWare systems: `\usr\omni\tmp\`
3. Create an ASCII file named `simtab` on Windows systems or `.simtab` on UNIX systems. Consider the following when creating this file:
   - The field separators should be a single ASCII character (tab or space)
   - The logical device name cannot be quoted and cannot contain spaces (e.g. "test drive")

   The content of the `simtab/.simtab` file should be the following:

   `CLEANME` *<file_name>* *<drive_name>*

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1604
Doc: 3702

17.260

Where *<file_name>* is the name of the file you will use to simulate a dirty drive, and *<drive_name>* is the name of the drive you want to test.

You can add multiple entries for various drives. Do not add any directories in front of the name of the file.

Testing the Configuration

In order to test your configuration, do the following:

1. In the Data Protector `tmp` directory, create an empty file that will be used to simulate a dirty drive. Use the same name as in the `simtab` or `.simtab` file.
2. Start a backup using the drive you are testing.

Data Protector behaves as though the selected drive were dirty and performs the cleaning action.

To stop simulating dirty drive behavior for the specific drive, delete the file used for simulation.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1605
Nº 3702
Doc:

17.259
L

Busy Drive Handling

Data Protector expects drives to be empty, i.e., there should not be a medium in the drive unless a restore or backup is currently active. Several factors can cause a medium to still be in a drive, for instance, if the medium was used with a different application and not removed, or if the system writing the data to the tape (Media Agent) failed during the backup. The next backup using this drive has to deal with this situation. Data Protector can respond automatically in several ways. The response is configurable via the library option `Busy Drive Handling`.

The following options are available:

Abort The backup will be aborted (default).

Eject Data Protector will eject the medium from the drive and put it in any empty slot.

Eject to mail slot Data Protector will eject the medium from the drive and put it in the library mailslot (CAP).

If the backup continues automatically, select **Eject**. Because the tape is moved to an unknown slot, the library should be scanned before the next backup.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1606
Doc: 3702

17.258

Activating Barcode Support

If a SCSI library device uses media with barcodes, Data Protector can use barcodes by providing the following support:

- Recognition of cleaning tapes with a CLN prefix.
- Reference to media by their barcodes. Data Protector adds the media barcode to the Data Protector media label.
- Quickly scanning the media in the slots of the library repository using media barcodes. This is considerably faster than scanning a repository without the barcode functionality. In the `Action` menu, click `Barcode Scan` to scan the library repository for media.

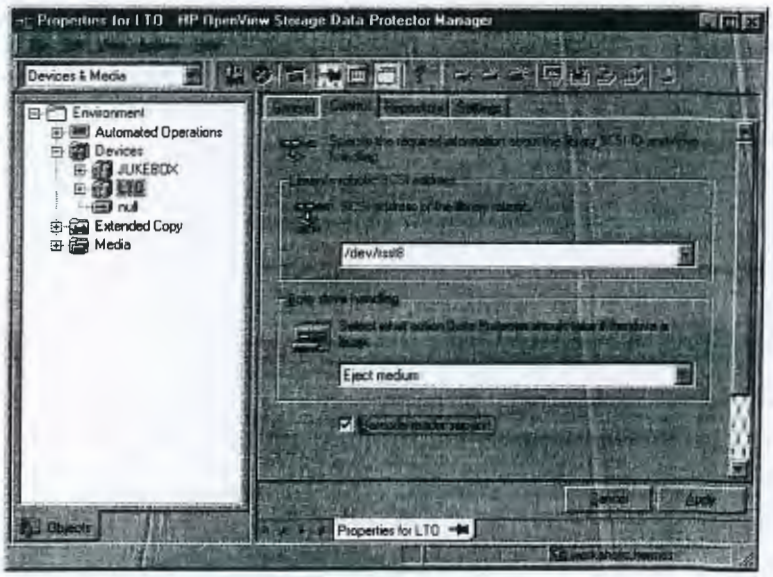
Activate barcode support by selecting the `Barcode reader support` option from the `Control` property page of the device. Refer to Figure 2-10 on page 67. For detailed steps, refer to the online Help index keyword "activating barcode reader support".

NOTE All barcodes in a cell should be unique, regardless of the type of media or the fact that there are multiple libraries.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1607
Doc: 3702

17.257
L

Figure 2-10 **Activating Barcode Reader Support**



RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1608
Doc: 3702

17.253

Activating Cartridge Memory Support

Cartridge memory support can be activated for drives with the LTO-Ultrium media type. It provides the following:

- Updating or changing media management information, such as medium label, medium location and pool name, and media usage information. The latter includes date of last access, date of last write, and number of writes.
- Importing of media that include information stored in Cartridge Memory.
- Listing all Cartridge Memory contents for the specific medium.
- Reformatting Cartridge Memory of a specific medium from the GUI and CLI in cases where medium header information in Cartridge Memory is not synchronized with the medium header on the medium.
- Recognizing media used by other applications.

Activate Cartridge Memory support for a drive by setting the `Advanced` options from the `Settings` property page of the drive. Refer to Figure 2-11.

Limitations

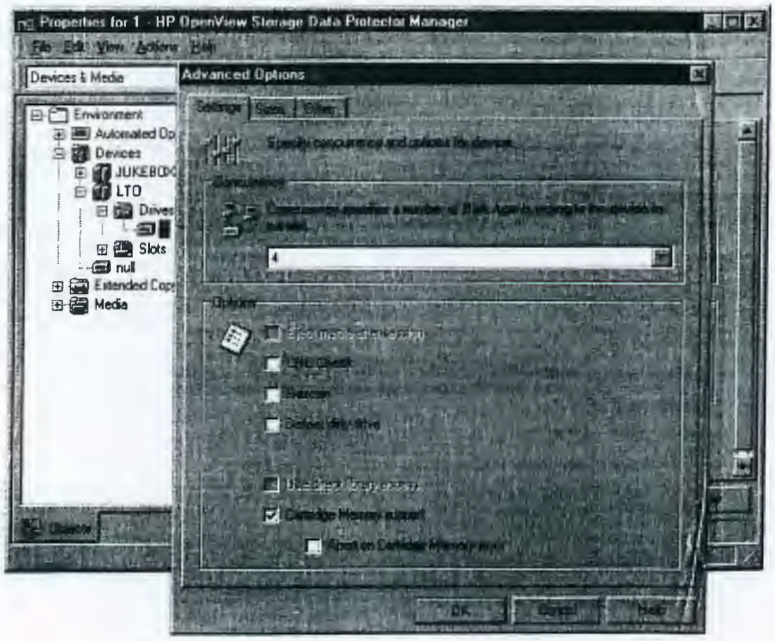
Cartridge Memory operations on LTO devices are not supported in the following cases:

- On Novell NetWare platforms
- On AIX platforms

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1609
Doc: 3702

17 252

Figure 2-11 **Cartridge Memory Support Activation for a Drive**



RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1610
Doc: 3702

17 251
2

Disabling a Backup Device

Disabling a backup device is useful when the device is damaged or in maintenance mode.

If you disable a backup device, all subsequent backups skip this device. The next available device defined in the list of devices for the backup specification is used, provided that load balancing has been selected. All devices using the same lock name as the disabled device are also disabled.

This lets you avoid backups that fail due to a device needing service, while keeping other devices available (and configured) for backup.

How to Disable a Device

Disable a backup device by selecting the `Disable device` option in the `Settings` property page of the device or drive. Refer to Figure 2-12. For detailed steps, refer to the online Help index keyword "disabling backup devices".

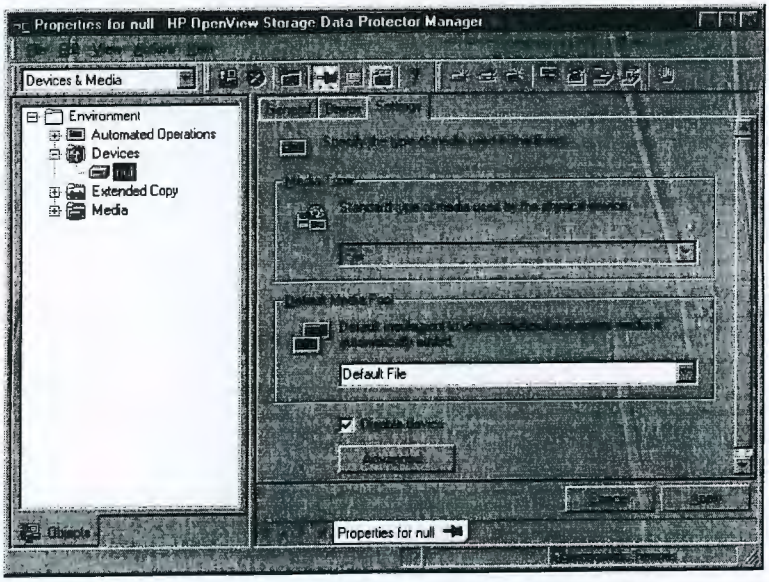
How to Restart the Device

To resume using the device for backups, deselect the `Disable device` option.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1611
Doc: 3702

12.250

Figure 2-12 **Disable Device**



RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1612
3702
Doc:

12.249

Removing a Backup Device

By removing a backup device from the Data Protector configuration, you stop using this device for backup or restore. Make sure that you remove the device from all backup specifications that use the device. Otherwise the backup or restore will fail.

TIP

Also, if you are not using a certain backup device with Data Protector anymore, you may want to delete the Data Protector Media Agent software from the system. This can be done using the Client context.

How to Remove a Backup Device

To remove a backup device, delete it from the `Devices & Media` context. For detailed steps, refer to the online Help index keyword "deleting backup devices".

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1613
Doc: 3702

17.243

Renaming a Backup Device

When you rename a backup device, the device is no longer used under its old name for backup or restore.

IMPORTANT Make sure that you remove the device's old name from all backup specifications that use the device. Otherwise, Data Protector tries to back up to or restore from a device that does not exist, and the session fails.

How to Rename a Backup Device Rename a backup device in the `General` property page of the device. For detailed steps, refer to the online Help index keyword "renaming backup devices".

ROS nº 03/2006 - CN - CPMI - CORREIOS
Fls Nº 1614
Nº 3702 Doc

17.247

Device Locking

Internal Locking

The internal locking of backup devices prevents two Data Protector sessions from accessing the same physical device at the same time. For example, if one backup session is using a particular device, all other backup/restore sessions must wait for this device to become free before starting to use it. When a backup or restore session starts, the Data Protector locks the device, the drive, and the slot used for that session.

Media sessions performing media operations such as initialization, scanning, verifying, copying, or importing also lock devices. During that time, no other operations can lock and use the device. If a media session cannot obtain a lock, the operation fails, and you have to retry the operation at a later time.

Locking When a Mount Request Is Issued

During a mount request of a backup or restore session, Data Protector allows the device to be used for media management operations, such as formatting a new medium.

When the mount request is confirmed, the backup or restore session locks the device again and continues with the session.

Locking with Data Protector

You can configure the same physical device many times with different characteristics, simply by configuring devices with different device names.

Since the internal locking operates on logical devices rather than on physical devices, a collision can occur if you specify one device name in one backup specification and another device name for the same physical device in another backup specification. Depending on the backup schedule, this may result in Data Protector trying to use the same physical device in several backup sessions at the same time. This can also happen when two device names are used in other operations, such as backup and restore, backup and scan, and so on.

To prevent this collision, you can specify a virtual lock name in both device configurations. Data Protector then uses this lock name to check if the device is available, thus preventing collisions.

If you configure two Data Protector backup devices that actually point to the same physical device, you are advised to specify the `Lock Name` in the advanced options for the two logical devices. `Lock Name` is the name that

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1615
Doc: 3702

17.246

Data Protector recognizes in order to lock the device before starting backup and restore sessions. Both logical devices need to have the same lock name. Refer to "Shared Devices in the SAN Environment" on page 44 for example on how to use `Lock Name`.

How to Lock a Device

Lock a backup device by selecting the `Use Lock Name` advanced option from the Settings property page for the device, and then entering the lock name of your choice. For detailed steps, refer to the online Help index keyword "locking backup devices".

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1616
Doc: 3702

17.245

Device Concurrency, Segment Size, and Block Size

Streaming

To maximize a device's performance, it has to be kept streaming. A device is streaming if it can feed enough data to the medium to keep it moving forward continuously. Otherwise, the tape has to be stopped, the device waits for more data, reverses the tape a little and resumes writing to the tape, and so on. In other words, if the data rate written to the tape is less than or equal to the data rate which can be delivered to the device by the computer system, the device is streaming. Device streaming is also dependent on other factors such as network load and the block size of the data written to the backup device in one operation.

For additional information on device concurrency, segment size, and block size, see the Media Management chapter in the *HP OpenView Storage Data Protector Concepts Guide*.

Changing Concurrency

Data Protector provides a default number of Disk Agents that are started for each device. Increasing the number of Disk Agents sending data to a Media Agent at the same time improves device streaming.

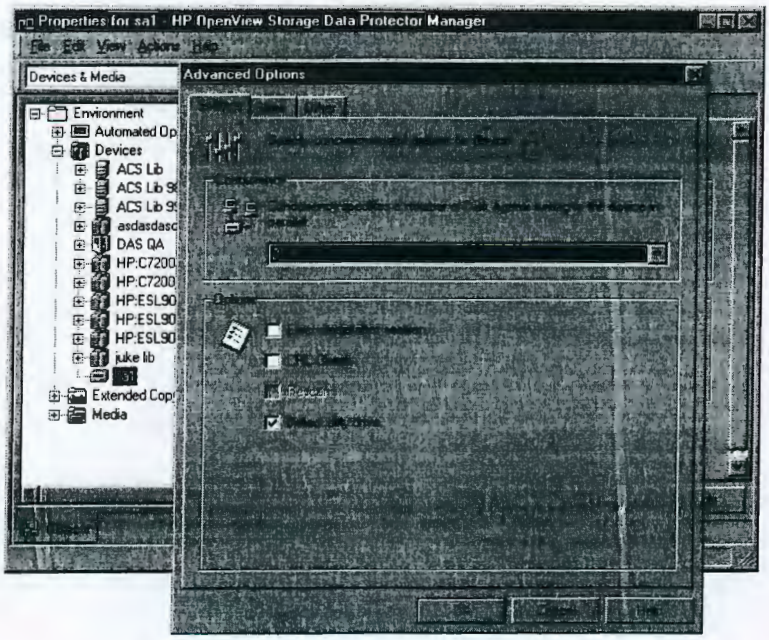
In the `Advanced Options` dialog box of a specific device, set the `Concurrency` to the maximum number of Disk Agents allowed to feed data to each Media Agent. See Figure 2-13 on page 77. For detailed steps, refer to the online Help index keyword "concurrency".

Concurrency can also be set in the backup specification. The concurrency set in the backup specification will take precedence over the concurrency set in the device definition. See Figure 2-14 on page 78. For detailed steps, refer to the online Help index keyword "concurrency".

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1617
Doc: 3702

17.244
L

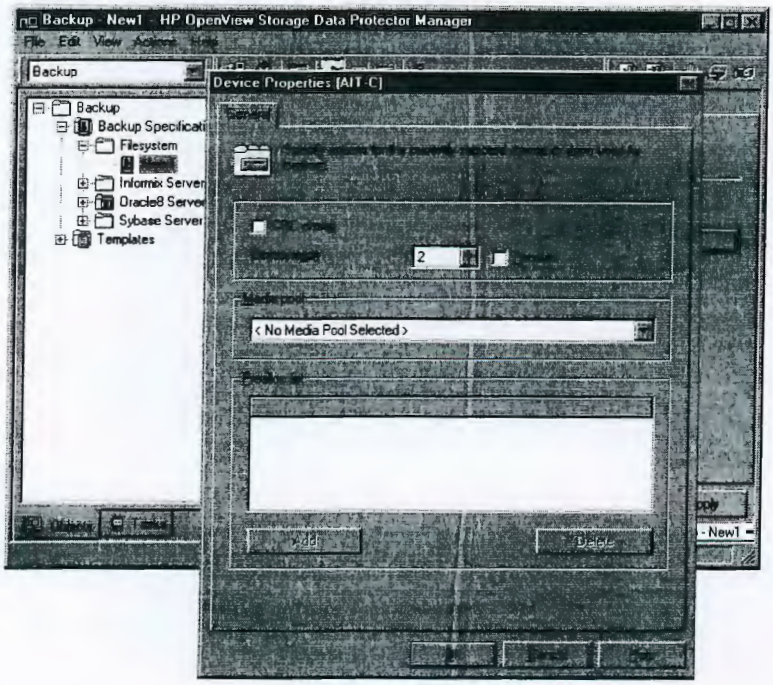
Figure 2-13 **Advanced Options Dialog Box: Concurrency**



RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1618
Nº
Doc: 3702
Doc:

17.243

Figure 2-14 **Device Properties Dialog Box: Concurrency**



Changing Segment Size

Segment size is related to the size of data areas which Data Protector uses in writing data to the media. It is user-configurable for each device. Note that a smaller segment size consumes media space because each segment has a file mark which takes up space on a medium. A larger number of file marks results in faster restores, because the Media Agent can quickly locate the segment containing the data to be restored.

Optimal segment size depends on the media type used in the device and the kind of data to be backed up. The average number of segments per tape is 50. The default segment size can be calculated by dividing the native capacity of a tape by 50. The maximum catalog size is limited to a fixed number (12 MB) for all media types.

Data Protector finishes a segment when the first limit is reached. When backing up a large number of small files, the media catalog limit is reached faster, which can result in smaller segment sizes.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1619
Doc: 3702

17.242

You can change the segment size in the `Advanced Options` dialog box of a specific device. For detailed steps, refer to the online Help index keyword "segment size".

Changing the Number of Buffers

Data Protector Media Agents and Disk Agents use memory buffers during data transfer. Memory is divided into a number of buffer areas. Values from 1 - 32 may be specified.

Each buffer area consists of 8 Disk Agent buffers, which are of the same size as the block size configured for the device. The default device block size is 64 KB.

You can change the number of buffers by changing the `Advanced Option` properties of the selected drive. For detailed steps, refer to the online Help index keyword "number of Disk Agent buffers".

Block Size

When a device receives data, it processes it using a device-type-specific (DDS, DLT) block size.

NOTE

Each backup device (drive) has a block size. A restore adjusts to block size.

Before Changing Block Size in Data Protector

Data Protector uses a default device block size for each device type. The block size applies to all devices created by Data Protector and to Media Agents running on the different platforms.

The device block size is written on a media header so that Data Protector knows the size to be used. If the device block size differs from the medium's block size, an error occurs.

You can change the device block size in the Data Protector GUI. However, before changing the block size you need to check the supported block size of the host adapter.

The minimum block size for old SCSI cards, such as the Adaptec 2940, was 56 KB. Currently, the minimum block size that is mainly used with newer SCSI cards is 64 KB.

You can increase the maximum block size on a Windows Media Agent client by modifying its Registry. For information on how to modify the block size, see the example in "Changing Block Size on Windows Media Agent" on page A-51.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1620
Doc: 3702

17.241
2

Before changing the block size for a particular SCSI card, refer to the SCSI vendor documentation or contact the vendor support.

Changing the Block Size in Data Protector

You can set the block size in the `Advanced Options` dialog box of a specific device. For detailed steps, refer to the online Help index keyword "block size".

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1621
Nº Doc: 3702

17.240

3 Configuring Users and User Groups

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1622
Nº Doc: 3702

17.239

In This Chapter

This chapter explains how to configure both user groups and individual users. It contains information about the following subjects:

"Data Protector User Rights" on page 83

"Predefined Data Protector User Groups" on page 86

"Adding or Deleting a User Group" on page 88

"Adding or Deleting a User" on page 90

"Modifying a User" on page 92

"Changing User Group Rights" on page 93

"Example User Configurations" on page 94

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1623
Doc: 3702

17.238

Data Protector User Rights

Data Protector users have the user rights of the user group they belong to. For example, all members of the Admin user group have the rights of the Data Protector Admin user group.

When configuring a Windows NT or a Windows 2000 user in a Data Protector cell running the Cell Manager on the HP-UX or Solaris platform, the user has to be configured with the Domain Name or the wildcard group "*".

The Data Protector user rights are described below:

Clients configuration	Allows the user to install and update Data Protector software on client systems.
User configuration	Allows the user to add, delete, and modify users and user groups. Note that this is a powerful right.
Device configuration	Allows the user to create, configure, delete, modify, and rename devices. This includes the ability to add a mount request script to a logical device.
Media configuration	Allows the user to manage media pools and the media in the pools and to work with media in libraries, including ejecting and entering media.
Reporting and notifications	Allows the user to create Data Protector reports. To use Web Reporting you also need a Java user under the Applet domain in the Admin user group.
Start backup	Allows users to back up their own data as well as monitor and abort their own sessions.

RQS nº 03/2005 - CN
CPMI - CORREIOS
1624
Fls Nº
Doc: 3702

17.237

Start backup specification	Allows the user to perform a backup using a backup specification, so that the user can back up objects listed in any backup specification and can also modify existing backups.
Save backup specification	Allows the user to create, schedule, modify, and save any backup specification.
Back up as root	Allows the user to back up any object with the rights of the root login on UNIX clients. This user right is effective only for UNIX clients. It is required to run any backup on Novell NetWare clients.
Switch session ownership	Allows the user to specify the owner of the backup specification under which the backup is started. By default, the owner is the user who started the backup. Scheduled backups are started as root on a UNIX Cell Manager and under the Cell Manager account on Windows systems. This user right is appropriate if the Start backup specification user right is enabled. See "Ownership: Who Will Be Able to Restore?" on page 235 for more details.
Monitor	Allows the user to view information about any active session in the cell and to access the IDB to view past sessions.
Abort	Allows the user to abort any active session in the cell.
Mount request	Allows the user to respond to mount requests for any active session in the cell.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1625
Doc: 3702

17.236
L

Start restore	Allows users to restore their own data as well as monitor and abort their own restore sessions. Users that have this user right are able to view their own objects and public objects on the Cell Manager.
Restore to other clients	Allows the user to restore an object to a system other than the one from where the object was backed up.
Restore from other users	Allows the user to restore objects belonging to another user. It is effective only for UNIX clients.
Restore as root	Allows the user to restore objects with the rights of the root UNIX user. Note that this is a powerful right that can affect the security of your system. This user right is required to run any restore on Novell NetWare clients.
See private objects	Allows the user to view and restore objects that were backed up as private.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1626
Doc: 3702

17 235

Predefined Data Protector User Groups

The following default groups are provided: Admin, Operator, and User.

User Rights	Admin	Operator	User
Clients configuration	Y		
User configuration	Y		
Device configuration	Y		
Media configuration	Y	Y	
Reporting and notifications	Y		
Start backup	Y	Y	
Start backup specification	Y	Y	
Save backup specification	Y		
Back up as root	Y		
Switch session ownership	Y	Y	
Monitor	Y	Y	
Abort	Y	Y	
Mount request	Y	Y	
Start restore	Y	Y	Y
Restore to other clients	Y		
Restore from other users	Y	Y	
Restore as root	Y		
See private objects	Y	Y	

TIP To see the exact user rights for each user group, select the group, right-click it, and select `Properties` from the menu.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1627
Doc: 3702

17.234
2

The user rights you have set on the Cell Manager determine the availability of the Data Protector Cell Manager GUI or GUI contexts to the computer from which you connect to the Cell Manager. For example, if you have only the `Start Restore` user right set, then only the `Restore` context is available when you install the User Interface component.

After the initial installation, all default user groups are empty except for the Admin group. Data Protector adds the following users to the Admin group:

- `root:sys` on HP-UX or Solaris
- The Cell Manager account as typed in during setup on Windows
- The `java` user, which enables Web Reporting

You do not have to add any other users if you do all the tasks as one of these users. Default user groups have been chosen so that the product can be operated smoothly and they should reflect the average configuration. They should be modified only if there is a good reason. Typically the operator group will be modified.

IMPORTANT Admin capabilities are very powerful. A member of the Data Protector Admin user group has system administrator capabilities for the whole cell.

ROS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1628
Doc: 3702

17.233
2

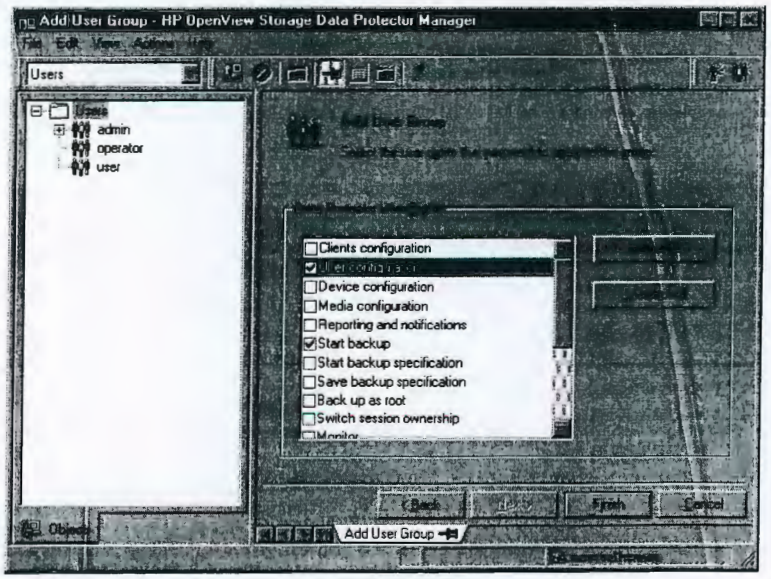
Adding or Deleting a User Group

The default Data Protector user groups are sufficient for most needs. It is recommended that you verify and, if necessary, modify the default user group rights to better fit your requirements.

Adding a User Group

1. In the `Data Protector Manager`, switch to the `Users` context.
2. In the Scoping Pane, right-click `Users`, and then click `Add User Group`. The `Add User Group` wizard appears.
3. Follow the wizard. For further information, press **F1**.

Figure 3-1 **Adding New User Groups**



ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1629
Doc 3702

17232
L

Deleting a User Group

1. In the `Data Protector Manager`, switch to the `Users` context.
2. In the Scoping Pane, expand `Users` to dispaly the user groups.
3. Right-click the user group to be deleted and click `Delete`.
4. Confirm the action.

CPMI - CORREIOS
Fls_Nº 1630
Doc: 3702

17.231
2

Adding or Deleting a User

After the product installation, the following users are configured in the Admin user group:

- UNIX root user on UNIX systems
- Windows administrator on Windows systems
- The user performing the installation

By adding a new user to one of the Data Protector user groups you assign this user the rights of that particular group. See "Data Protector User Rights" on page 83 for a description of the user rights.

NOTE Before you can start using the Data Protector GUI on the client system, add a user from that system to an appropriate Data Protector user group on the Cell Manager.

You can configure users from both UNIX and Windows environments.

UNIX users are defined by their login name, UNIX user group, and the system from which they log on. A wildcard (*) may be used.

Windows NT and Windows 2000 users are defined by their logon name, Windows user group (domain), and the system from which they log on. A wildcard (*) can be used.

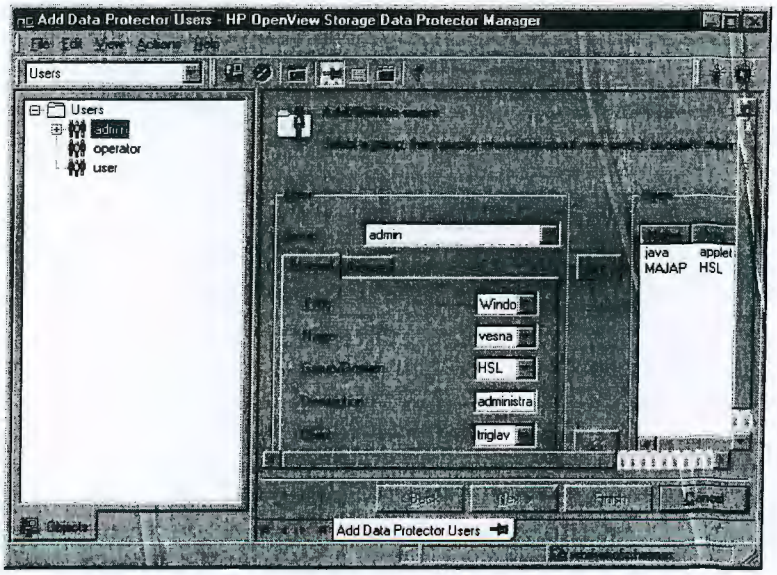
To add a user, do the following:

1. In the `Data Protector Manager`, switch to the `Users` context.
2. In the Scoping Pane, expand `Users`.
3. Right-click the group to which you want to add a user, or from which you want to delete a user, and then click `Add/Delete Users` to open the wizard.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
1631
Fls Nº
Doc 3702

17-230
L.

Figure 3-2 **Adding New Users**



For further information, press **F1**.

RQS nº 03/20
CPMI
CORREIOS
Fls Nº 1632
3702
Doc:

17.229
L

Modifying a User

You can change the properties of an existing user, or move the user from one user group to another.

NOTE You cannot change user rights for individual users, but only for the entire user group.

Changing User Properties

To modify a user's properties, follow these steps:

1. In the `Data Protector Manager`, switch to the `Users` context.
2. In the Scoping Pane, expand `Users`, and click the user group to which the user belongs.
3. Right-click the user and click `Properties` to open the user's property page.

   For further information, press **F1**.

Moving a User to Another User Group

To change the user rights of an individual user, move the user to another user group.

1. In the `Data Protector Manager`, switch to the `Users` context.
2. In the Scoping Pane, expand `Users`, and click the user group to which the user belongs.
3. In the Results Area, right-click the user and click `Move`.

   For further information, click `Help`.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1633
Doc: 3702

17.228

Changing User Group Rights

Users have the rights of the groups to which they belong. So, changing the user rights of the user group changes the user rights for all users in that group. You can change the rights of user groups and, in doing so, change the rights of each user within that group. You cannot change the rights of the Admin user group, however.

NOTE You can also modify the properties of each user within a group, for example the domain to which the user belongs, the user's real name, and the user's user group.

The following steps explain how to change user group rights, and consequently, the rights of each user in the group:

1. In the `Data Protector Manager`, switch to the `Users` context.
2. Browse for and select the user group whose rights you want to change.

NOTE If you select a group that does not have any users in it, the Results Area will display the properties for the group. If you select a group that has users in it, the Results Area will list the users in the group. You can also modify properties of each user in a user group by clicking on the user whose properties you want to modify.

3. Right-click the user group you selected, and then click `Properties`. The properties for the user group appear in the Results Area.
4. Click the `User Rights` tab to display the list of rights available to this group.

   For further information, press **F1**.

ROS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1634
Doc: 3702

17.227
L

Example User Configurations

This section gives some examples of typical user configurations.

Allowing Users to Restore Their Own Files

This restore policy allows all or just selected users to restore their own data. It provides sufficient security and may relieve the backup operator from doing a number of restore operations.

When to Use This Policy

- When the users have sufficient knowledge to handle restores. You need to provide some way of training the users on basic backup concepts and restore operations.
- You use library backup devices with media of all most recent backups. The Data Protector User group by default does not allow users to handle mount requests for needed media. The users will still need an intervention from the backup operator in case of a mount request.

What Needs to Be Done?

1. Add the users who will be allowed to restore their own data to the Data Protector `users` user group. For additional security, you may limit the access to Data Protector for these users to a specific system only.
2. Install the Data Protector User Interface on the systems the users are using. Data Protector automatically checks the user rights and allows restore functionality only.
3. When you configure backup of the user systems, make backups visible to the users by setting it to public.

Enabling Users to Back Up Their Systems

Data Protector differentiates between the user's right to configure a backup and the user's right to run an already configured backup.

To create rights for a user to run their own backup, follow these steps:

1. Create a new user group or modify the existing group so that it has the `Start backup` user right.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1635
Doc: 3702

17.226
L

2. Add the users who will be able to configure their own backups to this user group.
3. Change the owner of the backup configuration so that the users will be able to start these backups. See Figure 3-1 on page 88.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1636
Doc: 3702

17.225
2

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1637
3702
Doc: