Doc.
000233

CPL/AC

PREGÃO
050/2003

LOCAÇÃO DE EQUIPAMENTOS DE INFORMÁTICA INCLUINDO ASSISTÊNCIA TÉCNICA E TREINAMENTO

NEC DO BRASIL S/A – PROPOSTA ECONÔMICA VOLUME I

2003
PASTA 21

NEC DO BRASIL S.A.
Rod. Presidente Dutra, Km 214 – Jd Cumbica
07210-902 - Guarulhos – SP -
Tel.(0xx11) 6462.6000 - Fax (0xx11) 6412.3261
www.nec.com.br

13117
14

PROPOSTA ECONÔMICA
PREGÃO N.º 050/2003 - CPL/AC

1. Razão Social da Empresa: NEC do Brasil S/A.
2. CNPJ Nº: 49.074.412/0001-65
3. Inscrição Estadual:336.440.680.114
4. Inscrição Municipal:072772-54
5. Endereço Completo: Rodovia Presidente Dutra, km 214, Bairro Jardim Cumbica; CEP 07210-902; Guarulhos-SP
6. Telefone: (0XX)11-6462-7049 Fax:11-6462-7053 E-mail: vaird@nec.com.br
7. Validade da Proposta: 60 dias
8. Prazo de Pagamento: conforme edital
9. Banco: Unibanco Agência:0398 Conta Corrente:100317-5
10. Representante da Empresa: Vair Doiche
11. Cargo: Gerente Geral Comercial RG:9.064.070 CPF: 324.292.746-04

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0002
Doc: 3696

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:

PREÇO UNITÁRIO MENSAL DA LOCAÇÃO DOS PRODUTOS

TIPO DE PRODUTO	PREÇO UNITÁRIO DE LOCAÇÃO (R$)	DISTRIBUIÇÃO		TOTAL
		CCD AC (DF)	CCD SPM (SP)	
SERVIDOR INTEL TIPO 01	23.326,86	14	7	21
SERVIDOR INTEL TIPO 02	11.632,43	29	6	35
SERVIDOR INTEL TIPO 03	2.891,10	27	24	51
SERVIDOR RISC TIPO 01	78.538,70	8	3	11
SWITCH TIPO 01	59.639,38	2	2	4
SWITCH TIPO 02	7.072,25	4	2	6
SWITCH TIPO 03	144.455,18	4	2	6
SWITCH TIPO 04	2.413,13	8	4	12
SWITCH TIPO 05	34.798,35	1	1	2
ROTEADOR TIPO 01	27.366,82	1	1	2
ROTEADOR TIPO 02	19.138,42	2	0	2
UNIDADE DE BACKUP ROBOTIZADO	431.962,84	1	1	2
SERVIDOR DE SEGURANÇA LÓGICA TIPO 01	20.571,80	2	2	4
SERVIDOR DE SEGURANÇA LÓGICA TIPO 02	23.558,04	1	1	2
SERVIDOR PARA DETECÇÃO DE INTRUSÃO	100.006,56	1	1	2
	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.

00017

Servidor Intel Tipo 1 → 489.864,06
Servidor Intel Tipo 2 → ~~407.135,05~~ 407.135,05
Servidor Intel Tipo 3 → 147.446,10
Servidor Risc Tipo 1 → 863.925,70
Switch Tipo 1 → 238.557,52
Switch Tipo 2 → 42.433,50
Switch Tipo 3 → 866.731,08
Switch Tipo 4 → 28.957,56
Switch Tipo 5 → 69.596,70
Roteador Tipo 1 → 54.733,64
Roteador Tipo 2 → 38.276,84
Unidade Backup Robotizado → 863.925,68

Servidor de seguranca lógica
Tipo 1 → 82.287,20

Servidor de segurança lógica
Tipo 2 → 47.116,08

Servidor p/ detecção de intrusão → 200.013,12

4.440.999,83

213.167.991,80

± 8,20

NEC

NEC DO BRASIL S.A.
Rod. Presidente Dutra, Km 214 – Jd Cumbica
07210-902 - Guarulhos – SP -
Tel.(0xx11) 6462.6000 - Fax (0xx11) 6412.3261
www.nec.com.br

ECT 113115

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.)**

213.167.991,90

Discriminação dos Valores:

VALOR TOTAL DA LOCAÇÃO (somatório dos 48 meses de aluguel)	**R$ 213.168.000,00 (duzentos e treze milhões, cento e sessenta e oito mil reais)**
APRESENTAÇÃO DO CRONOGRAMA DE TRABALHO (1% do Valor Total da Locação) 2.131.679,92	**R$ 2.131.680,00 (dois milhões, cento e trinta e um mil, seiscentos e oitenta reais)**
VALOR GLOBAL DA PROPOSTA (VALOR TOTAL DA LOCAÇÃO+Cronograma de Trabalho) 215.299.671,70	**R$ 215.299.680,00 (duzentos e quinze milhões, duzentos e noventa e nove mil, seiscentos e oitenta reais)**

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 percentual de cada um)	PERCENTUAL
1. EQUIPAMENTOS:	**65%**
Subtotal	**R$ 2.890.935,85**
2. SOFTWARE:	**6%**
Subtotal	**R$ 274.925,56**
3. TREINAMENTOS	**2%**
Subtotal	**R$ 87.539,53**
4. ASSISTÊNCIA TÉCNICA / GARANTIA	**8%**
Subtotal	**R$ 351.199,41**
5. INSTALAÇÃO	**19%**
Subtotal	**R$ 836.399,65**
6. TRIBUTOS	
Subtotal	
7. TRANSPORTE / FRETE / SEGURO	
Subtotal	
8. DESPESAS ADMINISTRATIVAS	
Subtotal	
9. LUCRO	
Subtotal	
10. OUTROS	
Subtotal	
TOTAL	**R$ 4.441.000,00**

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0004
Doc: 3696

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,

0002

NEC DO BRASIL S.A.
Rod. Presidente Dutra, Km 214 – Jd Cumbica
07210-902 - Guarulhos – SP -
Tel.(0xx11) 6462.6000 - Fax (0xx11) 6412.3261
www.nec.com.br

13114

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 o proponente 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:
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.

Guraulhos, 23 de Julho de 2003

NEC do Brasil S/A / CNPJ 49.074.412/0001-65

Vair Doiche

RQS nº 03/2005 - CN - CPMI - CORREIOS
0005
Fls. Nº
3696
Doc:

0003

NEC DO BRASIL S/A.

ECT 13313 CPI

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

Ref.: Pregão Nº 050/2003 – CPL/AC

Empresa NEC do Brasil S.A., inscrita no CNPJ 49.074.412/0001-65, por intermédio legal o Sr. Vair Doiche, portador da Carteira de Identidade Nº 9.064.070 e do CPF Nº 324.292.746-04, declara que o fornecimento de equipamentos / softwares ou prestação de serviços por terceiros, constantes da nossa proposta, não diminui, em hipótese alguma, a nossa total responsabilidade pelo perfeito e completo funcionamento do objeto do Edital do Pregão Nº 050/2003 – CPL/AC.

Declaramos, ainda, de que 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,

Guarulhos, 23 de julho de 2003.

NEC do Brasil S.A. / CNPJ 49.074.412/0001-65

VAIR DOICHE

NEC DO BRASIL S. A.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0006
Doc: 3696

0004

Sun Microsystems, Inc.
Sun Microsystems do Brasil
R. Alexandre Dumas, 2.016
04717-004 - São Paulo - SP
Tel.: (0xx11) 5187-2100
Fax: (0xx11) 5181-0974

ECT
13112
A
CPL

Sun microsystems

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

DECLARAÇÃO DE FORNECIMENTO DE PRODUTOS NOVOS

A empresa SUN MICROSYSTEMS, INC., sediada à 901 San Antonio Road, Palo Alto, California, E.U.A., na qualidade de fabricante dos produtos Sun Microsystems, **declara** que, para o atendimento ao Pregão em epígrafe, os produtos cotados pela NEC do Brasil S.A., CNPJ: 49.074.412/0001-65, sediada à Rodovia Presidente Dutra, Km. 214, Guarulhos - SP, conforme relação abaixo mencionada, serão de linha de produção continuada e terão o fornecimento garantido de peças de reposição pelo período mínimo de 60 (sessenta) meses.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0007
3696
Doc:

- Marca: SUN MICROSYSTEMS Modelo: Sun Fire 15K Server
- Marca: SUN MICROSYSTEMS Modelo: Sun Fire V480 Server
- Marca: SUN MICROSYSTEMS Modelo: Sun StorEdge L700 Library
- Marca: SUN MICROSYSTEMS Modelo: Sun Blade 150 Workstation
- Marca: SUN MICROSYSTEMS Modelo: Sun StorEdge 2GB Brocage Silkworm 1200 Switch

(F) CONFERIDO POR

São Paulo, 22 de julho de 2003

Sun Microsystems, Inc.
Cleber Pereira de Morais
Procurador

CARTORIO REGISTRO CIVIL IBIRAPUERA
Av. Independencia, 51 Fone: 5506.5744
VALIDO SOMENTE C/SELO DE AUTENTICIDADE
RECONHECO POR SEMELHANCA 0001 FIRMAS DE
CLEBER PEREIRA DE MORAIS
S. PAULO, 22 DE JULHO DE 2003.
EM TESTEMUNHO DA VERDADE
BATISTA CORREIA ESC. AUTORIZ.
Custas ******2,07
DOC.S/V.ECONOMICO
4A056275

Colegio Notarial do Brasil - SP
FIRMA 1
Batista Correia
Escrevente Autorizado

Sun microsystems Jurídico

0005

CISCO SYSTEMS

ECT 13111 A CPL-AC

São Paulo, 21 de julho de 2003

EMPRESA BRASILEIRA DE CORREIOS E TELÉGRAFOS - ECT

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0008
Doc: 3696

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 **NEC do Brasil S.A.,** com endereço em Rodovia Presidente Dutra, km 214, CEP 07210-902, Cumbica, Guarulhos-SP, doravante EMPRESA, é revendedor autorizado Cisco no Brasil.

We hereby inform for the purposes of the above process that **NEC do Brasil S.A.** with address at Rodovia Presidente Dutra, km 214, CEP 07210-902, Cumbica, Guarulhos-SP, hereinafter COMPANY is an authorized reseller in Brazil.

Asseguramos para fins do certame em referência:

We certify for the purposes of the above process:

- o fornecimento e a garantia dos produtos Cisco no anexo relacionados; e que
- os equipamentos Cisco cotados pela EMPRESA, relacionados no anexo são de linha de produção continuada e que serão fornecidas peças de reposição pelo período mínimo de 60 (sessenta) meses.

- the supply and warranty of the Cisco products listed in the attachment hereto; and that
- the Cisco equipment offered by COMPANY are from a continued line of production and that spare parts will be available for a minimum period of 60 (sixty) months.

Atestamos ainda, com relação aos equipamentos Cisco relacionados no anexo:

We also certify with regards to the Cisco products listed in the attachment hereto:

a) nossa solidariedade para com a EMPRESA no âmbito dos produtos Cisco quanto aos compromissos que a EMPRESA venha a assumir perante a ECT, no escopo desta licitação;

a) our joint liability with COMPANY with regards to Cisco products in relation to the obligations that COMPANY commits before ECT, within this process;

b) que a EMPRESA está apta a prestar assistência técnica, com o uso de peças e componentes originais, bem como suporte aos produtos Cisco cotados;

b) that COMPANY is capable of rendering technical assistance, with the use of original spare parts, as well as support to the Cisco products offered;

c) nossa responsabilidade solidária para com a EMPRESA pelo perfeito cumprimento das exigências de garantia dos produtos Cisco,

c) our joint liability responsibility with COMPANY for the perfect fulfillment of warranty of Cisco products, during the whole

0016

ECT 13110 A. CPL-AC

Cisco Systems

durante todo o prazo de vigência do contrato. 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 DE:
001-SERGIO FUMIAKI TSUJIOKA
SAO PAULO, 22 DE JULHO DE 2003.
EM TESTEMUNHO DA VERDADE

ALCIDES BATISTA CORREIA-ESC. AUTORIZ.
Total Custas.:*****2,07
Car.:1337023 DOC.S/V.ECONOMICO
Selo:1063AA055801

Cartório Notarial do Brasil S/C
FIRMA 1
1063AA055801
Marcio Roberto Trevino
Escrevente Autorizado

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0009
3696
Doc:

0007

NEC

QTDE	PART NUMBER	DESCRIÇÃO
4	WS-C6513	Cat 6513 Chassis, 13slot, 19RU, No Pow Supply, No Fan Tray
4	WS-C6K-13SLT-FAN2	High Speed Fan Tray for Catalyst 6513 / Cisco 7613
4	WS-CAC-2500W=	Catalyst 6000 2500W AC Power Supply
4	WS-CAC-2500W=	Catalyst 6000 2500W AC Power Supply
8	CAB-AC-2500W-INT	Power Cord, 250Vac 16A, INTL
4	S6S22ZK2-12119E	Catalyst 6000 SUP2/MSFC2 IOS SP W/VIP SSH 3DES
4	WS-X6K-S2-MSFC2=	Catalyst 6500 Supervisor Engine-2, 2GE, plus MSFC-2 / PFC-2
4	WS-X6500-SFM2=	Catalyst 6500 Switch Fabric Module 2, Spare
4	WS-X6516A-GBIC=	Catalyst 6500 16-port GigE Mod, fabric-enabled (Req. GBICs)
4	WS-F6K-DFC	Dist Fwd Card for 65xx, 6816 Modules used with SUP1A/SUP2
4	MEM-DFC-128MB	128 MB DRAM FOR DFC
12	WS-X6548-GE-TX=	Catalyst 6500 48-port fabric-enabled 10/100/1000 Module
16	WS-X6516-GE-TX=	Catalyst 6500 16-port Gig/Copper Module, x-bar
16	WS-F6K-DFC	Dist Fwd Card for 65xx, 6816 Modules used with SUP1A/SUP2
16	MEM-DFC-128MB	128 MB DRAM FOR DFC
4	WS-X6066-SLB-APC=	Catalyst 6500/7600 Content Switching Module
4	SC6K-3.1.3-CSM	CSM 3.1.3 Software Release
4	WS-SVC-NAM-1=	Catalyst 6500 Network Analysis Module-1
4	SC-SVC-NAM-3.1	Catalyst 6500 NAM SW Release 3.1
64	WS-G5484=	1000BASE-SX Short Wavelength GBIC (Multimode only)
4	MEM-S2-128MB	Catalyst 6000 Sup2 Mem, 128MB DRAM Option
4	MEM-MSFC2-128MB	Catalyst 6000 MSFC-2 Mem, 128MB DRAM Option
6	WS-C2950G-48-EI	Catalyst 2950, 48 10/100 with 2 GBIC slots, Enhanced Image
6	CAB-AC	Power Cord,110V
6	WS-G5484=	1000BASE-SX Short Wavelength GBIC (Multimode only)
6	WS-X3500-XL	GigaStack Stacking GBIC and 50cm cable
6	PWR300-AC-RPS-N1	Redundant Power System 300 (RPS 300) w/ 1 connector cable
6	CAB-AC	Power Cord,110V
4	CVPN3060-NR	VPN 3060 Concentrator (Non-Redun, 1 P/S); 5000users@100Mbps
4	CVPN3060-SW-K9	Software for VPN3060 Concentrator
4	CAB-AC	Power Cord,110V
4	CVPN3000-PWR=	Cisco VPN 3000 Concentrator Power Supply
2	CSACSE-1111-K9	Cisco Secure ACS 3.2 Solution; includes HW and SW
2	CAB-AC	Power Cord,110V
2	CSACSE-3.2-SW-K9	Config. Option; CSACS 3.2 Software loaded on Cisco 1111
2	CISCO3745	3700 Series, 4-Slot, Dual FE, Multiservice Access Router
2	PWR-3745-AC	AC Power Supply for the Cisco 3745
2	PWR-3745-AC=	AC Power Supply Spare for the Cisco 3745
4	CAB-AC	Power Cord,110V
2	S374C-12208T	Cisco 3745 Series IOS IP
2	**MÍDIA**	**SUPORTE INFORMÁTICO**
2	S374AK9-12208T=	Cisco 3745 Series IOS ENTERPRISE PLUS IPSEC 3DES
2	**MÍDIA**	**SUPORTE INFORMÁTICO**

0008

2	NM-1FE2W=	1 10/100 Ethernet 2 WAN Card Slot Network Module
4	WIC-2T=	2-Port Serial WAN Interface Card spare
4	NM-1A-E3=	1-Port E3 ATM Network Module
2	NM-1GE=	1 Port GE Network Module
4	WIC-2T=	2-Port Serial WAN Interface Card spare
16	CAB-SS-V35MT=	V.35 Cable, DTE Male to Smart Serial, 10 Feet
2	WS-G5483=	1000BASE-T GBIC
2	CISCO1751-V	10/100 Modular Router w/Voice,32F/64D
2	MEM1700-64D=	Cisco 1700 64MB DRAM DIMM
2	CD17-CVP-12.1.5=	Cisco 1700 IOS IP/VOICE PLUS ADSL Feature Pack
2	**MÍDIA**	**SUPORTE INFORMÁTICO**
2	S17C7VK9-12208T=	Cisco 1700 IOS IP/ADSL/VOICE PLUS IPSEC 3DES
2	**MÍDIA**	**SUPORTE INFORMÁTICO**
2	WIC-2T=	2-Port Serial WAN Interface Card spare
2	VIC-2FXO=	Two-port Voice Interface Card - FXO-Spare
2	VIC-2FXS=	Two-port Voice Interface Card - FXS-Spare
2	PVDM-256K-4	4-Channel Packet Voice/Fax DSP Module
2	CAB-AC	Power Cord,110V
2	CAB-SS-V35FC=	V.35 Cable, DCE Female to Smart Serial, 10 Feet
2	CAB-SS-V35MT=	V.35 Cable, DTE Male to Smart Serial, 10 Feet
2	PVDM-256K-4=	4-Channel Packet Voice/Fax DSP Module
4	PIX-535	PIX Firewall 535 Chassis
4	CAB-AC	Power Cord,110V
4	PIX-VPN-3DES	168-bit 3DES VPN feature license for PIX Firewall
4	PIX-535UR-SW	Unrestricted feature license for PIX 535 Firewall
4	**MÍDIA**	**SUPORTE INFORMÁTICO**
4	SF-PIX-6.2	PIX v6.2 Software for the PIX 515E, 525 and 535 Chassis
4	PIX-1GE-66	66MHz Gigabit Ethernet Interface, Multimode (SX) SC
4	PIX-1GE-66	66MHz Gigabit Ethernet Interface, Multimode (SX) SC
4	PIX-4FE-66	PIX 66-MHz Four-port 10/100 Ethernet Interface, RJ45
4	PIX-535-PWR-AC	Redundant AC power supply for PIX 535
4	PIX-1FE	Single 10/100 Fast Ethernet Inteface for PIX Firewall, RJ45
4	PIX-1FE	Single 10/100 Fast Ethernet Inteface for PIX Firewall, RJ45
4	PIX-VPN-ACCEL	VPN Accelerator Card for PIX 515E/525/535-UR/FO Firewall
4	PIX-535-MEM-512	PIX 535 512MB RAM Upgrade (2-256MB DIMM, UR Only)
4	PIX-535-PWR-BLANK	Blank to fill unused power supply slot on PIX 535
4	PIX-535	PIX Firewall 535 Chassis
4	CAB-AC	Power Cord,110V
4	PIX-VPN-3DES	168-bit 3DES VPN feature license for PIX Firewall
4	PIX-535FO-SW	Failover feature license for PIX 535 Firewall
4	**MÍDIA**	**SUPORTE INFORMÁTICO**
4	SF-PIX-6.2	PIX v6.2 Software for the PIX 515E, 525 and 535 Chassis
4	PIX-1GE-66	66MHz Gigabit Ethernet Interface, Multimode (SX) SC
4	PIX-1GE-66	66MHz Gigabit Ethernet Interface, Multimode (SX) SC
4	PIX-4FE-66	PIX 66-MHz Four-port 10/100 Ethernet Interface, RJ45
4	PIX-535-PWR-AC	Redundant AC power supply for PIX 535
4	PIX-1FE	Single 10/100 Fast Ethernet Inteface for PIX Firewall, RJ45
4	PIX-1FE	Single 10/100 Fast Ethernet Inteface for PIX Firewall, RJ45
4	PIX-VPN-ACCEL	VPN Accelerator Card for PIX 515E/525/535-UR/FO Firewall

4	PIX-535-MEM-512	PIX 535 512MB RAM Upgrade (2-256MB DIMM, UR Only)
4	PIX-535-PWR-BLANK	Blank to fill unused power supply slot on PIX 535
2	PIX-525	PIX Firewall 525 Chassis
2	CAB-AC	Power Cord,110V
2	PIX-VPN-3DES	168-bit 3DES VPN feature license for PIX Firewall
2	PIX-525-SW-UR	Unrestricted feature license for PIX 525 Firewall
2	**MÍDIA**	**SUPORTE INFORMÁTICO**
2	SF-PIX-6.2	PIX v6.2 Software for the PIX 515E, 525 and 535 Chassis
2	PIX-4FE-66=	PIX 66-MHz Four-port 10/100 Ethernet Interface, RJ45
2	PIX-1GE-66=	66MHz Gigabit Ethernet Interface, Multimode (SX) SC
2	PIX-VPN-ACCEL	VPN Accelerator Card for PIX 515E/525/535-UR/FO Firewall
2	PIX-525	PIX Firewall 525 Chassis
2	CAB-AC	Power Cord,110V
2	PIX-VPN-3DES	168-bit 3DES VPN feature license for PIX Firewall
2	PIX-525-SW-FO	Failover feature license for PIX 525 Firewall
2	**MÍDIA**	**SUPORTE INFORMÁTICO**
2	SF-PIX-6.2	PIX v6.2 Software for the PIX 515E, 525 and 535 Chassis
2	PIX-4FE-66=	PIX 66-MHz Four-port 10/100 Ethernet Interface, RJ45
2	PIX-1GE-66=	66MHz Gigabit Ethernet Interface, Multimode (SX) SC
2	PIX-VPN-ACCEL	VPN Accelerator Card for PIX 515E/525/535-UR/FO Firewall
2	IDS-4250-TX-K9	4250 Sensor (chassis, s/w, SSH, 10/100/1000BaseT w/ RJ-45)
2	CAB-AC	Power Cord,110V
2	CWVMS-2.2-UR-K9	VMS 2.2 WIN/SOL Unrestricted
2	**MÍDIA**	**SUPORTE INFORMÁTICO**
2	CWVMS-MCCSA-4.0	Expanded Part use Only: MC for Cisco Security Agents 4.0
2	CWLMS-2.2-K9	LAN Managment 2.2 for WIN/SOL; CM, DFM, RME, RTM, CV
2	**MÍDIA**	**SUPORTE INFORMÁTICO**
2	CWRW-1.3-K9	Routed WAN Mgmt 1.3 for WIN/SOL; ACL, IPM, RME, CV
2	**MÍDIA**	**SUPORTE INFORMÁTICO**

Itec
www.itec.com.br

DECLARAÇÃO

São Paulo, 23 de Julho de 2003.

À
EMPRESA BRASILEIRA DE CORREIOS E TELÉGRAFOS –ECT
SBN – Quadra 01, Bloco "A" – Sobreloja – Ed. Sede ECT
Fax: (61) 426-2759

Ref.: PREGÃO Nº 050/2003 – CPL/AC

ITEC S.A. – GRUPO ITAUTEC PHILCO, com sede na Av. Paulista nº 1938 – 20.andar, inscrita no CNPJ/MF sob nº 96.452.347/0001-44, como **Distribuidora Autorizada da IBM Brasil e sediada no Brasil**, conforme declaração em anexo do fabricante, **DECLARA** para os devidos fins, que a empresa **NEC DO BRASIL S/A**, com sede Rodovia Presidente Dutra, Km 214 – Cumbica - Guarulhos, inscrita no CNPJ/MF sob nº 49.074.412/0001-65, é sua Revenda Autorizada para ofertar os produtos abaixo relacionados no Pregão ECT nº 050/2003 – CPL/AC.

Produtos ***Servidores Intel IBM – IBM eServers xSeries x440, x360, x235.***

Por ser verdade, firmamos a presente.

Simon Ruben Schvartzman
Diretor de Operações

Renato Mantovani
Gerente de Desenvolvimento de Mercado

ITEC S.A.

0011

ECT 13104

Declaração do Fabricante IBM

Á ITEC S.A. - Grupo Itautec Philco
Av. Paulista, 1938 20º andar
CNPJ 96.452.347/0001-44

Ref: Edital do Pregão ECT No. 050/2003 – Objeto: locação e instalação de 119 (cento e dezenove) 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.

A IBM BRASIL - Indústria Máquinas e Serviços Ltda., sediada na Avenida Pasteur, 138/146 - bairro Botafogo - Rio de Janeiro - RJ, inscrita no CNPJ n.º 33.371.251/001-56, declara para os devidos fins que os equipamentos por ela fabricados, abaixo listados e conforme apresentados no Edital acima referenciado, são de linha de produção continuada e se compromete a fornecer peças de reposição pelo período mínimo de 60 (sessenta) meses:

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

São Paulo 23, de julho de 2003.

4º Tab

Paulo Zirnberger de Castro
Gerente de Unidades de Negócios - xSeries
IBM Brasil Indústria, Máquinas e Serviços Ltda.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0014
Doc: 3696

4º TABELIÃO DE NOTAS - Estado de São Paulo - Comarca da Capital
RUA ESTADOS UNIDOS, 28 - CEP: 01427-000 - FONE: (0XX11) 3887-6700
Tabelião: Bel. OSVALDO CASHEO - Tabelião Substituto: Bel. JOSÉ ALEXANDRE NASCIMENTO

RECONHECO por semelhança 0001 firma(s) de:
PAULO ZIRNBERGER DE CASTRO
23/07/2003 EM TEST. DA VERDADE.
EDMILSON NUNES DA SILVA-ESCREVENTE AUTORIZADO
Car.:856863 Pago:R$ 2,07 DOC.S/VL.EC.
Selo(s): AAM043285

VALIDO SOMENTE COM O SELO DE AUTENTICIDADE E SEM EMENDAS E/OU RASURAS

4º TABELIÃO - SP
FIRMA
1038AA043285

01 12

Sun Microsystems, Inc.
Sun Microsystems do Brasil
R. Alexandre Dumas, 2.016
04717-004 - São Paulo - SP
Tel.: (0xx11) 5187-2100
Fax: (0xx11) 5181-0974

E C T
13103
A
C P L - A C

Sun microsystems

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

CERTIFICADO DE REVENDA AUTORIZADA SUN MICROSYSTEMS

A empresa SUN MICROSYSTEMS, INC., sediada à 901 San Antonio Road, Palo Alto, California, E.U.A., na qualidade de fabricante dos produtos Sun Microsystems, declara que a empresa NEC do Brasil S.A., CNPJ: 49.074.412/0001-65, sediada à Rodovia Presidente Dutra, Km. 214, Guarulhos - SP, é nossa Revenda Autorizada, estando habilitada a comercializar os produtos Sun Microsystems, em particular ao Pregão em epígrafe.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0015
Doc: 3696

(F) CONFERIDO POR

São Paulo, 22 de julho de 2003

Sun Microsystems, Inc.
Cleber Pereira de Morais
Procurador

Sun microsystems
jurídico

ARTÓRIO REGISTRO CIVIL IBIRAPUERA
Independencia,51 Fone:5506.5744
SOMENTE C/SELO DE AUTENTICIDADE
POR SEMELHANÇA 0001 FIRMAS DE
CLEBER PEREIRA DE MORAIS
PAULO,22 DE JULHO DE 2003.
TESTEMUNHO DA VERDADE
BATISTA CORREIA-ESC. AUTORIZ.
Custas.R$*****2,07
DOC.S/V.ECONOMICO
063AA056274

Colégio Notarial do Brasil
Alcides Batista Correia Escrevente
FIRMA 1
1063AA056274

0013

BLACK BOX
NETWORK SERVICES

São Paulo, 23 julho de 2003.

A
EMPRESA BRASILEIRA DE CORREIOS E TELEGRAFOS
BRASILIA/DF

Ref.: PREGÃO Nº050/2003

Objeto.: Fornecimento e instalação de solução de comutação de servidores

DECLARAÇÃO DE SOLIDARIEDADE

Declaramos, na qualidade de fabricante, que a Nec do Brasil S/a, CNPJ nº49.074.412/0001-65 ,Rod.Pres.Dutra Km-214 –Jr.Cumbica,Guarulhos-SP é nosso revendedor autorizado e está apto a comercializar os equipamentos por nós produzidos, descritos abaixo:

KV138A	KV134A-R2	EHN151-0020	EHN382-0050	EHN383-0100
KV1301C-R2	KV131A-R2	KV1300C	KV1305C	KV1306C
KV140035	KV180035	EHN151-0020	ACU1009A	RMK19A

Declaramos ainda:

a) Nossa fidedignidade em relação às características dos produtos cotados;
b) Nossa solidariedade para com a Nec do Brasil S/A ,quanto aos compromissos que esta venha a assumir perante a EMPRESA BRASILEIRA DE CORREIOS E TELEGRAFOS;
c) Que a Nec do Brasil S/A está apta a prestar manutenção, com uso de peças e componentes originais, bem como suporte aos produtos e equipamentos cotados;
d) Que somos responsáveis solidários com a Nec Do Brasil S/A, pelo perfeito cumprimento das exigências de garantia dos equipamentos, durante todo o seu prazo de vigência.
e) A Black Box do Brasil assegura que os referidos equipamentos são de linhas de produção continuada,comprometendo fornecer peças reposição no período de 60 meses.

Atenciosamente

Fagan, Carlos Cezar
Gerente de Vendas e Suporte
Black Box do Brasil Ltda

5º Tabelionato de Notas FRANCA

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 0016
3696
Doc.

5o.Tabelionato de Notas - Jose Roberto Pacheco Franca - Tabeliao
Av. Joao Dias, 2320-Santo Amaro - Fone:5641-6072
Reconheco por semelhanca *******0001******* firma(s)
001-CARLOS CEZAR FAGAN
VALIDO SOMENTE COM SELO DE AUTENTICIDADE - Doc. com valor econ.
Carimbo:139470 : 23 DE JULHO DE 2003
Total..:******5,50 : Em testemunho ______________ da verdade.
Conf...:FIRMA : DIVAR ODEVO BRANO JUNIOR - ESCREVENTE

Simone Brulico
Escrevente

Colégio Notarial do Brasil - SP
VALOR ECONÔMICO
ARPEN
1036AA019648

AA003100

14

Carta de Solidariedade

Á ITEC S.A. - Grupo Itautec Philco
Av. Paulista, 1938 20° andar
CNPJ 96.452.347/0001-44

Ref: Edital do Pregão ECT No. 050/2003 – Objeto: locação e instalação de 119 (cento e dezenove) equipamentos de informática – novos de fábrica - incluindo: a configuração, o treinamento, a assistência técnica e a garantia, destinados aos Centros Corporativos de Dados da ECT, localizados nas cidades de Brasília e São Paulo.

Vimos, por meio desta, apresentar nossa solidariedade com a ITEC S.A. - Grupo Itautec Philco, Av. Paulista, 1938 20° andar, 96.452.347/0001-44, no Edital supracitado, que estamos solidários a esta, garantindo o fornecimento dos seguintes produtos:

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

Adicionalmente atestamos:

a) nossa solidariedade com a Itec no âmbito dos produtos acima listados, quanto aos compromissos por ela assumidos na licitação supra-citada;
b) A assistência técnica estará sendo realizada pelo fabricante, com o uso de peças e componentes originais, bem como suporte aos produtos cotados devido a aquisição do contrato de manutenção.
c) Nossa responsabilidade solidária com a Itec 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.

1º Tab

Paulo Zimberger de Castro
Gerente de Unidades de Negócios - xSeries
IBM Brasil Indústria, Máquinas e Serviços Ltda.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0017
Doc: 3696

0017

Project Management Institute

This is to certify that

Heliaura N. Duarte

has successfully completed all prescribed requirements and is hereby designated by the Project Management Institute as a

Project Management Professional

17 July 2000 – 31 December 2003

In testimony whereof, we have subscribed our signatures under the seal of the Institute.

Hugh Woodward
Chair, Board of Directors

Executive Director

Certification Number: 25897

CORREIOS **ADMINISTRAÇÃO CENTRAL**

ECT 13097 A

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) MARCELO CHAVES CURCIO, representante da empresa NEC DO BRASIL S.A, esteve visitando nesta data, as instalações físicas do Centro Corporativo de Dados de BRASILIA, visando obter subsídios para a proposta econômica da licitação em questão.

1. Responsável pelo Termo de Vistoria
   Nome em letra de forma: LUY NEY MUNIZ BARBOSA
   Matrícula: 8139930-2
   Assinatura: _____
   Data: 21/7/2003.

2. Representante da Licitante
   Nome em letra de forma: MARCELO CHAVES CURCIO
   Assinatura: _____
   Data: 21/07/2003.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0019
Doc 3696

Brasília-DF, 21 de JULHO de 2003.

OBSERVAÇÕES:

- Os interessados em participar desta Licitação deverão realizar, ***obrigatoriamente***, vistoria nos Centros Corporativos de Dados de Brasília e São Paulo, devidamente acompanhada de representante da ECT.
  Os endereços dos CCDs são os seguintes:
  Brasília : SBN - QUADRA 01- BLOCO A - 2º SUBSOLO - ED. SEDE ECT - BRASÍLIA/DF
  São Paulo : RUA MERGENTHALER, Nº 592 – BLOCO 3 – 4º 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

0019

13096

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) CRISTIANO MARTINS F VILLAR, representante da empresa NEC DO BRASIL S.A., esteve visitando nesta data, as instalações físicas do Centro Corporativo de Dados de SÃO PAULO - SPM, visando obter subsídios para a proposta econômica da licitação em questão.

1. Responsável pelo Termo de Vistoria
   Nome em letra de forma: OCAVO DE BRITO
   Matrícula: 8.918.438-6
   Assinatura: _____
   Data: 21 / 07 /2003.

2. Representante da Licitante
   Nome em letra de forma: CRISTIANO MARTINS F VILLAR
   Assinatura: _____
   Data: 21 / 07 /2003.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0020
Doc: 3696

SÃO PAULO
Brasília-DF, 21 de julho de 2003.

OBSERVAÇÕES:

- Os interessados em participar desta Licitação deverão realizar, ***obrigatoriamente***, vistoria nos Centros Corporativos de Dados de Brasília e São Paulo, devidamente acompanhada de representante da ECT.
  Os endereços dos CCDs são os seguintes:
  Brasília : SBN - QUADRA 01- BLOCO A - 2º SUBSOLO - ED. SEDE ECT - BRASÍLIA/DF
  São Paulo : RUA MERGENTHALER, Nº 592 – BLOCO 3 – 4º 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

Características Técnicas do Objeto Licitado

23/07/03

0021

Resumo dos equipamentos fornecidos		
Equipamento	Fabricante	Modelo
Switch tipo 1	Cisco	Catalyst 6513
Switch tipo 2	Cisco	Catalyst 2950
Switch tipo 3	Brocade	Silkworm 12000
Switch tipo 4	Black Box	ServSwitch Affinity
Switch tipo 5	Cisco	VPN 3060
Roteador tipo 1	Cisco	3745
Roteador tipo 2	Cisco	1751-V
Servidor Intel tipo 1	IBM	x440
Servidor Intel tipo 2	IBM	x360
Servidor Intel tipo 3	IBM	x235
Sevidor RISC tipo 1	SUN	Sunfire 15k
Unidade de Backup	SUN	L700
Servidor de Segurança Lógica tipo 01	Cisco	PIX FW 535
Servidor de Segurança Lógica tipo 02	Cisco	PIX FW 525
Servidor para Detecção de Intrusão	Cisco	IDS 4250
Rack	IBM	NetBAY42

Planilha de Quantitativos de Servidores Intel		
Código	**Descrição**	**Qtd.**
xSeries440	**Equipamentos Tipo 1**	
86877RX	x440, 4xXeon MP 2.0GHz/400MHz, 2MB, 2GB, O/Bay, 2x1050W p/s, Rack	21
59P5173	xSeries 2.0GHz/400Mhz, 2MB L3 Upgrade with Xeon Processor MP	84
59P5188	xSeries SMP Expansion Module	21
33L3324	512MB PC133 ECC SDRAM RDIMM	252
06P5756	IBM 73.4GB 10K rpm Ultra160 SCSI Hot-Swap SL HDD	42
06P5740	IBM ServeRAID-4Lx Ultra160 SCSI Controller	21
24P0960	IBM Total Storage FAStT FC2-133 Host Bus Adapter	42
31P6301	NetXtreme 1000 T Ethernet adapter (copper)	63
xSeries360	**Equipamentos Tipo 2**	
86869RX	x360, 2xXeon MP 2.0GHz/400MHz, 2MB, 2GB, O/Bay, 2x370W p/s, Rack	37
59P6817	2.0GHz/400Mhz, 2MB L3 Cache Upgrade with Xeon Processor MP	74
33L3283	512MB PC1600 ECC DDR SDRAM RDIMM	148
06P5756	IBM 73.4GB 10K rpm Ultra160 SCSI Hot-Swap SL HDD	74
06P5740	IBM ServeRAID-4Lx Ultra160 SCSI Controller	37
24P0960	IBM Total Storage FAStT FC2-133 Host Bus Adapter	74
31P6108	xSeries 370W Hot Swap Redundant Power Supply	37
31P6301	NetXtreme 1000 T Ethernet adapter (copper)	74
xSeries235	**Equipamentos Tipo 3**	
86718AX	x235, Intel Xeon 2.4GHz/533MHz, 512KB, 512MB, O/Bay, 2x660W p/s, Ultra320, Tower	61
59P4211	IBM 5Ux24D Tower to Rack Conversion Kit III (xSeries 235)	61
02R1988	3.06GHz/533Mhz, 512KB Upgrade with Intel Xeon Processor	61
33L5038	512MB PC2100 CL2.5 ECC DDR SDRAM RDIMM	122
32P0727	IBM 73.4GB 10K-rpm Ultra320 SCSI Hot-Swap SL HDD	122
31P6301	NetXtreme 1000 T Ethernet adapter (copper)	112
24P0960	IBM Total Storage FAStT FC2-133 Host Bus Adapter	2
Racking	**Local A**	
9306420	NetBAY42 SR Standard Rack Cabinet - includes Perforated front door, rear door and side panels	1
9306421	NetBAY42 SX Standard Expansion Rack Cabinet - includes Perforated front door and rear door	7
32P1736	IBM DPI Universal Rack PDU	32
94G7448	Hi-volt Power Cable (required for server, monitor, console switch, devices)	64
94G6670	Blanking Plate sets	6
Racking	**Local B**	
9306420	NetBAY42 SR Standard Rack Cabinet - includes Perforated front door, rear door and side panels	1
9306421	NetBAY42 SX Standard Expansion Rack Cabinet - includes Perforated front door and rear door	4
32P1736	IBM DPI Universal Rack PDU	16
94G7448	Hi-volt Power Cable (required for server, monitor, console switch, devices)	54
94G6670	Blanking Plate sets	4
Monitores		
31P8136	E74 17.0-inch (16.0-inch viewable) MPRII Color Monitor (6332)	12
31P7453	Preferred Pro Full-size Keyboard	12
28L3673	Sleek mouse	12

0023

NEC

13092
A.

Planilha de Quantitativos

QTDE	PART NUMBER	DESCRICAO
4	WS-C6513	Cat 6513 Chassis, 13slot, 19RU, No Pow Supply, No Fan Tray
4	WS-C6K-13SLT-FAN2	High Speed Fan Tray for Catalyst 6513 / Cisco 7613
4	WS-CAC-2500W=	Catalyst 6000 2500W AC Power Supply
4	WS-CAC-2500W=	Catalyst 6000 2500W AC Power Supply
8	CAB-AC-2500W-INT	Power Cord, 250Vac 16A, INTL
4	S6S22ZK2-12119E	Catalyst 6000 SUP2/MSFC2 IOS SP W/VIP SSH 3DES
4	WS-X6K-S2-MSFC2=	Catalyst 6500 Supervisor Engine-2, 2GE, plus MSFC-2 / PFC-2
4	WS-X6500-SFM2=	Catalyst 6500 Switch Fabric Module 2, Spare
4	WS-X6516A-GBIC=	Catalyst 6500 16-port GigE Mod, fabric-enabled (Req. GBICs)
4	WS-F6K-DFC	Dist Fwd Card for 65xx, 6816 Modules used with SUP1A/SUP2
4	MEM-DFC-128MB	128 MB DRAM FOR DFC
12	WS-X6548-GE-TX=	Catalyst 6500 48-port fabric-enabled 10/100/1000 Module
16	WS-X6516-GE-TX=	Catalyst 6500 16-port Gig/Copper Module, x-bar
16	WS-F6K-DFC	Dist Fwd Card for 65xx, 6816 Modules used with SUP1A/SUP2
16	MEM-DFC-128MB	128 MB DRAM FOR DFC
4	WS-X6066-SLB-APC=	Catalyst 6500/7600 Content Switching Module
4	SC6K-3.1.3-CSM	CSM 3.1.3 Software Release
4	WS-SVC-NAM-1=	Catalyst 6500 Network Analysis Module-1
4	SC-SVC-NAM-3.1	Catalyst 6500 NAM SW Release 3.1
64	WS-G5484=	1000BASE-SX Short Wavelength GBIC (Multimode only)
4	MEM-S2-128MB	Catalyst 6000 Sup2 Mem, 128MB DRAM Option
4	MEM-MSFC2-128MB	Catalyst 6000 MSFC-2 Mem, 128MB DRAM Option
6	WS-C2950G-48-EI	Catalyst 2950, 48 10/100 with 2 GBIC slots, Enhanced Image
6	CAB-AC	Power Cord,110V
6	WS-G5484=	1000BASE-SX Short Wavelength GBIC (Multimode only)
6	WS-X3500-XL	GigaStack Stacking GBIC and 50cm cable
6	PWR300-AC-RPS-N1	Redundant Power System 300 (RPS 300) w/ 1 connector cable
6	CAB-AC	Power Cord,110V
4	CVPN3060-NR	VPN 3060 Concentrator (Non-Redun, 1 P/S); 5000users@100Mbps
4	CVPN3060-SW-K9	Software for VPN3060 Concentrator
4	CAB-AC	Power Cord,110V
4	CVPN3000-PWR=	Cisco VPN 3000 Concentrator Power Supply
2	CSACSE-1111-K9	Cisco Secure ACS 3.2 Solution; includes HW and SW
2	CAB-AC	Power Cord,110V
2	CSACSE-3.2-SW-K9	Config. Option; CSACS 3.2 Software loaded on Cisco 1111
2	CISCO3745	3700 Series, 4-Slot, Dual FE, Multiservice Access Router
2	PWR-3745-AC	AC Power Supply for the Cisco 3745
2	PWR-3745-AC=	AC Power Supply Spare for the Cisco 3745
4	CAB-AC	Power Cord,110V
2	S374C-12208T	Cisco 3745 Series IOS IP
2	**MÍDIA**	**SUPORTE INFORMÁTICO**
2	S374AK9-12208T=	Cisco 3745 Series IOS ENTERPRISE PLUS IPSEC 3DES
2	**MÍDIA**	**SUPORTE INFORMÁTICO**
2	NM-1FE2W=	1 10/100 Ethernet 2 WAN Card Slot Network Module
4	WIC-2T=	2-Port Serial WAN Interface Card spare
4	NM-1A-E3=	1-Port E3 ATM Network Module
2	NM-1GE=	1 Port GE Network Module
4	WIC-2T=	2-Port Serial WAN Interface Card spare
16	CAB-SS-V35MT=	V.35 Cable, DTE Male to Smart Serial, 10 Feet
2	WS-G5483=	1000BASE-T GBIC
2	CISCO1751-V	10/100 Modular Router w/Voice,32F/64D
2	MEM1700-64D=	Cisco 1700 64MB DRAM DIMM
2	CD17-CVP-12.1.5=	Cisco 1700 IOS IP/VOICE PLUS ADSL Feature Pack

NEC

13091
4.

2	**MÍDIA**	**SUPORTE INFORMÁTICO**
2	S17C7VK9-12208T=	Cisco 1700 IOS IP/ADSL/VOICE PLUS IPSEC 3DES
2	**MÍDIA**	**SUPORTE INFORMÁTICO**
2	WIC-2T=	2-Port Serial WAN Interface Card spare
2	VIC-2FXO=	Two-port Voice Interface Card - FXO-Spare
2	VIC-2FXS=	Two-port Voice Interface Card - FXS-Spare
2	PVDM-256K-4	4-Channel Packet Voice/Fax DSP Module
2	CAB-AC	Power Cord,110V
2	CAB-SS-V35FC=	V.35 Cable, DCE Female to Smart Serial, 10 Feet
2	CAB-SS-V35MT=	V.35 Cable, DTE Male to Smart Serial, 10 Feet
2	PVDM-256K-4=	4-Channel Packet Voice/Fax DSP Module
4	PIX-535	PIX Firewall 535 Chassis
4	CAB-AC	Power Cord,110V
4	PIX-VPN-3DES	168-bit 3DES VPN feature license for PIX Firewall
4	PIX-535UR-SW	Unrestricted feature license for PIX 535 Firewall
4	**MÍDIA**	**SUPORTE INFORMÁTICO**
4	SF-PIX-6.2	PIX v6.2 Software for the PIX 515E, 525 and 535 Chassis
4	PIX-1GE-66	66MHz Gigabit Ethernet Interface, Multimode (SX) SC
4	PIX-1GE-66	66MHz Gigabit Ethernet Interface, Multimode (SX) SC
4	PIX-4FE-66	PIX 66-MHz Four-port 10/100 Ethernet Interface, RJ45
4	PIX-535-PWR-AC	Redundant AC power supply for PIX 535
4	PIX-1FE	Single 10/100 Fast Ethernet Inteface for PIX Firewall, RJ45
4	PIX-1FE	Single 10/100 Fast Ethernet Inteface for PIX Firewall, RJ45
4	PIX-VPN-ACCEL	VPN Accelerator Card for PIX 515E/525/535-UR/FO Firewall
4	PIX-535-MEM-512	PIX 535 512MB RAM Upgrade (2-256MB DIMM, UR Only)
4	PIX-535-PWR-BLANK	Blank to fill unused power supply slot on PIX 535
4	PIX-535	PIX Firewall 535 Chassis
4	CAB-AC	Power Cord,110V
4	PIX-VPN-3DES	168-bit 3DES VPN feature license for PIX Firewall
4	PIX-535FO-SW	Failover feature license for PIX 535 Firewall
4	**MÍDIA**	**SUPORTE INFORMÁTICO**
4	SF-PIX-6.2	PIX v6.2 Software for the PIX 515E, 525 and 535 Chassis
4	PIX-1GE-66	66MHz Gigabit Ethernet Interface, Multimode (SX) SC
4	PIX-1GE-66	66MHz Gigabit Ethernet Interface, Multimode (SX) SC
4	PIX-4FE-66	PIX 66-MHz Four-port 10/100 Ethernet Interface, RJ45
4	PIX-535-PWR-AC	Redundant AC power supply for PIX 535
4	PIX-1FE	Single 10/100 Fast Ethernet Inteface for PIX Firewall, RJ45
4	PIX-1FE	Single 10/100 Fast Ethernet Inteface for PIX Firewall, RJ45
4	PIX-VPN-ACCEL	VPN Accelerator Card for PIX 515E/525/535-UR/FO Firewall
4	PIX-535-MEM-512	PIX 535 512MB RAM Upgrade (2-256MB DIMM, UR Only)
4	PIX-535-PWR-BLANK	Blank to fill unused power supply slot on PIX 535
2	PIX-525	PIX Firewall 525 Chassis
2	CAB-AC	Power Cord,110V
2	PIX-VPN-3DES	168-bit 3DES VPN feature license for PIX Firewall
2	PIX-525-SW-UR	Unrestricted feature license for PIX 525 Firewall
2	**MÍDIA**	**SUPORTE INFORMÁTICO**
2	SF-PIX-6.2	PIX v6.2 Software for the PIX 515E, 525 and 535 Chassis
2	PIX-4FE-66=	PIX 66-MHz Four-port 10/100 Ethernet Interface, RJ45
2	PIX-1GE-66=	66MHz Gigabit Ethernet Interface, Multimode (SX) SC
2	PIX-VPN-ACCEL	VPN Accelerator Card for PIX 515E/525/535-UR/FO Firewall
2	PIX-525	PIX Firewall 525 Chassis
2	CAB-AC	Power Cord,110V
2	PIX-VPN-3DES	168-bit 3DES VPN feature license for PIX Firewall
2	PIX-525-SW-FO	Failover feature license for PIX 525 Firewall
2	**MÍDIA**	**SUPORTE INFORMÁTICO**
2	SF-PIX-6.2	PIX v6.2 Software for the PIX 515E, 525 and 535 Chassis
2	PIX-4FE-66=	PIX 66-MHz Four-port 10/100 Ethernet Interface, RJ45
2	PIX-1GE-66=	66MHz Gigabit Ethernet Interface, Multimode (SX) SC
2	PIX-VPN-ACCEL	VPN Accelerator Card for PIX 515E/525/535-UR/FO Firewall
2	IDS-4250-TX-K9	4250 Sensor (chassis, s/w, SSH, 10/100/1000BaseT w/ RJ-45)
2	CAB-AC	Power Cord,110V

RQS nº 03/2005 - CN - CPMI - CORREIOS
0025
Fls. Nº
3696
Doc:

0025

NEC

13090
A-

2	CWVMS-2.2-UR-K9	VMS 2.2 WIN/SOL Unrestricted
2	**MÍDIA**	**SUPORTE INFORMÁTICO**
2	CWVMS-MCCSA-4.0	Expanded Part use Only: MC for Cisco Security Agents 4.0
2	CWLMS-2.2-K9	LAN Managment 2.2 for WIN/SOL; CM, DFM, RME, RTM, CV
2	**MÍDIA**	**SUPORTE INFORMÁTICO**
2	CWRW-1.3-K9	Routed WAN Mgmt 1.3 for WIN/SOL; ACL, IPM, RME, CV
2	**MÍDIA**	**SUPORTE INFORMÁTICO**

NEC

13089
A-

Sun microsystems

Quotation

Invoice Number: F-BR-14953-G
[Quote Valid for 38 Days]

Invoice Date: 23/07/03

Customer :

Sun
Sun Microsystems, Inc.

Tel / Fax : /

Tel / Fax :

We are pleased to quote as follows:

Approved by: A

Reference	F.O.B.	Page
	NULL	{P} of {N}

Item	Product Number	Description	Qty
		Sun Fire 15K para ECT - 8 para BSB e 3 para SP	
1		Configuration: F15K-CAB3	11
1.1	F15K-CAB3	Sun Fire 15K server cabinet with Fireplane, Fans, Power Supplies and System Controllers and updated Expanders	1
1.1.1	3848A	Power Cord for 68"Enterprise System and Expansion Cabinet,International Version (IEC 309, 32A, 250V Plug) OEM ready - 05/96	6
1.1.2	3859A	International power cord for 72" StorEdge expansion cabinet (IEC 309, 32A, 250V plug)	6
1.1.3	4610A	Top (Slot 0) Filler Panel for the CPU board slot in a Sun Fire 15K server	7
1.1.4	4615A	Bottom (Slot 1) Filler Panel for Sun Fire F15K server	9
1.2	DOMAIN	Domain A	1
1.2.1	1150A	Gigabit Ethernet Network Interface Card for high-performance Cat 5 UTP and PCI applications with full IEEE 802.3 compliance.	2
1.2.2	2222A	PCI Adapter with two Fast Ethernet Interfaces and Two SCSI Interfaces - Factory Configured	1
1.2.3	4575A	Hot Swap PCI Assembly for Sun Fire 15K includes 4 Standard PCI Slots Two running at 66mhz and two at 33mhz in 4 cassettes.	2
1.2.4	6768A	Sun StorEdge 2Gb PCI dual fibre channel network adapter, 200MB/s per channel with optical interface	1
1.2.5	CPUBD-441-1050	Uniboard bundle with: 4 CPUs running at 1050MHz; 4x8MB Ecache; 4 banks of 1GB memory options (16 x 256MB DIMMs, 4GB total for the board). For use with the Sun Fire 3800, 4800, 4810, 6800, 12K and 15K	2
1.3	DOMAIN	Domain B	1
1.3.1	1150A	Gigabit Ethernet Network Interface Card for high-performance Cat 5 UTP and PCI applications with full IEEE 802.3 compliance.	2
1.3.2	2222A	PCI Adapter with two Fast Ethernet Interfaces and Two SCSI Interfaces - Factory Configured	1
1.3.3	4575A	Hot Swap PCI Assembly for Sun Fire 15K includes 4 Standard PCI Slots Two running at 66mhz and two at 33mhz in 4 cassettes.	2
1.3.4	6768A	Sun StorEdge 2Gb PCI dual fibre channel network adapter, 200MB/s per channel with optical interface	1
1.3.5	CPUBD-441-1050	Uniboard bundle with: 4 CPUs running at 1050MHz; 4x8MB Ecache; 4 banks of 1GB memory options (16 x 256MB DIMMs, 4GB total for the board). For use with the Sun Fire 3800, 4800, 4810, 6800, 12K and 15K	1
1.4	DOMAIN	Domain B-2	1
1.4.1	1150A	Gigabit Ethernet Network Interface Card for high-performance Cat 5 UTP and PCI applications with full IEEE 802.3 compliance.	2
1.4.2	2222A	PCI Adapter with two Fast Ethernet Interfaces and Two SCSI Interfaces - Factory Configured	1

*Accepted By:*_____ *Title:*_____ *Date:*_____

NEC

19088

Sun microsystems

Quotation

Invoice Number: F-BR-14953-G
[Quote Valid for 38 Days]

Invoice Date: 23/07/03

Item	Product Number	Description	Qty
1.4.3	4575A	Hot Swap PCI Assembly for Sun Fire 15K includes 4 Standard PCI Slots Two running at 66mhz and two at 33mhz in 4 cassettes.	1
1.4.4	6768A	Sun StorEdge 2Gb PCI dual fibre channel network adapter, 200MB/s per channel with optical interface	1
1.4.5	CPUBD-481-1050	Uniboard bundle with: 4 CPUs running at 1.05 GHz; 4x8MB Ecache; 8 banks of 1GB memory options (32 x 256MB DIMMs, 8GB total for the board). For use with the Sun Fire 3800, 4800, 4810, 6800, 12K and 15K.	1
1.5	DOMAIN	Domain B-3	1
1.5.1	1150A	Gigabit Ethernet Network Interface Card for high-performance Cat 5 UTP and PCI applications with full IEEE 802.3 compliance.	2
1.5.2	2222A	PCI Adapter with two Fast Ethernet Interfaces and Two SCSI Interfaces - Factory Configured	1
1.5.3	4575A	Hot Swap PCI Assembly for Sun Fire 15K includes 4 Standard PCI Slots Two running at 66mhz and two at 33mhz in 4 cassettes.	1
1.5.4	6768A	Sun StorEdge 2Gb PCI dual fibre channel network adapter, 200MB/s per channel with optical interface	1
1.5.5	CPUBD-481-1050	Uniboard bundle with: 4 CPUs running at 1.05 GHz; 4x8MB Ecache; 8 banks of 1GB memory options (32 x 256MB DIMMs, 8GB total for the board). For use with the Sun Fire 3800, 4800, 4810, 6800, 12K and 15K.	1
1.6	DOMAIN	Domain B-4	1
1.6.1	1150A	Gigabit Ethernet Network Interface Card for high-performance Cat 5 UTP and PCI applications with full IEEE 802.3 compliance.	2
1.6.2	2222A	PCI Adapter with two Fast Ethernet Interfaces and Two SCSI Interfaces - Factory Configured	1
1.6.3	4575A	Hot Swap PCI Assembly for Sun Fire 15K includes 4 Standard PCI Slots Two running at 66mhz and two at 33mhz in 4 cassettes.	1
1.6.4	6768A	Sun StorEdge 2Gb PCI dual fibre channel network adapter, 200MB/s per channel with optical interface	1
1.6.5	CPUBD-481-1050	Uniboard bundle with: 4 CPUs running at 1.05 GHz; 4x8MB Ecache; 8 banks of 1GB memory options (32 x 256MB DIMMs, 8GB total for the board). For use with the Sun Fire 3800, 4800, 4810, 6800, 12K and 15K.	1
1.7	DOMAIN	Domain B-4-2	1
1.7.1	1150A	Gigabit Ethernet Network Interface Card for high-performance Cat 5 UTP and PCI applications with full IEEE 802.3 compliance.	2
1.7.2	2222A	PCI Adapter with two Fast Ethernet Interfaces and Two SCSI Interfaces - Factory Configured	1
1.7.3	4575A	Hot Swap PCI Assembly for Sun Fire 15K includes 4 Standard PCI Slots Two running at 66mhz and two at 33mhz in 4 cassettes.	1
1.7.4	6768A	Sun StorEdge 2Gb PCI dual fibre channel network adapter, 200MB/s per channel with optical interface	1
1.7.5	CPUBD-481-1050	Uniboard bundle with: 4 CPUs running at 1.05 GHz; 4x8MB Ecache; 8 banks of 1GB memory options (32 x 256MB DIMMs, 8GB total for the board). For use with the Sun Fire 3800, 4800, 4810, 6800, 12K and 15K.	1
1.8	DOMAIN	Domain B-4-2-2	1
1.8.1	1150A	Gigabit Ethernet Network Interface Card for high-performance Cat 5 UTP and PCI applications with full IEEE 802.3 compliance.	2
1.8.2	2222A	PCI Adapter with two Fast Ethernet Interfaces and Two SCSI Interfaces - Factory Configured	1
1.8.3	4575A	Hot Swap PCI Assembly for Sun Fire 15K includes 4 Standard PCI Slots Two running at 66mhz and two at 33mhz in 4 cassettes.	1
1.8.4	6768A	Sun StorEdge 2Gb PCI dual fibre channel network adapter, 200MB/s per channel with optical interface	1
1.8.5	CPUBD-481-1050	Uniboard bundle with: 4 CPUs running at 1.05 GHz; 4x8MB Ecache; 8 banks of 1GB memory options (32 x 256MB DIMMs, 8GB total for the board). For use with the Sun Fire 3800, 4800, 4810, 6800, 12K and 15K.	1

*Accepted By:*_____ *Title:*_____ *Date:*_____

NEC

Sun microsystems

Quotation

Invoice Number: F-BR-14953-G
[Quote Valid for 38 Days]

Invoice Date: 23/07/03

1308 A

Item	Product Number	Description	Qty
1.9	DOMAIN	Domain B-4-2-3	1
1.9.1	1150A	Gigabit Ethernet Network Interface Card for high-performance Cat 5 UTP and PCI applications with full IEEE 802.3 compliance.	2
1.9.2	2222A	PCI Adapter with two Fast Ethernet Interfaces and Two SCSI Interfaces - Factory Configured	1
1.9.3	4575A	Hot Swap PCI Assembly for Sun Fire 15K includes 4 Standard PCI Slots Two running at 66mhz and two at 33mhz in 4 cassettes.	1
1.9.4	6768A	Sun StorEdge 2Gb PCI dual fibre channel network adapter, 200MB/s per channel with optical interface	1
1.9.5	CPUBD-441-1050	Uniboard bundle with: 4 CPUs running at 1050MHz; 4x8MB Ecache; 4 banks of 1GB memory options (16 x 256MB DIMMs, 4GB total for the board). For use with the Sun Fire 3800, 4800, 4810, 6800, 12K and 15K	1
1.10	NS-XDSKS1-236GAC	Rackable thin storage 1U high, 2x36GB disk array, 10Krpm hot-swap drives, Ultra2/3 SCSI to host, AC powered. (Standard Configuration)	8
1.10.1	X3831A	10-meter 68 [illegible] to VHDC differential Ultra SCSI cable	8
1.10.2	X6920A	19" Rack Mount Kit for use with Netra st D130 in a SunFire 3800, 4800, 4810, 6800 server rack. Includes front or center fixed mount brackets and front & rear mount rail system.	8

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0029
Doc 3696

Accepted By: _____ *Title:* _____ *Date:* _____

0029

NEC

Sun microsystems

Quotation

Invoice Number: F-BR-14954-G
[Quote Valid for 9 Days]

Invoice Date: 23/07/03

13036 A.

Customer :

Sun
Sun Microsystems, Inc.

Tel / Fax : /

Tel / Fax :

We are pleased to quote as follows:

Approved by: A

Reference	F.O.B.	Page
	NULL	{P} of {N}

Item	Product Number	Description	Qty
		Library L700 (12 drives LTO-2) para SP	
1		Configuration: SG-XLIBL700-BASE3	1
1.1	SG-XLIBL700-BASE3	Sun StorEdge(TM) L700 Base library enclosure. Includes 20 cartridge access port with four (5-slot) media magazines, support for up to six 9x40 or 10 (S)DLT/LTO drives, 228 cartridge slots, power distribution unit, power supply, power cord, terminator and 6 meter SCSI data cable and installation guide. Installation is included. L700 frame is enabled to connect to another L700 unit.	1
1.1.1	SG-XLIBFCCARD	An upgrade card to move the L180 and L700 from SCSI to Native Fiber.	1
1.1.2	SG-XLIBL700-2POWER	Additional drive tower (2nd), additional power distribution unit (PDU) (2nd); redundant power supply for StorEdge L700 library.	1
1.1.3	SG-XMEDLTO200GB-10	10 Pack LTO Gen 2 media with 200 GB capacity.	41
1.1.4	SG-XMEDLTOUNVCL-10	LTO Universal cleaning cartridge	2
1.1.5	SG-XTAPLTO2FC-DRV	LTO Gen 2 Fibre Channel drive for the Sun StorEdge(TM) L180 and L700 tape libraries. Specs include 30MB/Sec. and 200GB capacity. Installation included.	12
1.1.6	X9734A	15M LC to LC FC Optical Cable	18
		Switches Brocade 12000 para SP e BSB	
2		Configuration: SG-XSWBRO12000-64P	1
2.1	SG-XSWBRO12000-64P	Brocade Silkworm 12000 switch w/64 ports, 2 Control Processors, 4 Power Supplies, Standard rack mount kit. Software bundle: Includes (WebTools, Advanced Zoning, Fabric Watch, Trunking and Advanced Performance Monitor). Media and Country Kit NOT included. Additional ports can be added up to a max of 128-ports in a chassis to make two independent 64-port switches.	6
2.1.1	SG-XSWBRO-12000-01	Brocade Silkworm 12000 Country Kit, North America. Includes: 2 Power cords.	6
2.1.2	SG-XSWBRO-12000TKR	Brocade Silkworm 12000 mid-mount rack mount kit. Required for mounting the Silkworm 12000 in a Telco rack.	6
2.1.3	XSFP-SW-2GB-4PK	4 pack of Small Form Pluggable 2 Gbit Fibre Channel Transceivers, short wave.	96
		Library L700 (20 drives LTO) para BSB	
3		Configuration: SG-XLIBL700-BASE3	1
3.1	SG-XLIBL700-BASE3	Sun StorEdge(TM) L700 Base library enclosure. Includes 20 cartridge access port with four (5-slot) media magazines, support for up to six 9x40 or 10 (S)DLT/LTO drives, 228 cartridge slots, power distribution unit, power supply, power cord, terminator and 6 meter SCSI data cable and installation guide. Installation is included. L700 frame is enabled to connect to another L700 unit.	1
3.1.1	SG-XCTXP180A-L700	168 slot plastic magazine kit which expands base configuration from 228 to 396 slots.	1
3.1.2	SG-XLIBFCCARD	An upgrade card to move the L180 and L700 from SCSI to Native Fiber.	1
3.1.3	SG-XLIBL700-2POWER	Additional drive tower (2nd), additional power distribution unit (PDU) (2nd); redundant power supply for StorEdge L700 library.	1
3.1.4	SG-XMEDLTO200GB-10	10 Pack LTO Gen 2 media with 200 GB capacity.	62

Accepted By: _____ *Title:* _____ *Date:* _____

NEC

13085
A.

Sun microsystems

Quotation

Invoice Number: F-BR-14954-G
[Quote Valid for 9 Days]

Invoice Date: 23/07/03

Item	Product Number	Description	Qty
3.1.5	SG-XMEDLTOUNVCL-10	LTO Universal cleaning cartridge	2
3.1.6	SG-XTAPLTO2FC-DRV	LTO Gen 2 Fibre Channel drive for the Sun StorEdge(TM) L180 and L700 tape libraries. Specs include 30MB/Sec. and 200GB capacity. Installation included.	20
3.1.7	X9734A	15M LC to LC FC Optical Cable	28
		Rack para acomodar switches + clusters	
4	X6825A	Front Door, Sun Rack 900	7
5	X6829A	Power Cable, International, Sun Rack 900 (Four 16A cables)	7
6	X6849A	Power Distribution System (PDS), Sun Rack 900	7
7	SR9-XKL038A-IP	Cabinet, Sun Rack 900 (This is an empty x-option rack without power.)	7
8	X9734A	15M LC to LC FC Optical Cable	460
		Hardware para cluster de servidores de backup	
9	X3837A	5 meter Null Ethernet Cable	4
10	X3830A	4-meter 68-pin to VHDC differential Ultra SCSI cable	4
11	X1134A	Cable, Ultra SCSI, SCSI-3/SCSI-3, 0.8m	4
12		Configuration: A41-UTA19C-256M-BA	4
12.1	A41-UTA19C-256M-BA	Sun Blade 150 Workstation 650-MHz UltraSPARC-IIi, 512-KB On-chip L2 Cache, 256-Mbyte SDRAM, PGX64 Onboard Graphics, 40-Gbyte Internal Disk, CD-ROM, SmartCard, 1.44MB Floppy, Sol 8 V.7 Installed, Universal Language Standard Configuration	1
12.2	X3531A	Type 6 Country Kits for U.S./ Universal/ Canada with USB interface	1
12.3	X7147A	17-inch Flat Display CRT Monitor, 16" diagonal viewable area, 0.24-mm dot pitch, 1280x1024 @ 75/76Hz, captive video cable with HD15-pin connector, Universal Power Supply, DDC1/2B, VESA DPMS, TCO'99, WW agency compliance, Standard version	1
13		Configuration: A37-WSPF2-04GQB	4
13.1	A37-WSPF2-04GQB	Sun Fire V480 Server 2 @ 900 MHz Cu, 4 GB memory, 2 - 36 GB, 1.0", 10,000 RPM, FC-AL disks, DVD, 2 power supplies. Standard Configuration.	1
13.1.1	X1150A	Gigabit Ethernet Network Interface Card for high-performance Cat 5 UTP and PCI applications with full IEEE 802.3 compliance.	2
13.1.2	X311L	Localized Power Cord Kit North American/Asian	2
13.1.3	X6540A	Dual-channel single-ended UltraSCSI host adapter, PCI; includes two 2m SCSI cables	2
13.1.4	X6768A	Sun StorEdge 2Gb PCI dual fibre channel network adapter, 200MB/s per channel with optical interface	2
13.2	NS-XDSKS1-236GAC	Rackable thin storage 1U high, 2x36GB disk array, 10Krpm hot-swap drives, Ultra2/3 SCSI to host, AC powered. (Standard Configuration)	1
13.2.1	X1134A	Cable, Ultra SCSI, SCSI-3/SCSI-3, 0.8m	1
13.2.2	X6920A	19" Rack Mount Kit for use with Netra st D130 in a SunFire 3800, 4800, 4810, 6800 server rack. Includes front or center fixed mount brackets and front & rear mount rail system.	1
13.2.3	X959A	2 meter external SCSI cable Netra st A1000/D1000 with right angle connector, connects to right hand side of back of array	1
13.3	SG-XTAP4MM-012A	20GB 4mm DDS-4 in a UniPack desktop enclosure.	1
13.3.1	X311L	Localized Power Cord Kit North American/Asian	1

RQS nº 03/2005 - CN - CPMI - CORREIOS
0031
Fls. Nº
3696
Doc:

Accepted By: _____ *Title:* _____ *Date:* _____

0031

NEC

Sun microsystems

Quotation

Invoice Number: **F-BR-14967-G** **[Quote Valid for 29 Days]**

Invoice Date: **23/07/03**

13084 A

Customer :

Sun
Sun Microsystems, Inc.

Tel / Fax : /

Tel / Fax :

We are pleased to quote as follows:

Approved by: A

Reference	F.O.B.	Page
	NULL	{P} of {N}

Item	Product Number	Description	Qty
		Software de Backup - Datacenter BSB	
1		Configuration: EBSDS-700-8570	1
1.1	EBSDS-700-8570	Sun StorEdge(TM) Enterprise Backup Software (EBS) 7.0 Software Documentation.	1
1.2	EBSIN-999-2003	Sun StorEdge(TM) Enterprise Backup Software (EBS) Power Edition Dedicated Storage Node for Windows	14
1.3	EBSIN-999-2107	Sun StorEdge(TM) Enterprise Backup Software (EBS) Dynamic Drive Sharing Option for Linux, Windows, Unix	20
1.4	EBSIN-999-2125	Sun StorEdge(TM) Enterprise Backup Software (EBS) Module for MS Exchange, Windows Client Tier 4 is 8+ processors	8
1.5	EBSIN-999-3304	Sun StorEdge(TM) Enterprise Backup Software (EBS) ClientPak License for Windows NT/Windows 2000	1
1.6	EBSIS-999-2005	Sun StorEdge(TM) Enterprise Backup Software (EBS) Power Edition Dedicated Storage Node for Unix	8
1.7	EBSIS-999-2154	Sun StorEdge(TM) Enterprise Backup Software (EBS) Module for Oracle, UNIX Client	10
1.8	EBSIS-999-2203	Sun StorEdge(TM) Enterprise Backup Software (EBS) Autochanger Software Module 1-400 slots	1
1.9	EBSIS-999-5102	Sun StorEdge(TM) Enterprise Backup Software (EBS) Power Edition for Solaris. Includes 10 client connections, supports unlimited number of clients.	1
1.10	EBSMS-700-2088	Sun StorEdge(TM) Enterprise Backup Software (EBS) 7.0 Media Kit and Documentation	1
1.11	EBSY9-999-2022	Sun StorEdge(TM) Enterprise Backup Software (EBS) Client Connection License for 25 Client Connections	3
		Software de Backup - Datacenter SP	
2		Configuration: EBSDS-700-8570	1
2.1	EBSDS-700-8570	Sun StorEdge(TM) Enterprise Backup Software (EBS) 7.0 Software Documentation.	1
2.2	EBSIN-999-2003	Sun StorEdge(TM) Enterprise Backup Software (EBS) Power Edition Dedicated Storage Node for Windows	7
2.3	EBSIN-999-2107	Sun StorEdge(TM) Enterprise Backup Software (EBS) Dynamic Drive Sharing Option for Linux, Windows, Unix	12
2.4	EBSIN-999-3304	Sun StorEdge(TM) Enterprise Backup Software (EBS) ClientPak License for Windows NT/Windows 2000	1
2.5	EBSIS-999-2005	Sun StorEdge(TM) Enterprise Backup Software (EBS) Power Edition Dedicated Storage Node for Unix	3
2.6	EBSIS-999-2044	Sun StorEdge(TM) Enterprise Backup Software (EBS) Autochanger Software Module 1-256 slots	1
2.7	EBSIS-999-5102	Sun StorEdge(TM) Enterprise Backup Software (EBS) Power Edition for Solaris. Includes 10 client connections, supports unlimited number of clients.	1
2.8	EBSMS-700-2088	Sun StorEdge(TM) Enterprise Backup Software (EBS) 7.0 Media Kit and Documentation	1

Accepted By: ______________ *Title:* ______________ *Date:* ______________

* Software que rodeja o back up

NEC

Sun microsystems

Quotation

Invoice Number: F-BR-14967-G
[Quote Valid for 29 Days]

Invoice Date: 23/07/03

13083

Item	Product Number	Description	Qty
2.9	EBSV9-999-2021	Sun StorEdge(TM) Enterprise Backup Software (EBS) Client Connection License for 5 Client Connections	1
2.10	EBSY9-999-2022	Sun StorEdge(TM) Enterprise Backup Software (EBS) Client Connection License for 25 Client Connections	1
		Licenças dos Clusters, compiladores e fitas DAT	
3	CLSIS-LCO-K999	SunPlex server license for Sun Fire 15k. One license required per server.	11
4	CLA9S-310-99M9	Sun Cluster 3.1 Agents 5/03 Media Kit for SunPlex systems.	2
5	CLUZS-999-99M9	Sun Cluster 3.1 Base Media Kit for SunPlex Systems latest. This part number always refers to the latest release of Sun Cluster 3.1 base software.	2
6	FCCMS-700-T999	Sun ONE Studio 7, Compiler Collection Media Kit, 1 Media Kit only, for SPARC, NO license included.	6
7	FCCYS-700-T999	Sun ONE Studio 7, Compiler Collection, 25-RTU, Slim Kit, contains C/C++, FORTRAN Compilers and Debugger for SPARC, includes software, on-line documentation and specified number of user licenses.	6
8	SG-XMED4MMDDS410	4MM 150-METER DDS4 TAPE CARTRIDGES- PACKAGE OF 10 TAPES	15
9	SG-XMED4MMCL-10	4MM DDS CLEANING TAPES - PACKAGE OF 10 TAPES	3
10	SOL99-090-MAD9	Solaris 9 Full Manual Doc Set, English	4
11	CLSIS-LCO-G999	SunPlex server license for Sun Fire V480. One license required per server.	4
12	CLAIS-30P-9999	Sun Cluster 3.0 Oracle Parallel Server and Real Application Cluster license ONLY. One license required per cluster.	5
13	CLCIS-999-9999	VxVM Cluster Functionality License. To be used with OPS/RAC and SC 3.0 only. One license required per node.	10
14	SG-XMONLIBSWL700	Horizon Monitoring Software for the L700 Version 2.0 key docs., sold seperately from base unit.	2
15	CLAIS-XXS-9999	SunPlex agent license for HA Siebel agent. One license required per cluster.	1
16	VFSSS-999-1B99	VERITAS File System License Tier 1B for V480, E450 and E420R Servers	4
17	VFSSS-999-4C99	VERITAS File System License Tier 4C for SF15K	11
18	SG-XSWBRO-FMG	Brocade Silkworm Fabric Manager 3.0. A host-based, centralized management platform dedicated to administering a multi-switch, multi-fabric Brocade environment. Only one license required per fabric. Other Brocade switches in the SAN can be managed by this version also. Benefits include streamline management of medium and large SANs by allowing administrative functions to be automated across groups of switches. Includes CD and documentation.	2

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0033
Doc: 3696

*Accepted By:*_____ *Title:*_____ *Date:*_____

COMPROVAÇÃO DAS ESPECIFICAÇÕES EXIGIDAS NO EDITAL

2. ASPECTOS GERAIS

REQUISITO	ATRIBUTOS OFERTADOS	ATRIBUTOS OFERTADOS ADICIONALMENTE	CONFIRMA ATENDIMENTO (SIM/NÃO)	PÁGINA DA DOCUMENTAÇÃO TÉCNICA
2.1. Comprovação de Performance para os Equipamentos da Plataforma RISC	O equipamento cotado para o item RISC 01 é o servidor SUN FIRE 15K. Este servidor foi auditado pelo Standard Performance Evaluation Corporation em 09/04/2002 com 72 processadores UltraSPARC III Cu de 1050 Mhz atingindo o resultado de 433.166 ops/s.		SIM	Resulta auditado da SF 15K com 72 processadores UltraSPARC III de 1.05 Ghz www.spec.org/jbb2000/results/res2002q2/jbb2000-20020507-00129.html
2.2. Comprovação de Performance para os Equipamentos da Plataforma INTEL	IBM xSeries 440 – 119.115 tpmc IBM xSeries 360 – 52.587 tpmc IBM xSeries 235 - 37.872 tpmc (projetado).		SIM	http://www.tpc.org/tpcc/results/tpcc_result_detail.asp?id=103040401 http://www.tpc.org/tpcc/results/tpcc_result_detail.asp?id=103022802 http://www.tpc.org/tpcc/results/tpcc_result_detail.asp?id=103071001
2.3. Requisitos gerais	1. Os servidores SUN FIRE 15K são ofertados são novos e saem de fabrica acomodados em embalagens especiais para transporte e adequadas para as suas dimensões e peso. 2. Todos os componentes e documentação técnica necessários para operação do equipamento serão entregues a CONTRATANTE. 3. Conforme demonstrado na documentação de comprovação dos servidores RISC 1, não serão fornecidas nenhuma controladora Fibre Channel ou de Rede integrada a		SIM	1. Conforme " *ATRIBUTOS OFERTADOS*" 2. Conforme " *ATRIBUTOS OFERTADOS*" 1. Referenciar os datasheets da adaptadora de fibre channel (6768A), gigabit ethernet (1150A) e controladora dual SCSI e dual fast ethernet (2222A) que foram anexadas com a documentação para o RISC 01 2. Datasheets da 1150A e 2222A 3. Conforme " *ATRIBUTOS OFERTADOS*"

	placa de sistema do servidor. 4. As placas de rede Gigabit Ethernet requeridas e as placas de rede Ethernet ofertadas adicionalmente possuem apenas uma e duas interfaces por cartão, respectivamente. 5. A CONTRATADA esta ciente desta condição e não cobrara serviços adicionais para as migrações de componentes durante a vigência do contrato.			
2.4. Garantia	A CONTRADA oferecera garantia aos produtos fornecidos durante toda a vigência do Contrato.		SIM	Conforme " *ATRIBUTOS OFERTADOS*"
2.5. Alimentacao eletrica	A CONTRADA se responsabilizará por qualquer adaptação de tensão elétrica para as localidades de instalação dos equipamentos inclusive o fornecimento e instalação de equipamentos adicionais para a compatibilização elétrica.		SIM	Conforme " *ATRIBUTOS OFERTADOS*"
2.6. Assistencia tecnica	A asistência técnica será ofertada conforme o edital.		SIM	Conforme " *ATRIBUTOS OFERTADOS*"
2.7 Recursos minimos de Patricionamento para os Servidores RISC	1. Cada servidores SUN FIRE 15K oferecido nesta proposta esta configurado com o hardware necessário para configurar ate 8 (oito) partições físicas sem a necessidade de hardware ou software adicional. Além disto, o servidor também possui escalabilidade para atingir ate 18 (dezoito) partições físicas. Por ser uma partição física, todas as	Equipamentos possuem escalabilidade ate 18 partições por servidor. Partições isolam não apenas erros de Sistema Operacional, mas possuem também isolamento de erros de hardware. Partições podem ser reconfiguradas dinamicamente sem necessidade de reboot.	SIM	1. http://www.sun.com/servers/comparison/sunfire/index.html 2. SF 15K System Overview: pg 1-2 "two System Control boards", pg 1-3 grifar todo o texto do item 1.1.3; SMS 1.3 Admin Guide pg 5 grifar todo o segundo parágrafo; SMS pg 6 "Network Connection..." grifar todo o parágrafo

partições possuem isolamento de falhas de software e hardware em outras partições (fault-isolated).

2. As partições em um SUN FIRE 15K são configuradas a partir da placa chamada System Control boards (SC) que acompanha o gabinete básico do servidor em configuração redundante (uma na traseira e outra na frente do gabinete do servidor). O acesso a SC para configurar as partições se da através de uma interface ethernet normalmente a partir de uma estação de controle em rede privada com a SC. Como as SC são acessadas via rede, duas (para melhor redundância) estações consoles podem ser usadas para gerenciamento das partições. Estamos ofertando as duas estações Sun Blade 150 por localidade para este fim.
3. Conforme mencionado acima as particoes da SUN FIRE 15K são físicas e isoladas de erros de software (inclusive do sistema operacional e/ou hardware de outras partições.
4. As partições ou domínios da SUN FIRE 15K são dinâmicos, ou seja, permitem a migração de. recursos de CPU, memória e IO, sem a necessidade de reboot, entre partições.

abaixo deste titulo.

3. System Overview pg 2-1 grifar todo o segundo e terceiro parágrafos. Pg 2-3 grifar o primeiro parágrafo após Domain Fault isolation
4. System Overview: Pg 1-8 todos os parágrafos do inicio do item 1-4 ate o parágrafo que começa com a palavra Board (inclusive)

2.7 Recursos mínimos de Particionamento para os Servidores RISC	1. As SC's são as responsáveis para criação e gerenciamento das partições, elas executam o software denominado System Management Software (SMS) que controlam as SC's para realizarem estas funções. O SMS acompanha o sistema básico de todas as SUN FIRE 15K. 2. Os notebooks estão sendo ofertado conforme requisitado		SIM	1. SMS 1.3 Admin Guide: pg 5 grifar todos os dois primeiros paragrafos; pg 6 "Network Connection..." grifar todo o paragrafo abaixo deste titulo "The nature of ....". 2. Conforme " *ATRIBUTOS OFERTADOS*"
2.8. Recursos mínimos de gerenciamento do hardware requeridos para os servidores INTEL	Ofertado software IBM Director 4.1		SIM	Conforme " *ATRIBUTOS OFERTADOS*" *
2.9. Recursos mínimos de hardware e software para os servidores INTEL	Servidores IBM xSeries 440, 360 e 235, configurados conforme edital		SIM	http://www5.pc.ibm.com/us/products.nsf/$wwwPartNumLookup/_86877RX http://www5.pc.ibm.com/us/products.nsf/$wwwPartNumLookup/_86869RX http://www-132.ibm.com/webapp/wcs/stores/servlet/ProductDisplay?productId=8599793&storeId=1&langId=-1&categoryId=2543009&dualCurrId=73&catalogId=-840
2.10. Recursos mínimos de hardware e software para os servidores RISC adicionais	4. Os servidores cotados adicionalmente para servir como servidores de backup conforme requisitado no item 5.15 do Anexo 1-B são 04 (quatro) servidores SUN FIRE V480. Estes servidores serão instalados em racks Sun RACK 900 de 19";		SIM	1. Datasheet das V480 & datasheet do Rack 900; 2. Conforme " *ATRIBUTOS OFERTADOS*" 3. Capítulo 50 do manual do administrador do Solaris 9 (procurar por UFS logging). Este manual está disponível

*º quantitativo de servidores para esta funcionalidade encontra-se expresso na página 43.

NEC

8079

5. Os servidores V480's possuem licenças do Solaris 9 para número ilimitado de usuários; 6. O Solaris 9 permite que os sistemas de arquivos sejam do tipo UFS logging, o qual habilita o journalling ou logging das modificações no sistema de arquivo antes de serem alterados em disco; 7. O Solaris 9 também inclui as ferramentas ufsdump e ufsrestore que realizam backup e restore de sistemas de arquivos em dispositivos remotos via rede; 8. As licenças do Concord SystemEdge estão sendo oferecidas para os servidores; 9. Os servidores V480 possuem e estão configurados com fontes redundantes , hot-swappable, bivolt (100-240 VAC) e que operam entre 47-63 Hertz; 10. As fontes de alimentação para os V480's são redundantes, independentes com entradas para alimentação redundante; 11. Cada servidor V480 está configurado com duas placas adaptadoras PCI Sun GigaSwift que operam a 10/100/1000 Base-T, atendem os padrões IEEE 802.ab e 802.u e possuem MIB's para gerenciamento SNMP;			no docs.sun.com; 4. Capítulo 47 do manual do administrador do Solaris 9 (procurar por "You can run the ufsdump command from a single.." e Capítulo 49 do manual do administrador do Solaris 9 (procurar por "device name (local or remote)". Estes manuais estão disponíveis no docs.sun.com. 5. Conforme " *ATRIBUTOS OFERTADOS*" 6. datasheet do V480; 7. datasheet do V480; 8. Doc sunsolve 41665 (fazer search para localizar MIB e 802.ab e 802.u

NEC

2.10. Recursos mínimos de hardware e software para os servidores RISC adicionais	1. As interfaces das adaptadoras Sun GigaSwift permitem o uso de conectores RJ-45 e cabeamento CAT 5 ou superior, a saber, CAT 6. 2. Cada servidor V480 está configurado com uma unidade de fita DDS-4, 10 (dez) fitas DDS-4 e 2 (duas) fitas de limpeza.		SIM	1. Doc sunsolve 41665 (fazer search por CAT 5 ou better) 2. Conforme " *ATRIBUTOS OFERTADOS*"
2.11. Comprovação dos requisitos técnicos	O modelo VIII do Anexo 3 está preenchido e a documentação anexada conforme solicitado.		SIM	Conforme " *ATRIBUTOS OFERTADOS*"
2.12. Organização da documentação técnica	Documentação, mídias em CD e atualizações dos softwares serão fornecidas.		SIM	Conforme " *ATRIBUTOS OFERTADOS*"
2.13. Suporte remoto	Será montada uma estrutura segura de acesso remoto a rede corporativa dos Correios. Adicionalmente, serão oferecidos os serviços do Sun Remote Services Net Connect para monitoramento pro-ativo com geração de relatórios e detecção e notificação de eventos.		SIM	Incluir datasheet do Net connect
2.14. Configuração das ferramentas de gerenciamento	Serviços de configuração prestados conforme descrito neste item.		SIM	Conforme " *ATRIBUTOS OFERTADOS*"

3 CONECTIVIDADE DA REDE

3.1 Switch Tipo 1 (Layer 3 GE)

ATRIBUTO	ATRIBUTOS OFERTADOS	ATRIBUTOS OFERTADOS ADICIONALMENTE	CONFIRMA ATENDIMENTO (SIM/NÃO)	PÁGINA DA DOCUMENTAÇÃO TÉCNICA
1 – Características Físicas	Os switches Cisco da série Cataliyst 6513 são switches do tipo chassis	-	SIM	Data Sheet "Cisco Catalyst 6500 Series Switch " (c6000_ds.pdf) em figura 1 da página 1
2 – Gabinete	(1) Chassis para ser instalado em RACK de 19. a ser fornecido juntamente com o equipamento. Deve vir acompanhado de kit de suporte específico para montagem em RACK de 19. (2) Com todos os módulos de interface, fontes de alimentação e ventiladores do tipo HOT-SWAPPABLE/HOT-PLUGGABLE.	-	SIM	Vide planilha de quantitativos.
3 – Portas Gigabit Ethernet	(1) Dispõe 16 interfaces Gigabit Ethernet no padrão 1000BASE-SX , compatíveis com o padrão IEEE 802.3z; (2) Dispõe 192 portas 10/100/1000BASE-T, autosensing, compatíveis com o padrão IEEE 802.3ab, para cabos UTP Categoria 6 e	-	SIM	Data Sheet " c60ge_ds.pdf " (1) página 1 no primeiro item de " Notes " (2) vide planilha de quantitativos. (3) O equipamento possui no total 13 slots, sendo que 11 estão disponíveis para

ATRIBUTO	ATRIBUTOS OFERTADOS	ATRIBUTOS OFERTADOS ADICIONALMENTE	CONFIRMA ATENDIMENTO (SIM/NÃO)	PÁGINA DA DOCUMENTAÇÃO TÉCNICA
	conectores RJ-45; (3) Suporta inclusão futura de, no mínimo, mais 48 portas 10/100/1000BASE-T.			inserção de placas de interfaces e serviços.
4 – Hot-swapping	O produto ofertado é do tipo Hot-Swapping HOTSWAPPABLE/HOT-PLUGGABLE. em todos os módulos, permitindo as manobras de inserção/retirada de módulos sem interrupção do funcionamento dos demais.	-	SIM	Data Sheet " 01overvw " pagina 1-85.
5 – Balanceamento de carga	(1) Implementa o balanceamento de servidores (tráfego) localizados em redes diferentes da rede deste SWITCH TIPO 01, baseado nos algoritmos Weighted Round Robin, Weighted Least Connections e URL Hashing; (2) Implementa o balanceamento baseado em protocolos das camadas 4 a 7 (RM-OSI), incluindo TCP, UDP, FTP, DNS, SMTP , HTTP e IPSec; (3) Possui a capacidade de vincular as conexões de cada cliente a um mesmo servidor por meio de endereçamento IP da fonte, de cookies e de Secure	-	SIM	Data sheet " overview.pdf " (1) pagina 1-4 em Table 1-2 CSM Feature Set Description. (2) pagina 1-4 em Table 1-2 CSM Feature Set Description. (3) Conforme atributos ofertados (4) Vide Data Sheet " c6000_des.pdf " pagina 17-32. (5) Conforme atributos ofertados (6) Conforme atributos ofertados

ATRIBUTO	ATRIBUTOS OFERTADOS	ATRIBUTOS OFERTADOS ADICIONALMENTE	CONFIRMA ATENDIMENTO (SIM/NÃO)	PÁGINA DA DOCUMENTAÇÃO TÉCNICA
	Socket Layer por identificador de sessão; (4) O balanceamento de tráfego possui redundância e alta disponibilidade com os outros SWITCHES do mesmo tipo, através dos protocolos HSRP ou VRRP, de maneira que, em caso de falha de um dos módulos de balanceamento, o estado de todas as conexões seja remanejado para o módulo redundante de forma totalmente transparente para os usuários; (5) Implementa adicionalmente qualidade de serviço (QoS) com diferenciação/priorização para todo o tráfego balanceado; (6) Suporta balanceamento global para servidores localizados em sites com diferentes saídas para a Internet.			
7 – Gerenciamento	Suporta as bases SNMP e MIB II, conforme RFC 1213, bem como os grupos RMON I (quatro grupos) e todos os grupos RMON II.	-	SIM	Data sheet " intro.pdf " em Network Management página 4 ou Data Sheet " supe_ds.pdf " em Extensive management tools página 2

ATRIBUTO	ATRIBUTOS OFERTADOS	ATRIBUTOS OFERTADOS ADICIONALMENTE	CONFIRMA ATENDIMENTO (SIM/NÃO)	PÁGINA DA DOCUMENTAÇÃO TÉCNICA
8 – Conectividade	Permiti 8 (oito) grupos de agregação com, 8 (oito) enlaces cada, conforme padrão IEEE 802.3ad.	-	SIM	Data sheet "c60ge_ds.pdf " página 1 no quarto item " Notes "
9 – Roteamento	Realiza o roteamento na camada 3	-	SIM	Data sheet " supe_ds.pdf " em Scalable Performance página 5.
10 – QoS	Implementa 4 (quatro) filas de prioridade em cada porta, permitindo a priorização do tráfego de rede e uma integração transparente de dados, voz e vídeo através do protocolo IEEE 802.1p com CoS (class-of-Service).	-	SIM	Data sheet " buffe_wp.pdf " pagina 2
11 – Fonte de Alimentação	(1) Possui o 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., (2) Freqüência de 60 (sessenta) Hertz; (3) 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	-	SIM	Data sheet " 01overvw.pdf " (1) pagina 1-3 (2) AC Power Supply (3) pagina 1-3

ATRIBUTO	ATRIBUTOS OFERTADOS	ATRIBUTOS OFERTADOS ADICIONALMENTE	CONFIRMA ATENDIMENTO (SIM/NÃO)	PÁGINA DA DOCUMENTAÇÃO TÉCNICA
	defeito ou por falta de alimentação elétrica em um dos 2 (dois) circuitos, o equipamento continue a funcionar sem prejuízo das aplicações.			
12 – Forwarding Performance	Suporta 100 Mpps para Layer 2, Layer 3 e Layer 4.	-	SIM	Conforme atributos ofertados
13 - Gerais	(1) Implementa o protocolo STP (Spanning Tree Protocol) para cada VLAN configurada (uma sessão STP por grupo de portas); (2) Suportar múltiplos agrupamentos simultâneos de no mínimo 8 interfaces cada um em quaisquer interfaces de rede e em módulos diferentes de forma a agregar taxa de transmissão; (3) Possui a facilidade de trunking (IEEE 802.1Q) com outros switches; (4) É capaz de implementar no mínimo 2 sessões simultâneas de espelhamento de tráfego, entrada e saída, de interfaces ou de VLANs; (5) Será fornecida a ferramenta que permita o gerenciamento dos equipamentos e de todas as suas interfaces através de	-	SIM	Data sheet " intro.pdf " (1) pagina 1-2 em Spanning Tree Protocol (2) Conforme atributos ofertados (3) pagina 1-2 em VLAN e pagina 1-3 em VLAN Trunks. (4) Conforme atributos ofertados (5) Conforme atributos ofertados (6) Conforme atributos ofertados

ATRIBUTO	ATRIBUTOS OFERTADOS	ATRIBUTOS OFERTADOS ADICIONALMENTE	CONFIRMA ATENDIMENTO (SIM/NÃO)	PÁGINA DA DOCUMENTAÇÃO TÉCNICA
	aplicação gráfica; (6) Será fornecido servidores adicionais para a instalação desta gerência.			*

* O quantitativo de servidores para esta finalidade encontra-se expresso na página 23.

3.2 Switch Tipo 2 (FE)

ATRIBUTO	ATRIBUTOS OFERTADOS	ATRIBUTOS OFERTADOS ADICIONALMENTE	CONFIRMA ATENDIMENTO (SIM/NÃO)	PÁGINA DA DOCUMENTAÇÃO TÉCNICA
1 – Switch	Os switches Cisco da série Catalyst 2950 são switches de configuração fixa, empilháveis, provendo conectividade Ethernet e Gigabit Ethernet "wire-speed". O modelo ora ofertado, o Catalyst 2950G-48, possui 48 portas Ethernet além de 2 conversores GBIC para uplinks Gigabit Ethernet. A tecnologia GigaStack permite a concentração de até 432 portas 10/100 (9 switches) por pilha.	-	SIM	Data sheet "*Cisco Catalyst 2950 Series Switches with Cisco Enhanced`Image Software*" (cdccont_0900aecd8009d987.pdf), páginas 1 e 2 Data sheet "*GigaStack Gigabit Interface Converter*" (gbic_ds.pdf), página 1
2 – Interfaces Fast e Gigabit Ethernet	O Catalyst 2950G-48 possui 48 portas Ethernet/Fast Ethernet autosense, para conectores RJ45, além de 2 conversores GBIC para até 2 uplinks Gigabit Ethernet. Foram propostos os GBICs compatíveis com o padrão 1000Base-SX, utilizando-se a tecnologia *Cisco GigaStack Gigabit Interface Converter*. O segundo GBIC de cada switch estará disponível para futuras expansões.	-	SIM	Data sheet "*Cisco Catalyst 2950 Series Switches with Cisco Enhanced`Image Software*" (cdccont_0900aecd8009d987.pdf), páginas 1 e 12
3 – Gerais	(1) Padrões IEEE: • 802.3u • 802.1Q • 802.1p	-	SIM	Data sheet "*Cisco Catalyst 2950 Series Switches with Cisco Enhanced`Image Software*" (cdccont_0900aecd8009d987.pdf),

ATRIBUTO	ATRIBUTOS OFERTADOS	ATRIBUTOS OFERTADOS ADICIONALMENTE	CONFIRMA ATENDIMENTO (SIM/NÃO)	PÁGINA DA DOCUMENTAÇÃO TÉCNICA
	(2) Gerenciamento • SNMP • Suporte a MIB II • Grupos RMON I (3) Storm control para tráfegos broadcast, unicast e multicast , por porta (4) Prevenção contra flooding IP Multicast (IGMP snooping)			(1) página 14 (2) páginas 13 e 15 (3) página 7 (4) página 7
3 – Gerais (Continuação)	(1) 4 filas de prioridade por porta (IEEE 802.1p - CoS) (2) Instalação em racks 19" (3) VLANs (IEEE 802.1Q) e trunking de VLANs entre portas dos switches da pilha (4) Protocolo STP para cada VLAN configurada ou por grupo de portas A ferramenta de Gerência que permite o gerenciamento dos switches Catalyst 2950G-48 via interface gráfica é o Cisco Works, módulos LAN (LAN Management Solution) / WAN (Routed WAN Management Solution), ofertados na presente proposta.	-	SIM	Data sheet "*Cisco Catalyst 2950 Series Switches with Cisco Enhanced Image Software*" (cdccont_0900aecd8009d987.pdf), (1) página 4 (2) página 16 (3) página 7 (4) página 7 Data sheets "*LAN Management Solution*" (camp_ds.pdf) e prospecto "*Routed WAN Management Solution 1.3*" (rwan_op.pdf)
4 – Fonte de Alimentação	(1) A fonte de alimentação é redundante e auto-regulável.	-	SIM	Data sheet "*Cisco Catalyst 2950 Series Switches with Cisco Enhanced Image Software*" (cdccont_0900aecd8009d987.pdf), (1) páginas 7 e 15

NEC

3.3. SWITCH TIPO 3 (FC)

REQUISITO	ATRIBUTOS OFERTADOS	ATRIBUTOS OFERTADOS ADICIONALMENTE	CONFIRMA ATENDIMENTO (SIM/NÃO)	PÁGINA DA DOCUMENTAÇÃO TÉCNICA
1. Recursos Básicos	1. Estamos oferecendo 6 (seis) switches Brocade Silkworm 12000 com 64 portas (expansível a 128 portas) Fibre Channel operando a 2 Gbit/sec para interligação às redes SAN da CONTRATANTE. Estes switches são comercializados pela SUN Microsystems em regime de OEM com a Brocade; 2. Os switches Silkworm 12000 permitem a configuração de portas de forma independente; 3. As portas do Silkworm 12000 são agrupadas em módulos hot-swappable de 16 portas; 4. O Silkworm 12000 cresce de forma modular acrescentando-se modulos de 16 portas. 5. Os switches serão montados em rack de 19" conforme solicitado	Switches expansível a 128 portas FC	SIM	1. Datasheet do Brocade Silkworm 12000 com logo SUN 2. FM_userguide: Através do software Fabric Manager, as portas do Silkworm 12000 podem ser renomeadas (pg. 4-5), agrupadas por tipo ou Port groups (pg. 6-3) , inseridas em zonas ou port zoning (pg. 8-3) , habilitadas ou desabilitadas (pg. D-6), etc. 3. Datasheet do 12000 procurar por "up to eight 16-port Fibre Channel modules" e "modules hot-swappable" 4. Datasheet do 12000 procurar por "up to eight 16-port Fibre Channel modules" 5. Conforme " *ATRIBUTOS OFERTADOS*"
2. Portas Ethernet	O Silkworm 12000 possui uma porta Fast Ethernet 10/100 BaseT que serve de acesso para monitoramento do switch. O switch também suporta o gerenciamento via protocolo SNMP		SIM	Datasheet do 12000, procurar por ethernet e SNMP
3. Cabeamento	Estamos ofertando fibras óticas multimodo com conectores LC para todas as portas do switch mais os 20% adicionais		SIM	Conforme " *ATRIBUTOS OFERTADOS*"

	solicitados.			
4. Recursos	1. Os switches serão acompanhados de todos os recursos de hardware, software, cabos e manuais, etc. para a instalação, configuração e gerenciamento e utilização; 2. Estamos ofertando o software Fabric Manager versão 4.0 para gerenciamento da rede SAN mais uma estação PC para servir de console de gerenciamento por localidade. 3. O Fabric Manager realiza a descoberta automática dos elementos da SAN através de utilitário incluso no software; 4. O Fabric Manager criar um mapa gráfico da topologia da SAN ilustrando as interconexões FC dos dispositivos de SAN, a saber, servidores, switches, storage, etc. em uma visão única.		SIM	1. Conforme " *ATRIBUTOS OFERTADOS*" e Quickstart do 12000 pg. 3/6 "Items included with the Silkworm 12000"; 2. Conforme " *ATRIBUTOS OFERTADOS*" e Datasheet do FM; 3. User guide do FM, pgs 4-2 e 4-3 4. Datasheet do FM (grifar figura 1) e User guide pgs. 14-3 e 14-4. O Fm demonstra os dispositivos e switches da SAN.
5. Compatibilidade e Integração	O Silkworm 12000 adere aos padrões Fibre Channel;		SIM	Datasheet 12000 – Fibre Channel Standards
6. Fonte de Alimentação	1. O Silkworm 12000 possui 4 (quatro) fontes internas redundantes e hot-swappable que operam a 200-240 VAC e a 47-63 Hertz. Para o CCD de SP serão realizadas as		SIM	1. Datasheet do 12000, procurar por power "four AC-DC power" "dual AC inputs". 2. Datasheet do 12000, procurar por power "four AC-DC power" "dual AC inputs".

	adequações elétricas necessárias para compatibilizar o equipamento a alimentação elétrica local. 2. O switch possui duas entradas de alimentação AC independentes que podem ser alimentadas por circuitos distintos e continuar funcionando em caso de falha de um circuito.			

NEC

3.4 Switch Tipo 4 (KVM)

ATRIBUTO	ATRIBUTOS OFERTADOS	ATRIBUTOS OFERTADOS ADICIONALMENTE	CONFIRMA ATENDIMENTO (SIM/NÃO)	PÁGINA DA DOCUMENTAÇÃO TÉCNICA
1 – Descrição	A NEC do Brasil está ofertando duas redes de comutação KVM (uma em Brasília e a outra em São Paulo) compostas pelo modelo ServSwitch® Affinity da Blackbox, equipamento já existente hoje nas dependências da ECT. Com o ServSwitch® Affinity, é possível acessar até 1000 servidores a partir de até 16 teclados, monitores e mouses. Cada chassi suporta o máximo de 4 usuários e 16 CPUs. Pode-se utilizar cabos de expansão para cascatear vários chassis e conectar até 4, 8, ou 16 usuários e um total de 1000 CPUs. O multiplataforma ServSwitch® Affinity, adaptável a racks 19", caracteriza-se por sua flexibilidade e facilidade de operação, sportando CPUs PC, Sun®, ou PC UNIX® e teclados, monitores e mouses usando os cabos adaptadores.	-	SIM	Documento 22921.pdf (ServSwitch Affinity)
2 – Quantidade de Portas	Estão sendo fornecidas um total de 160 portas de comutação para o CCD de Brasília e 96 portas para o CCD de São	-	SIM	-

ATRIBUTO	ATRIBUTOS OFERTADOS	ATRIBUTOS OFERTADOS ADICIONALMENTE	CONFIRMA ATENDIMENTO (SIM/NÃO)	PÁGINA DA DOCUMENTAÇÃO TÉCNICA
	Paulo. Estas portas incluem o atendimento mínimo a 72 servidores legados (24 RISC e 48 INTEL) em Brasília e 48 (INTEL) em São Paulo.			
3 – Consoles	Os 12 consoles fornecidos (8 em Brasília e 4 em S. Paulo) são compostos de: • Monitores 17", dot pitch 0,28, resolução máxima de 1280x1240, bivolt, 60Hz; • Mouse padrão PS/2 • Teclado padrão ABNT2 Foram considerados ainda os respectivos cabos para conexão ao switch KVM, bem como os cabos extensores para mouse e teclado, sempre que aplicáveis.	-	SIM	Documento 22921.pdf (Servswitch Affinity), p. 2
4 – Solução Alternativa para Comutação dos Servidores INTEL	A NEC do Brasil não está oferecendo esta alternativa na presente proposta.	-	-	-
5 – Gerais	ServSwitch® Affinity oferece ainda: • Memória Flash para facilitar a atualização do firmware. • Completa emulação de teclado e mouse. • Resolução de vídeo de até 1280 x 1024. • Fonte de alimentação autosense integrada. • Comutação de CPU a partir do teclado, menus de tela, ou porta RS-232. Tecnologia de menus de tela	-	SIM	Documento 22921.pdf (Servswitch Affinity), p. 2

ATRIBUTO	ATRIBUTOS OFERTADOS	ATRIBUTOS OFERTADOS ADICIONALMENTE	CONFIRMA ATENDIMENTO (SIM/NÃO)	PÁGINA DA DOCUMENTAÇÃO TÉCNICA
	impressionante: • Caixas de mensagem surgem sobre o vídeo corrente. • Menus de fácil uso para executar todas as configurações. • Apresenta 80 colunas/25 linhas de texto em 16 cores. • Os nomes das CPUs podem ser mostradas em seis diferentes cores. • Escolha das CPUs a partir de uma janela com cores e posição ajustáveis. • Protetores de tela com quatro padrões. • Caracteres de acordo com o ISO8859-I para suporte internacional.			

3.5 Switch Tipo 5 (Concentrador de VPN's)

ATRIBUTO	ATRIBUTOS OFERTADOS	ATRIBUTOS OFERTADOS ADICIONALMENTE	CONFIRMA ATENDIMENTO (SIM/NÃO)	PÁGINA DA DOCUMENTAÇÃO TÉCNICA
1 – Descrição	O Cisco VPN 3060 é um concentrador VPN composto por sistema integrado de hardware e software, com o objetivo de concentrar, configurar e monitorar acessos remotos via VPN.	-	SIM	Data Sheet "*Cisco VPN 3000 Series Concentrator*" (vpn3k_ds.pdf), pg. 1
2 – Características e Funcionalidades do Sistema	(1) Capacidades de firewall; (2) Protocolos de tunelamento PPTP, IPsec, L2TP, L2TP/IPsec for Windows 2000, NAT transparent IPSEC; (3) Suporte a certificados digitais padrão X.509 v.3; (4) Alta disponibilidade, com redundância e capacidade de tolerância à falhas (failover); (5) Suporte ao gerenciamento de chaves do tipo IKE; Capacidade de registrar eventos e de envio de notificações por e-mail; (6) Protocolos de roteamento RIP, RIP2, OSPF e estático; (7) Permitir que as	-	SIM	Data Sheet "*Cisco VPN 3000 Series Concentrator*" (vpn3k_ds.pdf): (1) item Security, pg. 4 (2) item High Performance, Distributed-Processing Architecture, pg. 4 (3) item Authentication and Accounting Servers, pg. 7 (4) item High Availability, pg. 4 (5) item Key Management, pg. 6 (6) item Routing, pg. 6 (7) (8) item Embedded LAN Interfaces, pg. 5

ATRIBUTO	ATRIBUTOS OFERTADOS	ATRIBUTOS OFERTADOS ADICIONALMENTE	CONFIRMA ATENDIMENTO (SIM/NÃO)	PÁGINA DA DOCUMENTAÇÃO TÉCNICA
	configurações e políticas de acesso sejam aplicadas ao cliente no momento em que a conexão for estabelecida; (8) 3 interfaces 10BaseT/BaseTX; (9) Para haver a integração com um sistema de autenticação externa, estamos fornecendo a solução Cisco Secure Access Control Server: (10) Capacidade de Autenticação de no mínimo 5.000 usuários; (11) Suporte ao padrão LDAP; (12) Integração com o domínio Microsoft Windows, compartilhando bases de grupos, usuários e permissões. (13) Permitir configuração de níveis de acesso administrativos; (14) Permitir a configuração e aplicação de políticas de segurança nas estações clientes; (15) Capacidade de gerenciamento de política para usuários e grupos;			(9) vide planilha de quantitativos (10) Data Sheet "*Cisco Secure Access Control Server Solution Engine Q&A*" (acsqp_qp.pdf): pg. 6 (11) Data Sheet "*Cisco Secure Access Control Server Solution Engine Q&A*" (acsqp_qp.pdf): pg. 6 (12) Data Sheet "*Cisco Secure Access Control Server Solution Engine Q&A*" (acsqp_qp.pdf): item Total Cost of Ownership, pgs 1 e 2 (13) Data Sheet "*Cisco Secure Access Control Server Solution Engine*" (acspp_ds.pdf): pg. 2 (14) Data Sheets "*Cisco Secure Access Control Server Solution Engine*" (acspp_ds.pdf), pg. 2 e "*Cisco Secure Access Control Server Solution Engine Q&A*" (acsqp_qp.pdf), pg 1 (15) "*Cisco Secure Access Control Server Solution Engine Q&A*" (acsqp_qp.pdf), pg. 1 (16) Data Sheet "*Cisco Secure Access Control Server Solution Engine*" (acspp_ds.pdf): pg. 2

ATRIBUTO	ATRIBUTOS OFERTADOS	ATRIBUTOS OFERTADOS ADICIONALMENTE	CONFIRMA ATENDIMENTO (SIM/NÃO)	PÁGINA DA DOCUMENTAÇÃO TÉCNICA
	(16) Controle de tempo e horário de acesso do usuário; (17) Suporte ao gerenciamento utilizando SNMP MIB-II; (18) O sistema possui uma ferramenta de gerenciamento que possibilita a verificação de estatísticas de tráfego criptografado, negociações de handshake e resposta a pacotes; (19) Possibilidade de crescimento (escalabilidade) conforme demanda, com configuração e gerência centralizada; (20) O sistema possui a capacidade de geração de relatórios gerenciais, com informações como: número de túneis estabelecidos, tráfego transferido, clientes com maior geração de tráfego, entre outras.			(17) Essa característica é suportada diretamente pelo concentrador VPN 3060, conforme o documento "*Management Protocols*" (mgtproto1.pdf), pg. 9-1 (19) Data Sheet "*Cisco Secure Access Control Server Solution Engine*" (acspp_ds.pdf): pg. 1 *
2 – Características e Funcionalidades do Sistema (continuação)	(1) O sistema de gerenciamento está sendo disponibilizado em hardware do tipo servidor, de forma exclusiva, sendo 01 (um) sistema para o CCD de Brasília-DF e 01 (um) sistema para o CCD de São Paulo-SP.	-	SIM	(1) vide planilha de quantitativos (2) vide planilha de quantitativos

* O quantitativo de servidores para esta solicitada encontra-se expresso na página 23.

NEC

ATRIBUTO	ATRIBUTOS OFERTADOS	ATRIBUTOS OFERTADOS ADICIONALMENTE	CONFIRMA ATENDIMENTO (SIM/NÃO)	PÁGINA DA DOCUMENTAÇÃO TÉCNICA
	(2) O sistema, está integrado em um mesmo framework dos SERVIDORES DE SEGURANÇA LÓGICA TIPO 1 e TIPO 2, ROTEADOR TIPO 1 e SISTEMA DE DETECÇÃO DE INTRUSÃO.			
3 – Características e Funcionalidades do Software Cliente VPN	Número mínimc de 5.000 licenças; Auto-atualização, realizando atualizações automáticas sem necessidade da intervenção do usuário; Personal firewall; Suporte aos sistemas operacionais Windows 95, 98, ME, NT 4.0, 2000 e XP; Interface padronizada, com o logotipo da Contratada.	-	SIM	
4 – Características de Desempenho	(1) Capacidade de tratar no mínimo 5.000 usuários simultâneos; (2) encriptação mínima de 100Mbps.	-	SIM	Data Sheet "*Cisco VPN 3000 Series Concentrator*" (vpn3k_ds.pdf): (1) item Cisco VPN 3060 Concentrator, pg. (2) Table1, pg. 3
5 – Fonte de Alimentação	(1) Deverá possuir alimentação elétrica de acordo com a localidade onde serão instalados os equipamentos, conforme subitem 2.5., freqüência de 60 (sessenta) Hertz;		SIM	Data Sheet "*Cisco VPN 3000 Series Concentrator*" (vpn3k_ds.pdf): (1) Table 3, pg. 8 (2) item High Availability, pg.

* O quantitativo de usuários, para ser atendido, encontra-se expresso na página 23.

NEC

ATRIBUTO	ATRIBUTOS OFERTADOS	ATRIBUTOS OFERTADOS ADICIONALMENTE	CONFIRMA ATENDIMENTO (SIM/NÃO)	PÁGINA DA DOCUMENTAÇÃO TÉCNICA
	(2) 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.			

3.6 Roteador Tipo 1

ATRIBUTO	ATRIBUTOS OFERTADOS	ATRIBUTOS OFERTADOS ADICIONALMENTE	CONFIRMA ATENDIMENTO (SIM/NÃO)	PÁGINA DA DOCUMENTAÇÃO TÉCNICA
1 – Router	(1) Estrutura de chassis modular com: • 2 portas 10/100 integradas • 2 slots AIM (advanced integration modules) • 3 slots WIC (WAN interface card) • 4 slots NM (network module) • 2 slots HDSM (high density service module) (2) Montável em rack 19"	-	SIM	Data sheet "*Cisco 3700 Series Multiservice Access Routers*" (3700a_ds.pdf) (1) página 3 (2) página 3
2 – Processamento	(1) Capacidade de roteamento de 225.000 pacotes/segundo	-	SIM	Data sheet "*Cisco 3700 Series Multiservice Access Routers*" (3700a_ds.pdf) (1) página 11
3 – Interfaces	(1) 3 interfaces 10/100Base-TX – 2 integradas e um NM (2) 8 interfaces seriais síncronas V.35 (3) 2 interfaces ATM E3 (NM) (4) 1 interface Gigabit Ethernet (NM)	-	SIM	Data sheet "*Cisco 3700 Series Multiservice Access Routers*" (3700a_ds.pdf), páginas 3 e 10
4 – Geral	(1) Gerenciamento • SNMP • MIB II (RFC 1213) (2) Protocolo SSH (3) Telnet para linha de comando (4) Proteção contra ataques do	-	SIM	Data sheet "*Cisco 3700 Series Multiservice Access Routers*" (3700a_ds.pdf)

NEC

ATRIBUTO	ATRIBUTOS OFERTADOS	ATRIBUTOS OFERTADOS ADICIONALMENTE	CONFIRMA ATENDIMENTO (SIM/NÃO)	PÁGINA DA DOCUMENTAÇÃO TÉCNICA
	tipo DoS (5) Suporte para Syslog Externo (6) Atualização de software via rede (7) Autenticação via RADIUS ou TACACS (8) Interface de comando protegida com senha (9) Protocolo HSRP, similar ao VRRP (10) PIM para roteamento Multicat (11) Roteamento RIP (v1 e 2), OSPF, BGP-4 (12) DHCP (13) Suporte para 1024 rotas estáticas (14) BGP-4 • Route reflectors • Route Confederations • Route Aggregation • IGP Synchronization • Route Flap Dampering			
4 - Geral (continuação)	(1) Police-based routing (2) NAT (3) VoIP e VoFR (4) Codecs G.711 e G.729 (5) Protocolo H.323 A ferramenta de Gerência que permite o gerenciamento dos roteadores Cisco 3745 via interface gráfica é o Cisco Works, módulos LAN (LAN Management Solution) / WAN (Routed WAN Management	-	SIM	Data sheet "*Cisco 3700 Series Multiservice Access Routers*" (3700a_ds.pdf) (3) página 8 e 5 (5) página 8 Data sheets "*LAN Management Solution*" (camp_ds.pdf) e prospecto "*Routed WAN Management Solution 1.3*" (rwan_op.pdf)

ROS nº 037/2003 - CN - CPMI - CORREIOS
Fls. Nº 0068
DOC: 3696

quantitativo de servidores para esta funcionalidade encontra-se exposto na página 23.

NEC

13056

ATRIBUTO	ATRIBUTOS OFERTADOS	ATRIBUTOS OFERTADOS ADICIONALMENTE	CONFIRMA ATENDIMENTO (SIM/NÃO)	PÁGINA DA DOCUMENTAÇÃO TÉCNICA
	Solution). Esta ferramenta já foi descrita no tópico 3 do item 3.2 – Switches Tipo 2			
5 – Fonte de alimentação	Fonte de alimentação interna redundante, bivolt, auto-ajustável, 60Hz	-	SIM	Data sheet "*Cisco 3700 Series Multiservice Access Routers*" (3700a_ds.pdf) (1) página 11 e 12

NEC

3.7 Roteador Tipo 2

ATRIBUTO	ATRIBUTOS OFERTADOS	ATRIBUTOS OFERTADOS ADICIONALMENTE	CONFIRMA ATENDIMENTO (SIM/NÃO)	PÁGINA DA DOCUMENTAÇÃO TÉCNICA
1 – Router – Processamento	(1) Capacidade: 12 Kpps (2) A ser montado em bandeja, dentro dos racks 19"	-	SIM	(1) http://www.cisco.com/en/US/partner/products/hw/routers/ps221/products_qanda_item09186a00800918d1.shtml (2) Data sheet "*Cisco 1751 Modular Access Router*" (C1751_ds.pdf)
2 – Gerenciamento	(1) SNMP (v1,2 e 3) (2) Telnet e acesso local	-	SIM	Data sheet "*Cisco 1751 Modular Access Router*" (C1751_ds.pdf) (1) página 6 (2) página 6
3 – Interfaces	(1) 1 interface 10BaseT/100Base-TX, integrada ao chassis, RJ-45 (2) 2 interfaces WAN seriais, com compressão e encriptação de dados (3) 2 interfaces FXS (4) 2 interfaces FXO	-	SIM	Data sheet "*Cisco 1751 Modular Access Router*" (C1751_ds.pdf) (1) página 10 (2) página 10 (3) página 11 (4) página 11
4 – Gerais	(1) Visualização visual das portas (2) Atualização de software via rede (3) Recursos de QoS: • Commited access rate • LLFQ, WFQ • Bandwidth on demand • RSVP • WRED • Policy based routing	-	SIM	Data sheet "*Cisco 1751 Modular Access Router*" (C1751_ds.pdf) (1) página 7 (2) página 6 (3) páginas 8 e 17 (4) página 6 (5) página 6 (6) página 14 (7) páginas 6, 8, 9 e 15 (8) página 6, 8

NEC

ATRIBUTO	ATRIBUTOS OFERTADOS	ATRIBUTOS OFERTADOS ADICIONALMENTE	CONFIRMA ATENDIMENTO (SIM/NÃO)	PÁGINA DA DOCUMENTAÇÃO TÉCNICA
	• FRF.12 • cRTP (4) Roteamento entre VLANs (802.1Q) (5) Túneis VPN com IPSec, L2TP e L2F (6) Roteamento IP baseado nos protocolos RIP (v1 e v2), OSPF, BGP (7) Criptografia 3DES (8) Autenticação via RADIUS, TACACS+ e PAP/CHAP (9) Suporte a VoIP e VoFR (10) Funcionalidades de firewall • ACLs • AAA • criptografia • VPN tunnel server (11) Interfaces FXS e FXO (12) Alimentação bivolt autosense, na freq. de 60Hz			(9) página 17 (10) páginas 5, 7 e 8 (11) páginas 11 e 12 (12) página 18

NEC

4.1. SERVIDORES INTEL

4.1.1. SERVIDORES INTEL TIPO 1

ATRIBUTO	ATRIBUTOS OFERTADOS	ATRIBUTOS OFERTADOS ADICIONALMENTE	CONFIRMA ATENDIMENTO (SIM/NÃO)	PÁGINA DA DOCUMENTAÇÃO TÉCNICA
1 – CPU e Performance	Ofertado com 8 processadores e demais características conforme edital	Expansível até 16 processadores	SIM	http://www5.pc.ibm.com/us/products.nsf/$wwwPartNumLookup/86877RX
2 – Barramento	Ofertado conforme edital		SIM	http://www5.pc.ibm.com/us/products.nsf/$wwwPartNumLookup/86877RX
3 – Memória Cache	L2 – 512KB L3 – 2MB		SIM	http://www5.pc.ibm.com/us/products.nsf/$wwwPartNumLookup/86877RX
4 – Memória RAM	Ofertado com 8GB e demais características conforme edital	Expansível até 32GB	SIM	http://www5.pc.ibm.com/us/products.nsf/$wwwPartNumLookup/86877RX
5 – Controladora e Unidade de Disco Rígido – Interno	Ofertado controladora IBM ServeRaid 4Mx e 2 discos IBM 73.4GB		SIM	http://www5.pc.ibm.com/us/products/nsf/$wwwPartNumLookup/06p5736 http://www5.pc.ibm.com/us/products.nsf/$wwwPartNumLookup/06P5756
6 – Interface de VIDEO	Ofertado conforme edital	128 bits	SIM	http://www5.pc.ibm.com/us/products.nsf/$wwwPartNumLookup/

				86877RX
7 – Unidade de CD/DVD-ROM	Ofertado unidade de CD-ROM 24x		SIM	http://www5.pc.ibm.com/us/products.nsf/$wwwPartNumLookup/86877RX
8 – Controladora de I/O (por equipamento)	Ofertada 2 IBM Total Storage FastT FC2-133 HBA e 1 NIC 10/100/1000 Ethernet Onboard Adapter	2 NIC NetXtreme 10/100/1000 Ethernet Adapter totalizando as 3 unidades solicitadas pelo edital.	SIM	http://www5.pc.ibm.com/us/products.nsf/$wwwPartNumLookup/24P0960 http://www-3.ibm.com/pc/support/site.wss/document.do?lndocid=MIGR-50474
9 – Ambiente Operacional	Ofertado Windows Server 2003 E.E, SQL 2000, Concorde SystemEdge e Sun StorEdge Enterprise Backup Software v7 com as características requisitadas no edital		SIM	HCL do Windows Server 2003 http://www.microsoft.com/windows/catalog/server/default.aspx Conforme "ATRIBUTOS OFERTADOS"
10 – Fonte de Alimentação	Servidor já contempla fontes redundantes na capacidade total		SIM	http://www5.pc.ibm.com/us/products.nsf/$wwwPartNumLookup/86877RX

NEC

4.1.2. SERVIDORES INTEL TIPO 2

ATRIBUTO	ATRIBUTOS OFERTADOS	ATRIBUTOS OFERTADOS ADICIONALMENTE	CONFIRMA ATENDIMENTO (SIM/NÃO)	PÁGINA DA DOCUMENTAÇÃO TÉCNICA
1 – CPU e Perfomance	Ofertado com 4 processadores e demais características conforme edital		SIM	http://www5.pc.ibm.com/us/products.nsf/$wwwPartNumLookup/86869RX
2 – Barramento	Ofertado conforme edital		SIM	http://www5.pc.ibm.com/us/products.nsf/$wwwPartNumLookup/86869RX
3 – Memória Cache	L2 – 512KB L3 – 2MB		SIM	http://www5.pc.ibm.com/us/products.nsf/$wwwPartNumLookup/86869RX
4 – Memória RAM	Ofertado com 4GB e demais características conforme edital	Expansível até 16GB	SIM	http://www5.pc.ibm.com/us/products.nsf/$wwwPartNumLookup/86869RX
5 – Controladora e Unidade de Disco Rígido – Interno	Ofertado controladora IBM ServeRaid 4Mx e 2 discos IBM 73.4GB		SIM SIM	http://www5.pc.ibm.com/us/products/nsf/$wwwPartNumLookup/06p5736 http://www5.pc.ibm.com/us/products.nsf/$wwwPartNumLookup/06P5756
6 – Interface de VIDEO	Ofertado conforme edital	128 bits	SIM	http://www5.pc.ibm.com/us/products.nsf/$wwwPartNumLookup/86869RX

7 – Unidade de CD/DVD-ROM	Ofertado unidade de CD-ROM 24x		SIM	http://www5.pc.ibm.com/us/products.nsf/$wwwPartNumLookup/_86869RX
8 – Controladora de I/O (por equipamento)	Ofertada 2 IBM Total Storage FastT FC2-133 HBA e 3 NIC 10/100/1000 Eth. Adapter	NIC card 10/100 Eth. Adapter Onboard	SIM	http://www5.pc.ibm.com/us/products.nsf/$wwwPartNumLookup/_24P0960 http://www-3.ibm.com/pc/support/site.wss/document.do?lndocid=MIGR-50474
9 – Ambiente Operacional	Ofertado Windows Server 2003 E.E, Concorde SystemEdge e Sun StorEdge Enterprise Backup Software v7 com as características requisitadas no edital		SIM	HCL do Windows Server 2003 http://www.microsoft.com/windows/catalog/server/default.aspx Conforme "ATRIBUTOS OFERTADOS"
10 – Fonte de Alimentação	Servidor já contempla fontes redundantes	Fornecimento de uma fonte adicional contemplando a capacidade total solicitada no edital	SIM	http://www5.pc.ibm.com/us/products.nsf/$wwwPartNumLookup/_86869RX

4.1.3 SERVIDORES INTEL TIPO 3

ATRIBUTO	ATRIBUTOS OFERTADOS	ATRIBUTOS OFERTADOS ADICIONALMENTE	CONFIRMA ATENDIMENTO (SIM/NÃO)	PÁGINA DA DOCUMENTAÇÃO TÉCNICA
. CPU e Perfomance 1.1 Servidor composto por processadores Intel, com no mínimo 2 (dois) processadores INTEL XEON, com clock mínimo de 2,4 GHz; 1.2 O equipamento deverá apresentar performance mínima de 30.000 tpm-C No caso de performance estimada, a mesma deverá ser calculada com base na fórmula: tpm-C estimado = tpm-C auditado * (nº de CPU ofertadas / nº CPU auditada). 1.3 O equipamento deverá ser montado em RACK próprio do fabricante com, no mínimo, 40U de altura.	1. Ofertamos servidores IBM eServer X Series 235 cada um com com 2 (dois) processadores Intel Xeon 2,4GHz MP sem formação de cluster. 2. O servidor IBM eServer X Series 235 foi auditado no benchmark em 10/07/2003 obtendo o resultado estimado em 37.872 tpm-c com 2 processadores Intel Xeon 2,4GHz MP sem formação de cluster. Tpm-C estimado = tpmC 1 processador * (2processadores / 1processador) Tpm-C estimado = 17559 * (2/1) Tpm-C estimado = 35118 3. Todos os servidores serão instalados em racks de fabricação da IBM NetBAY42 Enterprise Rack Cabinet com altura de 42U. 4. Cada servidor terá a configuração abaixo indicada.		SIM	1. http://www-132.ibm.com/webapp/wcs/stores/servlet/ProductDisplay?productId=8599793&storeId=1&langId=-1&categoryId=2543009&dualCurrId=73&catalogId=-840 2. http://www.tpc.org/tpcc/results/tpcc_result_detail.asp?id=102081601 3. http://www-132.ibm.com/webapp/wcs/stores/servlet/ProductDisplay?lang=en_US&catalogId=-840&productId=1932473&langId=-1&prmenbr=1&cntrfnbr=1&storeId=1&cntry=840&prrfnbr=1932473 4. http://www-132.ibm.com/webapp/wcs/stores/servlet/ProductDisplay?lang=en_US&catalogId=-840&prnbr=59P4211&langId=-1&prmenbr=1&cntrfnbr=1&partNumber=59P4211&storeId=1&cntry=840
2. Barramento Barramento do sistema de, no mínimo, 533 MHz	Barramento do sistema de 533MHz Front Side Bus		SIM	http://www-132.ibm.com/webapp/wcs/stores/servlet/ProductDisplay?productId=8599793&storeId=1&langId=-1&categoryId=2543009&dualCurrId=73&catalogId=-840

NEC
3048

3. Memória Cache 512kB por processador.	512kB de memória cache L2 por processador Intel Xeon Processor MP		SIM	http://www-132.ibm.com/webapp/wcs/stores/servlet/ProductDisplay?productId=8599793&storeId=1&langId=-1&categoryId=2543009&dualCurrId=73&catalogId=-840
4. Memória RAM Memória RAM 1,5GB (um gigabyte e meio) ECC SDRAM ou tecnologia superior, instalada.	1.5 GB de memória RAM PC2100 266MHz SDRAM DIMMs	Expansivel até 12GB.	SIM	http://www-132.ibm.com/webapp/wcs/stores/servlet/ProductDisplay?productId=8599793&storeId=1&langId=-1&categoryId=2543009&dualCurrId=73&catalogId=-840
5. Controladoras e 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 defeituosos sem interrupção no funcionamento do equipamento. Serão aceitas controladoras de disco instaladas na placa de sistema.	1. 02 (dois) discos internos de 73.4GB 10000 RPM Ultra160 SCSI Hot Swap 2. 01 (uma) Controladora ServeRAID – 4MX Ultra160 SCSI.	Capacidade máx. 1314GB	SIM	http://www5.pc.ibm.com/us/products/nsf/$wwwPartNumLookup/06p5736 http://www5.pc.ibm.com/us/products.nsf/$wwwPartNumLookup/06P5756

NEC

6. Interface de VIDEO Padrão SVGA, PCI 32 Bits ou superior, com 8 Mbytes no mínimo.	01 (uma) Controladora Gráfica SVGA ATI Rage XL 8MB SDRAM PCI 32 Bits		SIM	http://www-132.ibm.com/webapp/wcs/stores/servlet/ProductDisplay?productId=8599793&storeId=1&langId=-1&categoryId=2543009&dualCurrId=73&catalogId=-840
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.	01 (uma) unidade de CD-ROM 24X e drive 3.5" 1.44MB diskette (IDE backplane for diskette and CD-ROM)		SIM	http://www-132.ibm.com/webapp/wcs/stores/servlet/ProductDisplay?productId=8599793&storeId=1&langId=-1&categoryId=2543009&dualCurrId=73&catalogId=-840
8. Controladora de I/O (por equipamento) Deverão 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.;	01 (uma) interface on board 10/100/1000 Base-T em conformidade com os padrões IEEE 802.3ab e 802.3u, com possibilidade de gerenciamento SNMP. 01 (duas) placa 10/100/1000 Base-T em conformidade com os padrões IEEE 802.3ab e 802.3u, com possibilidade de gerenciamento SNMP.		SIM	http://www-132.ibm.com/webapp/wcs/stores/servlet/ProductDisplay?productId=8599793&storeId=1&langId=-1&categoryId=2543009&dualCurrId=73&catalogId=-840 http://www-3.ibm.com/pc/support/site.wss/document.do?lndocid=MIGR-50474

ROSTI 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0070
Doc: 3696

NEC

9. Ambiente operacional Os Servidores INTEL TIPO 1 deverão 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 do Cliente; - 1 (uma) licença do agente .Concord SystemEdge., - 1 (uma) licença de software agente de backup compatível com o software gerenciador de fitoteca que permita backup LAN FREE, devidamente instalado e configurado conforme orientação da equipe técnica do Cliente; Deverá 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.	Ofertado Windows Server 2003 E.E, Concorde SystemEdge e Sun StorEdge Enterprise Backup Software v7 com as características requisitadas no edital		SIM	HCL do Windows Server 2003 http://www.microsoft.com/windows/catalog/server/default.aspx Conforme "Atributo Ofertados".

10 . Fonte de Alimentação Instalada na configuração máxima do equipamento; Recurso de troca sem interrupção (HOT-SWAPPABLE/HOT-PLUGGABLE). As fontes de alimentação deverão ser redundantes por fontesinternas 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.	02 (duas) Fontes de Alimentação hot-swap 660 watts / 220v ou 550 watts at 110v redundantes em 220v front access .		SIM	http://www-132.ibm.com/webapp/wcs/stores/servlet/ProductDisplay?productId=8599793&storeId=1&langId=-1&categoryId=2543009&dualCurrId=73&catalogId=-840

NEC

4.2. SERVIDORES RISC

4.2.1. SERVIDORES RISC TIPO 1

ATRIBUTO	ATRIBUTOS OFERTADOS	ATRIBUTOS OFERTADOS ADICIONALMENTE	CONFIRMA ATENDIMENTO (SIM/NÃO)	PÁGINA DA DOCUMENTAÇÃO TÉCNICA
1. CPU e Performance	1. Ofertamos 11 (onze) servidores Sun Fire 15K com processadores UltraSPARC III Cu de 1.05 Ghz. 2. O servidor Sun Fire 15K foi auditado no benchmark SPECjbb2000 em 09/04/2002 obtendo o resultado 433.166 ops/s com 72 processadores UltraSPARC III de 1.05 GHz. Baseado na formula descrita no item 2.1 do Anexo 1-B para atingir a performance de 260.000 SPECjbb200 estamos ofertando 44 processadores UltraSPARC III de 1.05 GHz, temos o seguinte: SPECjbb2000 estimado = 433.166 * (44/72) SPECjbb2000 estimado = 264.712,22 ops/s 3. O resultado do SPECjbb2000 apresentado acima não envolve a formação de cluster		SIM	1. lhttp://www.sun.com/processors/UltraSPARC-III/; 2. www.spec.org/jbb2000/results/res2002q2/jbb2000-20020507-00129.html 3. www.spec.org/jbb2000/results/res2002q2/jbb2000-20020507-00129.html
	1. 64 GB de memória instalada; 2. Expansibilidade a 576 GB; 3. Memória com proteção Error Correcting Code (ECC).		SIM	1. Conforme " *ATRIBUTOS OFERTADOS*" 2. Spec da 15K; (sunsolve) 3. http://www.sun.com/servers/highend/sunfire15k/details.xml – seção High Performance – Parágrafo UltraSPARC III Cu

NEC

				Processors
3. Suporte à Arquitetura	Symmetric Multiprocessing		SIM	Datasheet F15K pg. 1
4. Fonte de alimentação	1. Seis fontes de alimentação de 4 KW com entradas duais, alimentam o servidor em sua capacidade máxima e permitem sem interrupção; 2. O equipamento opera a 200-240 VAC com freqüência entre 47-63 Hz. A alimentação entre 200-220 VAC está de acordo com com o CCD de Brasília. No CCD de São Paulo, serão realizadas as adequações necessárias para compatibilizar as especificações dos equipamentos com o CCD; 3. Servidor possui fontes redundantes independentes e circuitos de alimentação redundantes que podem ser alimentados por fontes de alimentação distintas. Falha em um dos circuitos não paralisa a operação do equipamento.		SIM	1. Spec SF 15K; ou SF 15k System Overview pg 1-4, tabela 1-1, pg 1-10 seção 1.5.3; pg 3-7 seção 3.3.6; 2. SPEC SF 15K; 3. SPEC SF 15K; ou SF 15K System Overview pg 1-10 seção 1.5.3; pg 3-7 seção 3.3.6;
5. Controladoras e Disco Rígido	1. Estamos ofertando 8 arrays Sun StorEdge S1 com 2 discos rígidos (total de 16 discos) de 36.4 GB, 10.000 rpm, hot-swappables. Os arrays Sun StorEdge S1 utilizam discos com tempo médio de acesso é de 5.6 ms para leitura e 6 ms para escrita; 2. Estamos ofertando oito placas controladoras PCI dual Ultra 2 SCSI (80 MB/s)	Cada placa controladora possui duas interfaces Fast Ethernet 10/100 Base-T e suporte a IEEE 802.3u integradas. Logo, estamos ofertando 16 interfaces adicionalmente.	SIM	1. Datasheet S1 (rpm, hot-swap e tamanho), Spec do S1 + doc. sobre disco x5250A (595-5960) 2. Datasheet da x2222a ou http://www.sun.com/products/networking/dualfastethernet/specs.html

	e dual Fast Ethernet.			
	1. Estamos ofertando 8 placas controladoras duais Fibre Channel 2 GB, totalizando 16 canais; 2. Estamos ofertando 16 placas adaptadoras PCI Sun GigaSwift que operam a 10/100/1000 Base-T, atendem os padrões IEEE 802.ab e 802.u e possuem MIB's para gerenciamento SNMP; 3. As interfaces das adaptadoras Sun GigaSwift permitem o uso de conectores RJ-45 e cabeamento CAT 5 e superior, a saber, CAT 6.		SIM	1. Datasheet 6768A; 2. Doc sunsolve 41665 (fazer search para localizar MIB e 802.ab e 802.u; 3. Doc sunsolve 41665.
7. Unidade de CD/DVD-ROM e Backup	1. Cada servidor Sun Fire 15K possui duas conjuntos de placas denominadas "System Control Board" que incluem um subconjunto de periféricos que formam a "System Control Peripheral Boards." Cada Peripheral Board contém uma unidade de fita DDS-4, uma unidade de DVD-ROM e dois discos discos de 18 GB; 2. Entre outras funções, a System Control Board é um sistema que controla e configura todo o equipamento da SF15K e é capaz de compartilhar os periféricos da System Control Peripheral Boards e servir como um boot initiator (iniciador de boot) para todos os domínios da Sun Fire 15K, compartilhando a unidade de DVD-ROM e	• Cada servidor possui Peripheral Boards redundantes. Logo estamos ofertando uma unidade de DDS-4, uma unidade de DVD-ROM e dois discos rígidos de 18 GB adicionalmente aos requisitos do edital. • Unidades de fitas são padrão DDS-4; • Unidades DVD-ROM operam a velocidade 10X.	SIM	1. Sun Fire 12K/15K Systems Overview pg. 5-11 , figura 5-6 ilustra a System Control e pg. 5-12, terceiro bullet; 2. SMS 1.3 Administrator Guide pg. 2. 3. Sun Fire 12K/15K spec; 4. Sun Fire 12K/15K spec; 5. Conforme " *ATRIBUTOS OFERTADOS*"

NEC

1341

	DDS-4 (para boot por DVD-ROM/CD-ROM ou fita) pela rede entre os domínios, sem interferir na atividade de qualquer outro domínio; 3. As unidades de DVD-ROM operam a velocidade 10X; 4. As unidades de fita são padrão DDS-4; 5. Estamos ofertando um conjunto de 10 (dez) fitas, por servidor (total 110 fitas), padrão DDS-4 e 3 conjuntos de 10 (dez) fitas de limpeza para unidades de fita DDS			
8. Ambiente Operacional	1. Cada novo servidor inclui licença do sistema operacional SUN Solaris 9 para o máximo de partições possíveis no equipamento, a saber, 18 (dezoito), sem custo adicional; 2. Sistema operacional SUN Solaris de 64 bits com licença para número de ilimitado de usuários simultâneos; 3. Estamos ofertando licenças do Veritas File System, software que implementa sistema de arquivos JFS; 4. Comandos ufsdump e ufsrestore realizam o backup e restore de sistemas de arquivos completos em fitas locais ou remotas via rede; 5. Agente Concord SystemEdge ofertado; 6. O sistema operacional Solaris 9 versão SPARC foi desenvolvido e projetado para sistemas baseados em		SIM	1. Conforme " *ATRIBUTOS OFERTADOS"* 2. Conforme " *ATRIBUTOS OFERTADOS"* 3. http://www.sun.com/storage/software/storage_mgmt/filesystem/index.html 4. Capítulo 47 do manual do administrador do Solaris 9 (procurar por "You can run the ufsdump command from a single.." e Capítulo 49 do manual do administrador do Solaris 9 (procurar por "device name (local or remote)". Estes manuais estão disponíveis no docs.sun.com. 5. Conforme " *ATRIBUTOS OFERTADOS"* 6. Arquivo Solaris Operating Systems.html (grifar a frase "designed for multiprocessing and 64-bit computing using UltraSPARC...).

o software de backup LAN FREE consta no catálogo técnico anexado à nova proposta da Dataprev 32

NEC

	processadores UltraSPARC desenvolvidos pela SUN Microsystems;			
	1. Estamos ofertando 6 cópias do compilador Sun ONE Studio 7 compiler collection para linguagem C e compatível com o padrão ANSI C. Os compiladores estão licenciados para um usuário sem restrição quanto ao número de processadores do equipamento. A licença do compilador vale para um número de usuários ilimitado. 2. Estamos ofertando 11 licenças do Sun Cluster3.0 Software para os 11 (onze) servidores Sun Fire 15K. Estas licenças permitem a criação de um ou mais nós de clusters no mesmo (e.g.: partições do mesmo servidor) servidor, o que possibilita a configuração requisitada dos 20 (vinte) clusters entre partições dos 11 (onze) servidores. Adicionalmente, estamos ofertando licenças para agentes de cluster do SGBD Oracle OPS ou RACi para 10 nós do cluster.	O Sun ONE Studio 7 compiler collection também inclui compiladores para as linguagens C++ e Fortran 95	SIM	1. Comprovação compatibilidade ANSI C no datasheet do compiler e licenciamento ilimitado, conforme "*ATRIBUTOS OFERTADOS*" 2. Datasheet Sun Cluster

NEC

5. UNIDADE DE BACKUP

ATRIBUTO	ATRIBUTOS OFERTADOS	ATRIBUTOS OFERTADOS ADICIONALMENTE	CONFIRMA ATENDIMENTO (SIM/NÃO)	PÁGINA DA DOCUMENTAÇÃO TÉCNICA
1.Descrição	Estamos oferecendo dois sistemas automatizados de armazenamento Sun StorEdge L700 (OEM da StorageTek) utilizando drives LTO Ultrium 2, controle robótico de rotação, gabinete próprio e software de gerenciamento.		SIM	1. http://www.sun.com/storage/tape/l700/details.html#sysman 2. datasheet da StorEdge L700
2. Capacidade da Biblioteca	O equipamento para o CCD de Brasília está configurado com 396 slots para cartuchos LTO Ultrium 2, o que dá uma capacidade total de aproximadamente 79,2 TB de armazenamento nativo. O equipamento para o CCD de São Paulo está configurado com 228 slots para cartuchos LTO Ultrium 2, o que dá uma capacidade total de aproximadamente 45,6 TB de armazenamento nativo.	Capacidade adicional de armazenamento de aproximadamente 17,6 TB no equipamento para o CCD de Brasília e aproximadamente 4,6 TB no equipamento para o CCD de São Paulo	SIM	1. Conforme " *ATRIBUTOS OFERTADOS*"
3. Capacidade dos cartuchos	Os cartuchos no padrão LTO Ultrium 2 possuem capacidade de armazenamento de 200 Gbytes nativo conforme especificações do formato Ultrium Geração 2 elaborado pelo consorcio IBM, Hewlett-Packard e Certance		SIM	http://sunsolve.sun.com/handbook_pub/Systems/L700/spec.html
4. Compatibilidade	Os drives de leitura e gravação do padrão LTO Ultrium 2 possuem compatibilidade .		SIM	Data sobre sobre tecnologia LTO2 da StorageTek
5. Quantidade de SLOTS	A quantidade de slots do equipamento para o CCD de Brasília é de 396 slots. A quantidade de slots do equipamento para o CCD de	Oferecemos 88 slots a mais no equipamento para o CCD de Brasília e 23 slots a mais no equipamento para o CCD de SP.	SIM	Conforme " *ATRIBUTOS OFERTADOS*" CCD de Brasília, multiplicamos 60 TB por 1024 para trabalharmos com valores em

	Brasília é de 228 slots.			gigabytes: Num. Slots = (60 x 1024)/ 200 = 307.8 = 308 slots Para o CCD de SP Num. Slots = (40 x 1024)/200 = 204.8 = 205 slots
6. Quantidade de cartuchos	Oferecemos 620 cartuchos padrão LTO Ultrium 2 para o CCD de Brasília e 410 cartuchos para o CCD de SP.	Oferecemos 4 cartuchos a mais do total requisitado	SIM	Conforme " *ATRIBUTOS OFERTADOS"*
7. THROUGHPUT por drive	O drive padrão LTO Ultrium 2 (ou geração 2) opera a um throughput nominal de 30 MB/s segundo,		SIM	http://sunsolve.sun.com/handbook_pub/Systems/L700/spec.html
8. Número de drives	Oferecemos 20 drive LTO Ultrium 2 Fibre Channel para o equipamento para o CCD de Brasília e 12 drives LTO Ultrium 2 Fibre Channel para o equipamento para o CCD de São Paulo.		SIM	Conforme " *ATRIBUTOS OFERTADOS"*
9. Conectividade	Os drives LTO Ultrium 2 oferecemos possuem interfaces Fibre Channel		SIM	http://sunsolve.sun.com/handbook_pub/Systems/L700/spec.html
10. Recursos de hardware	1. As bibliotecas Sun StorEdge L700 possuem uma porta de acesso a cartuchos denominada CAP (cartdrige access port) que permite a substituição de cartuchos sem parada de operação do robot e/ou drives, ou seja, sem interromper o backup ou restore 2. A Sun StorEdge L700 possui uma porta de comunicação RJ-45 que é utilizada pelo software de gerenciamento para realizar teste de diagnósticos		SIM	1. L700 Operator's Guide pg 1-10 2. L700 Operator's Guide pg 1-12

11. Retirada de fitas	1. O software de backup e restore oferecido Sun StorEdge Enterprise Backup versão 7.0 permite e controla a retirada de cartuchos da biblioteca através das portas de accesso a cartuchos (CAPs) além da cópia de dados cartucho a cartucho denominada de tape cloning. 2. Através da porta de acesso a cartuchos é possível sacar ou inserir até 20 cartuchos por vez sem interrupção das operações de backup e restore. 3. Serão fornecidos rótulos de cartuchos compatíveis com as bibliotecas oferecidas		SIM	1. http://www.sun.com/storage/software/data_services/backup/details.html (procurar por "Support for cartridge access ports" e "tape cloning"); 2. L700 Operator's Guide pg 1-10 3. Conforme " *ATRIBUTOS OFERTADOS"*
12. Recursos necessários	1. As bibliotecas Sun StorEdge L700's possuem recursos chamados Auto Clean para realização de limpeza automática de drives que necessitem de limpeza em função da freqüência de sua utilização; 2. Estamos oferecendo 20 (cinte) cartuchos de limpeza para o CCD de BSB e 20 (vinte) cartuchos de limpeza para o CCD de SP.	Oferecemos 8 (oito) cartuchos de limpeza adicionais.	SIM	1. L700 Operator's Guide pg 1-13 na seção Auto Clean Feature; 2. Conforme " *ATRIBUTOS OFERTADOS"*
13. Recursos de software	Estamos oferecendo duas cópias (uma para CCD de Brasília e outra para o CCD de SP) do software Sun StorEdge Enterprise Backup Software versão 7 para desempenhar a função de gerenciador de fitoteca e de backup. As licenças contemplam todos os		SIM	Conforme " *ATRIBUTOS OFERTADOS"*

0080

NEC

3036

	servidores Intel tipo 1, 2 e 3 e os servidores RISC tipo 1 na modalidades de backup LAN FREE para os servidores Intel tipo 1 e RISC tipo 1 e backup via rede para os demais servidores Intel ofertados em ambas localidades. Estamos oferecendo também 10 (dez) módulos de aplicação para backup dos SGBD Oracle em servidores RISC tipo 1 e 8 (oito) módulos de aplicaçào para backup do MS Exchange Server 2000 em oito servidores Intel tipo 1			
14. Fonte de alimentação interna	1. Estamos oferecendo ambas as Sun StorEdge L700's com fontes redundantes e em quantidade máxima com a segunda torre de drives 2. As bibliotecas operam a 90-254 VAC e entre 47 a 63 Hertz adaptando-se assim a ambas localidades sem necessidade de adaptações ou ajustes elétricos. 3. Com a torre adicional, as bibliotecas possuem alimentação redundante e podem ser alimentadas por circuitos distintos e manter a operação da biblioteca em caso de falta de alimentação elétrica em um dos circuitos.		SIM	1. http://www.sun.com/storage/tape/l700/specs.html(procurar por redundant power); 2. http://www.sun.com/storage/tape/l700/specs.html 3. L700 Operator Guide pg 2-18 procure notas do "two circuit breakers".
15. Geral	Estamos oferecendo dois servidores Sun Fire V480 para o CCD de Brasília e dois servidores Sun Fire V480 para o CCD de São Paulo configurados em cluster e que atuarão com servidores de backup em ambas		SIM	Conforme " *ATRIBUTOS OFERTADOS*"

as localidades. Cada servidor está configurado para atender 150 clientes de backup. Cada servidor possui 2 processadores UltraSPARC III de 1.05 Ghz, 4 GB de memória, unidade de fita DAT, DVD-ROM, 4 (quatro) interfaces Fibre Channel, duas interfaces Gigabit Ethernet, arrays de storage, etc (vide proposta comercial)			

6 AMBIENTE DE SEGURANÇA

6.1 Servidor de Segurança Lógica Tipo 01

ATRIBUTO	ATRIBUTOS OFERTADOS	ATRIBUTOS OFERTADOS ADICIONALMENTE	CONFIRMA ATENDIMENTO (SIM/NÃO)	PÁGINA DA DOCUMENTAÇÃO TÉCNICA
1 – Descrição	(1) Os servidores de segurança lógica ofertados são firewalls operando em configuração redundante (possível através de uma porta exclusiva para failover). A solução será ofertada aos pares, ou seja, 1 par de firewalls em substituição a um módulo (conforme Anexo 1-B), totalizando 2 pares para São Paulo e 2 para Brasília. Esta configuração garante a alta disponibilidade do sistema. (1.1) Os produtos permitem que se configure uma miríade muito grande de regras de segurança, baseadas em pacotes entrantes e saintes.	-	SIM	(1) Documento 535_ds.pdf, página 2, item "Award-Winning Resiliency Provides Maximum Business Uptime". Para quantitivos, favor referir-se á planilha de quantitativos. (1.1) Documento 535_ds.pdf, página 3, terceiro bullet.
2 – Características e Funcionalidades	Além de Controle de Acesso, o produto deve prover as seguintes funcionalidades e características: (2) Autenticação; Tanto para autenticação do gerenciamento dos firewalls			(2) Documento 535_ds.pdf, página 5, item "Command level authorization" e página 4, item "Site-to-site VPN". (3) Documento 535_ds.pdf, página 4, item NAT/PAT Support e documento

ATRIBUTO	ATRIBUTOS OFERTADOS	ATRIBUTOS OFERTADOS ADICIONALMENTE	CONFIRMA ATENDIMENTO (SIM/NÃO)	PÁGINA DA DOCUMENTAÇÃO TÉCNICA
	(com 16 níveis de usuários), e também para autenticação de usuários remotos. (3) Network Address Translation (NAT 1-1 e NAT 1-n); (4) Segurança de Conteúdo (antivírus, checagem de URL e Java/ActiveX); (5) Auditoria pode ser feita através da análise dos logs de tentativas de ataques, assim como através da interação do firewall com o sistema de detecção de intrusão (através do comando "ip audit"); (6) Garantia de disponibilidade. No caso de falhas, uma segunda máquina (ou módulo) deve assumir o controle de forma não perceptível aos usuários (stateful firewall failover); (7) Gerar alertas em tempo real por meio de e-mail quando se tentar violar a política de segurança; (8) Proteção baseada no algoritmo de segurança adaptável (ASA- Adaptive Secure Algorithm), ou			pix_qa.pdf, item "What is Network Address Translation (NAT)". (4) Documento 535_ds.pdf, página 3, item "Stateful inspection Firewall", e página 4, item "Integration with leading third-party solutions". (5) Documento idsdp_rg.pdf, páginas 5 e 8. (6) Documento 535_ds.pdf, página 2, item "Award-Winning Resiliency Provides Maximum Business Uptime". (7) Documento 535_ds.pdf, página 2, item "Integrated Intrusion Protection Guards Against Popular Internet Threats". (8) Documento 535_ds.pdf, página 3, item "Stateful firewall Inspection". (9) Documento 535_ds.pdf, página 4, item "Intrusion Protection". (10) Documento 535_ds.pdf, página 1, item "Market-Leading Voice-over-IP Security Services Protect Next-Generation Converged Networks".

NEC

ATRIBUTO	ATRIBUTOS OFERTADOS	ATRIBUTOS OFERTADOS ADICIONALMENTE	CONFIRMA ATENDIMENTO (SIM/NÃO)	PÁGINA DA DOCUMENTAÇÃO TÉCNICA
	compatível, que oferece um firewall orientado à conexão com classificação; (9) Prevenção contra ataques de negação de serviço; (10) Suporte a aplicações multimídia; (11) Suporte à gerência de Listas de Acesso em Roteadores. Essa funcionalidade é possível através do software de gerenciamento de segurança-VMS, objeto de fornecimento desta proposta; (12) Configuração e gerência centralizada em cada um dos sites; (13) Capacidade de gerenciamento remoto. (14) O suporte a serviços deve ser estendido a todo e qualquer serviço que funcione sobre protocolo IP, com a possibilidade de customização. (15) A interface deve permitir a visualização da política de segurança definida, com a opção de ocultar e visualizar grupos de regras desejados, e			(12) Documento 535_ds.pdf, página 2, item "Robust Remote-Management Solutions Lower Total Cost of Ownership". (13) Documento 535_ds.pdf, página 2, item "Robust Remote-Management Solutions Lower Total Cost of Ownership". (14) Documentos 535_ds.pdf, página 3, item "Stateful inspection Firewall". (15) Documento mcpix_ds.pdf, página 3, item "Granular Administrative Privileges for Customer/Device Groups" (16) Documentos 535_ds.pdf, página 5, item "SNMP and Syslog". (17, 17.1 e 17.2) Documentos 535_ds.pdf, página 3, item "Stateful inspection Firewall", e página 4, item "Integration with leading third-party solutions". (18) Documento 535_ds.pdf, página 4, item "Intrusion protection". (19) Documento 535_ds.pdf, página 3, item "Stateful

1303

NEC

ATRIBUTO	ATRIBUTOS OFERTADOS	ATRIBUTOS OFERTADOS ADICIONALMENTE	CONFIRMA ATENDIMENTO (SIM/NÃO)	PÁGINA DA DOCUMENTAÇÃO TÉCNICA
	o diagrama da rede protegida. (16) Capacidade de gerar relatórios gerenciais, com informações sobre estatísticas de tráfego, regras mais utilizadas, entre outras informações. As informações serão disponibilizadas através dos logs do firewall. (17) A solução tem que suportar a integração com outros produtos complementares, tais como: (17.2) Sistemas de inspeção de conteúdo (http, FTP, SMTP) de terceiros; (17.2) Suporte ao protocolo H.323. (18) O produto deverá integrar-se perfeitamente com o Sistema para Detecção de Intrusão oferecido. (19) O produto tem que suportar autenticação de usuário, autenticação de sessão e autenticação de cliente, bem como interagir com os seguintes sistemas de autenticação: (19.1) RADIUS;			Inspection Firewall". Página 4, itens "Site-to-site VPN" e "AAA Support". (19.1 e 19.2) Documento 535_ds.pdf, página 4, item "AAA Support". (20) O sistema de gerenciamento será fornecido conforme solicitado.

NEC

ATRIBUTO	ATRIBUTOS OFERTADOS	ATRIBUTOS OFERTADOS ADICIONALMENTE	CONFIRMA ATENDIMENTO (SIM/NÃO)	PÁGINA DA DOCUMENTAÇÃO TÉCNICA
	(19.2) TACACS. (20) O sistema de gerenciamento do ambiente de Firewall deverá ser disponibilizado pela CONTRATADA em hardware à parte, sendo 01 (um) sistema para o CCD de Brasília-DF e 01 (um) sistema para o CCD de São Paulo-SP, podendo estar integrado em um mesmo framework de gerenciamento dos SERVIDORES PARA DETECÇÃO DE INTRUSÃO, SWITCH TIPO 06 e ROTEADOR TIPO 01.			
3 – Características de Desempenho	A configuração do produto deverá apresentar as seguintes características mínimas de desempenho: (21) Capacidade de tratar no mínimo 400.000 conexões simultâneas; (22) Possuir capacidade de processamento superior a 1.5Gbps, em texto claro.	-	SIM	(21 e 22) Documento 535_ds.pdf, página 6, item "Performance Summary"
4 – Configuração Física do Equipamento	Os firewalls propostos possuem no 6 (seis) interfaces 100BaseTX, e 2 (duas) interfaces 1000BaseSX.		SIM	Vide planilha de quantitativos

NEC

ATRIBUTO	ATRIBUTOS OFERTADOS	ATRIBUTOS OFERTADOS ADICIONALMENTE	CONFIRMA ATENDIMENTO (SIM/NÃO)	PÁGINA DA DOCUMENTAÇÃO TÉCNICA
5 – Características Adicionais	Todo o ambiente de firewalls será acompanhado de documentação de instalação e configuração. Os firewalls possuem alimentação elétrica de acordo com a localidade onde serão instalados os equipamentos, conforme subitem 2.5., freqüência de 60 (sessenta) Hertz.	-	SIM	Documento 535_ds.pdf, página 7, item "Power".

0088

NEC

6.2 Servidor de Segurança Lógica Tipo 02

ATRIBUTO	ATRIBUTOS OFERTADOS	ATRIBUTOS OFERTADOS ADICIONALMENTE	CONFIRMA ATENDIMENTO (SIM/NÃO)	PÁGINA DA DOCUMENTAÇÃO TÉCNICA
1 – Descrição	Os servidores de segurança lógica ofertados são firewalls operando em configuração redundante (possível através de uma porta exclusiva para failover). A solução será ofertada aos pares, ou seja, 2 firewalls para São Paulo e 2 para Brasília. Os produtos permitem que se configure uma miríade muito grande de regras de segurança, baseadas em pacotes entrantes e saintes.	-	SIM	Documento pix2_ds.pdf, página 1 (coluna 2) e página 2, sub-título "Award-Winning Resiliency Provides Maximum Business Uptime".
2 – Características e Funcionalidades	(1) Autenticação; Tanto para autenticação do gerenciamento dos firewalls (com 16 níveis de usuários), e também para autenticação de usuários remotos. (2) Network Address Translation (NAT 1-1 e NAT 1-n); (3) Segurança de Conteúdo (antivírus, checagem de URL e Java/ActiveX); (4) Auditoria pode ser feita através da análise dos logs de tentativas de ataques, assim como através da interação do	-	SIM	(1) Documento pix2_ds.pdf, página 5, item "Command level authorization" e página 4, item "Site-to-site VPN". (2) Documentos pix2_ds.pdf e pix_qa.pdf, ambos na página 4. (3) Documento pix2_ds.pdf, página 3, item "Stateful inspection Firewall", e página 4, item "Integration with leading third-party solutions". (4) Documento idsdp_rg.pdf, páginas 5 e 8.

ATRIBUTO	ATRIBUTOS OFERTADOS	ATRIBUTOS OFERTADOS ADICIONALMENTE	CONFIRMA ATENDIMENTO (SIM/NÃO)	PÁGINA DA DOCUMENTAÇÃO TÉCNICA
	firewall com o sistema de detecção de intrusão (através do comando "ip audit"); (5) Gerenciamento Corporativo, permitindo que vários equipamentos sejam gerenciados a partir de uma única console. Essa funcionalidade é possível através do software de gerenciamento de segurança- VMS, objeto de fornecimento desta proposta; (6) Garantia de disponibilidade. No caso de falhas, uma segunda máquina (ou módulo) deve assumir o controle de forma não perceptível aos usuários (stateful firewall failover); (7) Gerar alertas em tempo real por meio de e-mail quando se tentar violar a política de segurança; (8) Proteção baseada no algoritmo de segurança adaptável (ASA- Adaptive Secure Algorithm), ou compatível, que oferece um firewall orientado à conexão com classificação; (9) Prevenção contra ataques			(5) Documento pix2_ds.pdf, página 3. (6) Documento pix2_ds.pdf, página 2, sub-título "Award-Winning Resiliency Provides Maximum Business Uptime". (7) Documento pix2_ds.pdf, página 2, item "Integrated Intrusion Protection Guards Against Popular Internet Threats". (8) Documento pix2_ds.pdf, página 3, item "Stateful firewall Inspection". (9) Documento pix2_ds.pdf,

NEC

ATRIBUTO	ATRIBUTOS OFERTADOS	ATRIBUTOS OFERTADOS ADICIONALMENTE	CONFIRMA ATENDIMENTO (SIM/NÃO)	PÁGINA DA DOCUMENTAÇÃO TÉCNICA
	de negação de serviço; (10) Suporte a aplicações multimídia; (11) Suporte à gerência de Listas de Acesso em Roteadores. Essa funcionalidade é possível através do software de gerenciamento de segurança-VMS, objeto de fornecimento desta proposta; (12) Configuração e gerência centralizada em cada um dos sites; (13) Capacidade de gerenciamento remoto. (14) O suporte a serviços deve ser estendido a todo e qualquer serviço que funcione sobre protocolo IP, com a possibilidade de customização. (15) A interface deve permitir a visualização da política de segurança definida, com a opção de ocultar e visualizar grupos de regras desejados, e o diagrama da rede protegida. (16) Capacidade de gerar relatórios gerenciais, com informações sobre estatísticas			página 4, item "Intrusion Protection". (10) Documento pix2_ds.pdf, página 1. (12) Documento pix2_ds.pdf, página 2 e 3, item "Robust Remote-Management Solutions Lower Total Cost of Ownership". (13) Documento pix2_ds.pdf, página 2 e 3, item "Robust Remote-Management Solutions Lower Total Cost of Ownership". (14) Documento pix2_ds.pdf, página 3, item "Stateful inspection Firewall". (15) Documento mcpix_ds.pdf, página 3, item "Granular Administrative Privileges for Customer/Device Groups"

ATRIBUTO	ATRIBUTOS OFERTADOS	ATRIBUTOS OFERTADOS ADICIONALMENTE	CONFIRMA ATENDIMENTO (SIM/NÃO)	PÁGINA DA DOCUMENTAÇÃO TÉCNICA
	de tráfego, regras mais utilizadas, entre outras Informações. As informações serão disponibilizadas através dos logs do firewall. (17) A solução suporta a integração com outros produtos complementares, tais como: (17.1) Sistemas de inspeção de conteúdo (HTTP, FTP, SMTP) de terceiros; (17.2) Suporte ao protocolo H.323. (18) O produto integra-se perfeitamente com o Sistema para Detecção de Intrusão oferecido. (19) O produto tem que suportar autenticação de usuário, autenticação de sessão e autenticação de cliente, bem como interagir com os seguintes sistemas de autenticação: (19.1) RADIUS; (19.2) TACACS. (19.3) ADMINISTRAÇÃO CENTRAL			(16) Documentos pix2_ds.pdf, página 5, item "SNMP and Syslog". (17, 17.1 e 17.2) Documentos pix2_ds.pdf, página 3, item "Stateful inspection Firewall", e página 4, item "Integration with leading third-party solutions". (18) Documento pix2_ds.pdf, página 4, item "Intrusion protection". (19) Documento pix2_ds.pdf, página 3, item "Stateful Inspection Firewall". Página 4, itens "Site-to-site VPN" e ""AAA Support". (19.1 e 19.2) Documento pix2_ds.pdf, página 4, item "AAA Support".

ATRIBUTO	ATRIBUTOS OFERTADOS	ATRIBUTOS OFERTADOS ADICIONALMENTE	CONFIRMA ATENDIMENTO (SIM/NÃO)	PÁGINA DA DOCUMENTAÇÃO TÉCNICA
				(19.3) Documento pix2_ds.pdf, página 3.
2 – Características e Funcionalidades (continuação)	(20) O produto deve suportar VPN padrão IPSEC, com as seguintes características: (20.1) Algoritmos de criptografia (DES, 3DES); (20.2) Capacidade superior a 1000 conexões simultâneas; (20.3) Capacidade de processamento em 3DES superior a 50Mbps; (20.4) Suporte a certificados digitais X.509v3. (21) O sistema de gerenciamento do ambiente de Firewalls será disponibilizado pela CONTRATADA no mesmo hardware gerenciador dos SERVIDORES DE SEGURANÇA LÓGICA TIPO 01 , sendo 01 (um) sistema para o CCD de Brasília-DF e 01 (um) sistema para o CCD de São Paulo-SP.	-	SIM	(20 e 20.1) Documento pix2_ds.pdf, página 4, item "Site-to-site VPN". (20.2 e 20.3) Documento pix2_ds.pdf, página 6, item "Performance Summary". (20.4) Documento pix2_ds.pdf, página 4, item "X.509 certificate and CRL support". (21) O sistema de gerenciamento será fornecido conforme solicitado.
3 – Características de Desempenho	A configuração do produto apresenta as seguintes características mínimas de	-	SIM	Documento pix2_ds.pdf, página 6, item "Performance Summary".

ATRIBUTO	ATRIBUTOS OFERTADOS	ATRIBUTOS OFERTADOS ADICIONALMENTE	CONFIRMA ATENDIMENTO (SIM/NÃO)	PÁGINA DA DOCUMENTAÇÃO TÉCNICA
	desempenho: o Capacidade de tratar no mínimo 280.000 conexões simultâneas; o Possui capacidade de processamento superior a 330Mbps, em texto claro.			
4 – Configuração Física do Equipamento	Os equipamentos fornecidos possuem 8 (oito) interfaces 10/100BaseTX, e 02 (duas) interface 1000BaseSX.	-	SIM	Vide planilha de itens fornecidos
5 – Características Adicionais	Todo o ambiente de firewalls deverá ser acompanhado de documentação de instalação e configuração. Deverá possuir alimentação elétrica de acordo com a localidade onde serão instalados os equipamentos, conforme subitem 2.5., freqüência de 60 (sessenta) Hertz.	-	SIM	Documento pix2_ds.pdf, página e, item "Power".

NEC

6.3 Servidor para Detecção de Intrusão

ATRIBUTO	ATRIBUTOS OFERTADOS	ATRIBUTOS OFERTADOS ADICIONALMENTE	CONFIRMA ATENDIMENTO (SIM/NÃO)	PÁGINA DA DOCUMENTAÇÃO TÉCNICA
1 – Descrição	A solução ofertada é composta por 2 módulos que farão a coleta do tráfego nos switches tipo 1 (um módulo em cada switch), conforme especificado no Anexo 1-B deste edital. A detecção de intrusão será feita por dois módulos externos, um para cada localidade, conforme Anexo 1-B deste edital.	-	SIM	Vide planilha de quantitativos do switch tipo 1 e IDS's.
2 – Características e Funcionalidades	O ambiente de IDS deve ser composto por dois elementos complementares: (1) Sensor: (1.1) Responsável por monitorar a rede a que está conectado, analisando tanto o cabeçalho (header) como a área de dados (payload) de cada pacote que trafega pela rede citada, de modo a verificar se os referidos pacotes constituem tráfego autorizado. Para pacotes que estão encriptados, o IDS deve ser posicionado antes da encriptação ser feita, de modo a poder analisar os pacotes não encriptados.	-	SIM	(1) Documento idsdp_rg.pdf, página 8, item "Differing Cisco IDS Produtcs", sub-item "Cisco IDS-4210, 4235, 4250". (1.1) Documento vpids_qa.pdf, página 6, item "Q. Can the sensor detect attacks if the traffic is encrypted, for example Psecurity (IPsec) or Secure Sockets Layer (SSL)".

ATRIBUTO	ATRIBUTOS OFERTADOS	ATRIBUTOS OFERTADOS ADICIONALMENTE	CONFIRMA ATENDIMENTO (SIM/NÃO)	PÁGINA DA DOCUMENTAÇÃO TÉCNICA
	(1.2) O sensor deve ser capaz de monitorar o tráfego de redes TCP/IP, observando no mínimo uma interface de rede com 500 Mbps em tráfego full. (1.3) O sensor deve oferecer uma interface de controle 10BaseT/100BaseTX (em caso de equipamento externo ao SWITCH TIPO 1); (1.4) 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 de utilização de módulos para o SWITCH TIPO 1); (1.5) O sensor deve possuir a capacidade de monitorar diversas VLANs simultaneamente, utilizando o recurso de captura VLAN ACL ou a funcionalidade SPAN. (2) Software de controle: (2.1) Software baseado em sistema operacional HP-UX, Solaris, AIX, Windows 2000 ou			(1.2) Documento ids4f_ds.pdf, página 2, primeiro parágrafo. (1.3) Documento ids4f_ds.pdf, página 3, item "Product specifications", sub-item "Standard command and control interface". (1.4) Estamos ofertando equipamento externo ao switch. (1.5) Documento ids4f_ds.pdf, página 1. quinto bullet, e documento vpids_qa.pdf, página 3, item "How does the IDS sensor work". (2.1) Para o Sistema Operacional, vide planilha de quantitativos. Vide também documento ch01.pdf, página 5, linha 2.

NEC

ATRIBUTO	ATRIBUTOS OFERTADOS	ATRIBUTOS OFERTADOS ADICIONALMENTE	CONFIRMA ATENDIMENTO (SIM/NÃO)	PÁGINA DA DOCUMENTAÇÃO TÉCNICA
	LINUX, capaz de monitorar de forma centralizada a atividade de múltiplos sensores, estejam estes localizados em segmentos de rede locais ou remotos. (2.1.1) Deve ser possível configurar remotamente os sensores utilizando-se o software de controle. (2.1.2) Em caso de falha de um dos sensores utilizados, um alarme deve ser enviado para o software de controle. (2.1.3) O software de controle deve registrar em uma base de dados às configurações de cada um dos sensores que lhe são subordinados. (2.1.4) O software de controle deve permitir integração com base de dados Oracle versão 8.i ou superior, ou SQL Server versão 2000 ou superior. (2.2) O sistema deve analisar cada um dos pacotes que trafegam pela rede a que está conectado e também a relação de tais pacotes com os adjacentes a ele no fluxo de dados da rede. Imediatamente			(2.1.1) Documento "Cisco Intrusion Detection System Ease of Management - Cisco Systems.htm", item "Simple Configuration", terceiro bullet. (2.1.2) Documento "Cisco Intrusion Detection System Ease of Management - Cisco Systems.htm", item "Easy Alarm Processing". (2.1.3) Documento cwvpn_ov.pdf, página 4, item "Network-Based IDS Management, sexto bullet". (2.1.4) Documento ch02.pdf, página 8, Step 10. (2.2) Documento idsdp_rg.pdf, página 4, item "Monitoring the Network".

ATRIBUTO	ATRIBUTOS OFERTADOS	ATRIBUTOS OFERTADOS ADICIONALMENTE	CONFIRMA ATENDIMENTO (SIM/NÃO)	PÁGINA DA DOCUMENTAÇÃO TÉCNICA
	após a identificação de uma eventual violação da política de segurança o sensor deve enviar um alarme para o software de controle. (3) O bloqueio de uma tentativa de invasão não deve afetar os demais usuários.			(3) As medidas de bloqueio podem ser aplicadas através de "ip audit parameters", vide documento idsdp_rg.pdf, página 4, item 1.
2 – Características e Funcionalidades (continuação)	(4) O sistema deve permitir a detecção das seguintes classes de ataques: (4.1) Ataques com nomes específicos: tais como PHF e Smurf; (4.2) Ataques genéricos: (ataques nomeados com múltiplas variações) tais como Pacotes IP fragmentados e Teardrop; (4.3) Ataques que utilizam recursos de detecção Whisker anti-IDS; (4.4) Ataques com assinaturas complexas: tais como Simplex-Mode TCP hijacking e E-mail Spam; (4.5) Ataques a servidores Web, a servidores de E-mail, .Denial of Service., .FTP			(4.1) Documento intro.pdf, página 8, sexto bullet. (4.2) A lista de assinaturas é encontrada no documento idssl_ds.pdf. (4.3) Documento "Cisco IDS Sensor Software Version 4_0 - Cisco Systems.htm", item "Multiple Detection Methods". (4.4) A lista de assinaturas é encontrada no documento idssl_ds.pdf. (4.5) A lista de assinaturas é encontrada no documento

ATRIBUTO	ATRIBUTOS OFERTADOS	ATRIBUTOS OFERTADOS ADICIONALMENTE	CONFIRMA ATENDIMENTO (SIM/NÃO)	PÁGINA DA DOCUMENTAÇÃO TÉCNICA
	exploits., acesso não autorizado, a servidores de banco de dados, a servidores de aplicação e serviço (NT, Solaris, HP-UX, AIX, Linux), a servidores DNS e Probin Attacks. (5) O sistema deve ainda 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 aos mesmos de modo a prevenir tentativas de reincidência. (6) O software de controle deve ser capaz de enviar alarmes via e-mail para notificar a violação de uma dada regra de segurança. (7) O sistema deve registrar informações tais como origem, destino, horário e tipo dos ataques ocorridos. (8) O sistema deve possibilitar a atualização automática das .assinaturas. através de			idssl_ds.pdf. (5) Documento Irlot_ds.pdf, página 1, item "Signature Instruction Language for Verifying Exploits and Reconnaissance (SILVER)". (6) Documento ids4f_ds.pdf, página 6, item "E-mail Alerts". (7) Item atendido através dos logs. (8) Documento swchap5.pdf,l página 5, Step 3 (através de https). (9) Documento Irlot_ds.pdf, página 2, item "Secure Administration".

NEC

ATRIBUTO	ATRIBUTOS OFERTADOS	ATRIBUTOS OFERTADOS ADICIONALMENTE	CONFIRMA ATENDIMENTO (SIM/NÃO)	PÁGINA DA DOCUMENTAÇÃO TÉCNICA
	download seguro via Web. (9) O Sistema deve possuir suporte a SSH para comunicação e configuração segura. (10) O sistema deve realizar a verificação do TCP Three Way Handshake.			(10) Documento ch07.pdf, página 5, Step 11.
2 – Características e Funcionalidades (continuação)	Além disso, o sistema deve: (11) Oferecer respostas em tempo real para os ataques via rede, com possibilidade de término da sessão e reconfiguração de regras de acesso em firewall, que seja possível configurar; (11.1) Suportar captura de log de sessão no formato padrão TCP Dump; (11.2) Bloquear tentativas de invasão, que seja possível configurar; (11.3) Permitir verificação de decodificação de protocolos, scripts CGI, DNS, acesso remoto via BIND, daemons; (11.4) Permitir customização de respostas a intrusões, mascaramento de tráfego,			(11) Documento idsdp_pdf, página 1, terceiro bullet e página 4, item "Monitoring the Network", quarto bullet. (11.1) Documento vpids_qa.pdf, página 6, item "Is it possible to record and replay the IP session of the source IP address that triggered an IDS alarm". (11.2) Documento ccmigration_09186a008015e3ab.pdf, capítulo 3, página 3-26, item "Configuring Block Devices", primeiro parágrafo. (11.3) A lista de assinaturas é encontrada no documento idssl_ds.pdf.

ATRIBUTO	ATRIBUTOS OFERTADOS	ATRIBUTOS OFERTADOS ADICIONALMENTE	CONFIRMA ATENDIMENTO (SIM/NÃO)	PÁGINA DA DOCUMENTAÇÃO TÉCNICA
	criação de conexões e modificação de ações de resposta; (11.5) Possuir ferramentas de configuração com interface gráfica, controlando múltiplos sistemas de detecção; (11.6) Registrar as sessões de ataques, com possibilidade de playback.; (11.7) Utilizar base de dados em tempo real para ajuda a resposta a incidentes ocorridos; (11.8) Gerar sumários de relatórios das atividades registradas; (11.9) Utilizar recurso de e-mail e traps SNMP para envio de informações a consoles com plataforma de gerenciamento; (11.10) Detectar eventos em ambientes computacionais com os sistemas operacionais Windows NT 4.0 (Server e Workstation) e Unix (AIX, Solaris, Linux, HP-UX); (11.11) Fornecer suporte ao gerenciamento de riscos através de relatórios técnicos			(11.4) Documento Irlot_ds.pdf, página 2, item "Shunning with the Cisco PIX Firewall and Cisco Catalyst Switches". (11.5) Documento vpids_qa.pdf, página 9, Table 1, linhas 2 e 3. (11.6) Possível via análise de logs. (11.7) Documento ccmigration_09186a008015e3ab.pdf, capítulo 6, página 6-31, quinto e sexto bullets. (11.8) Documento Irlot_ds.pdf, página 2, item "Alarm Summarization". (11.9) Documento ids4f_ds.pdf, página 6, item "E-mail Alerts". (11.10) A lista de assinaturas é encontrada no documento idssl_ds.pdf. (11.11) Documento ccmigration_09186a008015e3ab.pdf, capítulo 6, página 6-1.

NEC

ATRIBUTO	ATRIBUTOS OFERTADOS	ATRIBUTOS OFERTADOS ADICIONALMENTE	CONFIRMA ATENDIMENTO (SIM/NÃO)	PÁGINA DA DOCUMENTAÇÃO TÉCNICA
	e gerenciais pré-definidos, com detalhamento das informações coletadas; (11.12) Permitir a criação de relatórios técnicos e gerenciais personalizados, em formas textuais e gráficas; (11.13) Possuir documentação detalhada para possibilitar a configuração; (11.14) Ser robusto para suportar qualquer tipo de ataque contra si próprio; (11.15) Permitir instalação sem necessidade de alteração na infra-estrutura de rede e sem causar degradação do seu desempenho; (11.16) Permitir configuração remota, a partir da console de gerenciamento.			(11.12) Documento ccmigration_09186a008015e3ab.pdf, capítulo 6, página 6-1. (11.13) Será fornecida a documentação pertinente após assinatura do contrato. (11.14) Documento "Cisco IDS Sensor Software Version 4_0 - Cisco Systems.htm", item "Multiple Detection Methods". (11.15) Os equipamentos ofertados serão instalados respeitando o projeto lógico, de modo a garantir a transparência e desempenho de todo o sistema. (11.16) Documento ids4f_ds.pdf, página 5, item "SSH for remote administration"
3 – Características Adicionais	(12) 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	-	SIM	(12) A Nec do Brasil está ofertando o ambiente de gerenciamento conforme solicitado, para maiores detalhes vide planilha de quantitativos.

ATRIBUTO	ATRIBUTOS OFERTADOS	ATRIBUTOS OFERTADOS ADICIONALMENTE	CONFIRMA ATENDIMENTO (SIM/NÃO)	PÁGINA DA DOCUMENTAÇÃO TÉCNICA
	SEGURANÇA LÓGICA, SWITCH TIPO 5 e ROTEADOR TIPO 1; (13) Todo o ambiente de deverá ser acompanhado de documentação de instalação e configuração; (14)O produto deverá integrar-se, de forma transparente, com o ambiente de gerência dos SERVIDORES DE SEGURANÇA LÓGICA, sendo capaz de reconfigurar automaticamente as regras desses equipamentos.			(13) O ambiente será fornecido com a devida documentação. (14) Todos os itens referente a segurança são de mesmo fabricante, e serão gerenciados pela mesma ferramenta de gerência (VMS). Vide planilha de quantitativos.

7- RACK PARA EQUIPAMENTOS

ATRIBUTO	ATRIBUTOS OFERTADOS	ATRIBUTOS OFERTADOS ADICIONALMENTE	CONFIRMA ATENDIMENTO (SIM/NÃO)	PÁGINA DA DOCUMENTAÇÃO TÉCNICA
1 – Estrutura Física	Rack de 19" para acomodar servidores Intel e equipamentos de conectividade.		SIM	http://www5.pc.ibm.com/us/products.nsf/$wwwPartNumLookup/930842s http://www-132.ibm.com/webapp/wcs/stores/servlet/ProductDisplay?lang=en_US&catalogId=-840&prnbr=32P1031&langId=-1&prmenbr=1&cntrfnbr=1&partNumber=32P1031&storeId=1&cntry=840 http://www-132.ibm.com/webapp/wcs/stores/servlet/ProductDisplay?lang=en_US&catalogId=-840&prnbr=09N4291&langId=-1&prmenbr=1&cntrfnbr=1&partNumber=09N4291&storeId=1&cntry=840 http://www-132.ibm.com/webapp/wcs/stores/servlet/ProductDisplay?lang=en_US&catalogId=-840&prnbr=94G7447&langId=-1&prmenbr=1&cntrfnbr=1&partNumber=94G7447&storeId=1&cntry=840 http://www-132.ibm.com/webapp/wcs/stores/servlet/ProductDisplay?lang=en_US&catalogId=-840&prnbr=94G6670&langId=-1&prmenbr=1&cntrfnbr=1&partNumber=94G6670&storeId=1&cntry=840

2 – Estrutura Funcional	Ofertado conforme edital		SIM	http://www5.pc.ibm.com/us/products.nsf/$wwwPartNumLookup/_37I6866 http://www-132.ibm.com/webapp/wcs/stores/servlet/ProductDisplay?lang=en_US&catalogId=-840&prnbr=94G7448&langId=-1&prmenbr=1&cntrfnbr=1&partNumber=94G7448&storeId=1&cntry=840
3 – Gerais	Ofertado conforme edital		SIM	Conforme "*Atributos Ofertados*"

NEC

13010
E

Comprovação das Especificações Exigidas no Edital 050/2003

2. Aspectos gerais

23/07/03

0106

TPC Transaction Processing Performance Council

The TPC defines transaction processing and database benchmarks and delivers trusted results to the industry.

- Home
- Results
- Benchmarks
  - TPC-C
  - **- Results**
  - - Description
  - - FAQ
  - TPC-H
  - TPC-R
  - TPC-W
  - Obsolete
  - - TPC-A
  - - TPC-B
  - - TPC-D
- Technical Articles
- Related Links
- What's New
- About the TPC
- Who We Are
- Member Login

TPC-C Result Highlights

IBM eServer xSeries 440 c/s 8p

Benchmark Stats

Result ID:	103040401
Result Status:	In Review
TPC-C Rev:	5.1
Report Date:	04/04/03

System Information

Total System Cost	781,556 US $
TPC-C Throughput	119,115
Price/Performance	6.56 US $
Availability Date	10/04/03
Database Manager	Microsoft SQL Server 2000 Enterprise Ed. SP3
Operating System	Microsoft Windows Server 2003 Datacenter Edition
Transaction Monitor	Microsoft COM+

Server Information

CPU:	Intel Xeon MP 2.0 GHz
# of CPUs:	8
Cluster:	N

Client Information

# of clients:	4
CPU:	Intel Xeon DP 2.4GHz
CPUs per client:	8

- Executive Summary (148 KB)
- Full Disclosure Report (2513 KB)

top

Home Results Benchmarks Technical Articles Related Links What's New
About the TPC Who We Are Privacy Policy About Pricing

0107

TPC Transaction Processing Performance Council

The TPC defines transaction processing and database benchmarks and delivers trusted results to the industry.

13008 E

- Home
- Results
- Benchmarks
  - TPC-C
  - **Results**
  - Description
  - FAQ
  - TPC-H
  - TPC-R
  - TPC-W
  - Obsolete
  - TPC-A
  - TPC-B
  - TPC-D
- Technical Articles
- Related Links
- What's New
- About the TPC
- Who We Are
- Member Login

TPC-C Result Highlights

IBM **IBM eServer xSeries 360/2.0GHz/4p**

Benchmark Stats

Result ID:	103022802
Result Status:	In Review
TPC-C Rev:	5.1
Report Date:	02/28/03

System Information

Total System Cost	226,504 US $
TPC-C Throughput	52,587
Price/Performance	4.31 US $
Availability Date	04/30/03
Database Manager	Microsoft SQL Server 2000 Enterprise Ed. SP3
Operating System	Microsoft Windows Server 2003 Enterprise Server
Transaction Monitor	Microsoft COM+

Server Information

CPU:	Intel Xeon MP 2.0 GHz
# of CPUs:	4
Cluster:	N

Client Information

# of clients:	2
CPU:	Intel Xeon DP 2.4GHz
CPUs per client:	1

- Executive Summary (216 KB)
- Full Disclosure Report (1433 KB)

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0108
Doc: 3696

top

Home Results Benchmarks Technical Articles Related Links What's New
About the TPC Who We Are Privacy Policy About Pricing

0108

TPC Transaction Processing Performance Council

The TPC defines transaction processing and database benchmarks and delivers trusted results to the industry.

- Home
- Results
- Benchmarks
  - TPC-C
    - **Results**
    - Description
    - FAQ
  - TPC-H
  - TPC-R
  - TPC-W
  - Obsolete
    - TPC-A
    - TPC-B
    - TPC-D
- Technical Articles
- Related Links
- What's New
- About the TPC
- Who We Are
- Member Login

TPC-C Result Highlights

IBM eServer xSeries 235/2.4GHz/1P

Benchmark Stats

Result ID:	102081601
Result Status:	In Review
TPC-C Rev:	5.0
Report Date:	08/16/02

System Information

Total System Cost	52,526 US $
TPC-C Throughput	17,559
Price/Performance	2.99 US $
Availability Date	08/16/02
Database Manager	Microsoft SQL Server 2000 Standard Ed. SP3
Operating System	Microsoft Windows 2000 Server SP2
Transaction Monitor	Microsoft COM+

Server Information

CPU:	Intel Xeon 2.4 GHz
# of CPUs:	1
Cluster:	N

Client Information

# of clients:	1
CPU:	Intel Pentium III 1.4GHz
CPUs per client:	1

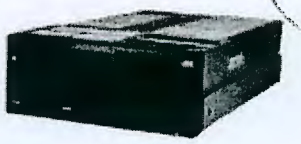
- Executive Summary (208 KB)
- Full Disclosure Report (1291 KB)

xSeries 440

Servers
Intel-based servers
Rack-optimized
Universal
Appliance
Storage
Accessories & upgrades
Services
Support
Certification
Education and training
News and awards
Library
HW/SW compatibility

$40,299.00 IBM List Price
Model Name: **86877RX**
Part Number: **86877RX**

Accessories & Upgrades



13006 E

IIII

Technical Details

Architecture

Form factor:	Rack
Orientations allowed:	Horizontal
Bus type/architecture:	
Slots x bays total (free):	6(6) x 4(2)
Expansion bus type:	PCI

Multimedia

Media device type:	CD-ROM
Media speed:	24X Max
Media interface type:	EIDE
Media data transfer rate:	2500KBps
Media average access time:	110ms
Media transport type:	Front tray loading
Recordable:	No
Removable:	Yes
Audio features:	
Multimedia features:	

Expansion Options

Slots total (free) and type:	2(2) 64 Bit Active PCI-X 100 MHz Hot Swap, 2 (2) 64 Bit Active PCI-X 133 MHz Hot Swap, 2(2 64 Bit Active PCI-X 66 MHz Hot Swap
3.5" bays	1(0) SL, 2(2) SL
- accessible (free) and height:	
- not accessible (free) and height:	
5.25" bays	1(0) SL
- accessible (free) and height:	
- not accessible (free) and height:	
Plug and play support:	Yes
Parallel ports (type):	
Serial ports (type):	1 (RS485), 3 (USB)
Expansion ports:	Keyboard, Mouse, RJ-45

Graphics Subsystems

Graphics Chip Set Model & Mfr.:	S3 Savage4 LT
Graphics Data Width:	128-bit
Graphics Type:	--
Default Memory Address:	
Video RAM Std (MB):	8MB
Video RAM Max (MB):	8MB
Video RAM Type:	SDRAM
Graphics Bus Interface:	PCI
Resolution Max (Video RAM Std), NI:	1024x768
Resolution Max (Video RAM Max), NI:	1600x1200
Colors Max (Video RAM Std):	16777216
Colors Max (Video RAM Max):	65536
Graphics features:	DDC-2B compliant

Hard Disk

Hard Disk 1:

Number of installed hard disks:	
Hard disk size[1]:	--
Hard disk controller:	Adaptec 7899 Integrated Dual Channel Ultra160 SCSI
Hard disk type:	Open bay
Total possible device types:	
Max internal hard disk capacity:	146.8GB
Average seek time:	--
Average latency:	--
RAID levels supported:	
Hot swappable drive bays:	2
Cache size:	--
Number of platters:	
Platter RPM:	
Burst transfer rate:	
Sustained data trans rate (low; high):	--
Additional storage features:	
Optional hard disk available:	

Memory

Memory (RAM) std/max:	2GB / 32768MB
RAM speed:	133MHz
Optional RAM configuration:	512:1024 DIMMs
RAM type:	PC133 SDRAM
RAM slots total (available):	16 DIMM (12 DIMM)

Networking

Network interface:	Gigabit Ethernet- Integrated
Network speed:	10Mbps, 100Mbps, 1000Mbps
Network features:	RJ-45 connector (for 10Base-T/100Base-TX), 10Base-T/100Base-TX port

Power Management

Power supply:	1050Watts
Power supply type:	110-220 volt Hot Swap Redundant 2 Std.
Power supply additional:	
Heat emissions:	361W
Sound emissions:	62dB
Cooling system:	4 fans
UPS:	Yes
Power management features4:	

System Management

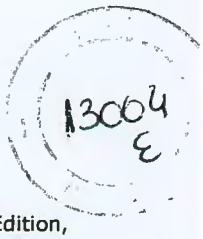
Adapter:	Remote Supervisor Adapter
Software:	Power-on password Privileged access password Selectable boot Unattended start-up
Features:	Ethernet and Fast Ethernet Compatible Networks; Network Speed of 100Mbps/10Mbps PCI Interface Bus; RJ11 Connectors; RJ45 Connectors; RS 232 Connectors; RS 485 Connectors; RS-232 Connectors; 32-bit Data/Address Width

Processor

Processor (CPU)2:	Intel Xeon MP
Processor internal clock speed2:	2.00GHz
Front Side Bus:	400MHz
Processor manufacturer:	Intel
Math co-processor:	
L1 internal CPU cache:	--
L2 internal CPU cache:	512KB
L2 external CPU cache std:	--
L2 external CPU cache type:	
Upgradable processor:	
Processor upgrade options:	
Processor upgrade method:	Add processor option
BIOS type:	Flash
Number of processors std/max:	4/8
SMP capable (multiple processors):	Yes
Multi-processor bus (slots/speed):	--
L3 cache:	2MB

Security

AssetCare features:	IBM Director Remote I/O ServerGuide
Security features:	Power-on password Privileged access password Selectable boot Unattended start-up
VPD support:	



Software

Tested operating systems:	Microsoft Windows NT 4.0 Enterprise Edition, Microsoft Windows 2000 Advanced Server, Microsoft Windows 2000 Server, Novell Netwar 6.0, Red Hat Linux Advanced Server 2.1, SuSE 8.0, VMware ESX Server v1.5
Operating system provided:	
Communication/networking applications:	
Device drivers/utilities:	
Multimedia applications:	
Productivity applications:	
Other applications provided:	

Standard Features

Pointing device type:	
Standard diskette size:	3.5" 1.44MB
Keyboard type standard:	
I20 Compliant:	
Product approvals/certifications4:	VCCI Class A (Japan); TUV-GS; UL-1950; CE MARK; CISPR-22 Class A; CSA C22.2 No. 950; FCC Class A - Part 15; ICES-003 Class A (Canada); IEC-60950 Certificate/Report; IEC-950; NOM 019; BSMI (Taiwan); C-Tick Mark (AS/NZS 3548 Class A)

Warranty

Limited Warranty period and type:	One year parts and labor IBM On-Site Repair (IOR)

Weight & Dimentions

Weight:	110lbs
Travel weight:	--
Height:	7in
Height with stand:	--
Width:	19in
Width with stand:	--
Depth:	27.5in
Operating Temperature (C) (low; high):	10; 35
Relative Humidity (%) (low; high):	8; 80

Other

Recommendation:	

Important Legal Information

xSeries 360

Servers
Intel-based servers
Rack-optimized
Universal
Appliance
Storage
Accessories & upgrades
Services
Support
Certification
Education and training
News and awards
Library
HW/SW compatibility

$15,679.00 IBM List Price
Model Name: **86869RX**
Part Number: **86869RX**

[redacted]

Accessories & Upgrades

IIII

Technical Details

Architecture

Form factor:	Rack
Orientations allowed:	Horizontal
Bus type/architecture:	PCI
Slots x bays total (free):	6(6) x 5(3)
Expansion bus type:	

Multimedia

Media device type:	CD-ROM
Media speed:	24X Max
Media interface type:	EIDE
Media data transfer rate:	2500KBps
Media average access time:	110ms
Media transport type:	Front tray loading
Recordable:	No
Removable:	Yes
Audio features:	
Multimedia features:	

Expansion Options

Slots total (free) and type:	2(2) 64 Bit PCI-X 100MHz up to 133MHz, 4(4) 64-Bit PCI-X 66MHz
3.5" bays	3(3) SL, 1(0) SL
- accessible (free) and height:	
- not accessible (free) and height:	
5.25" bays	1(0) SL
- accessible (free) and height:	
- not accessible (free) and height:	
Plug and play support:	
Parallel ports (type):	
Serial ports (type):	1 (RS485), 3 (USB)
Expansion ports:	Video, Keyboard, Mouse, RJ-45

Graphics Subsystems

Graphics Chip Set Model & Mfr.:	S3 Savage4 LT
Graphics Data Width:	128-bit
Graphics Type:	--
Default Memory Address:	
Video RAM Std (MB):	8MB
Video RAM Max (MB):	8MB
Video RAM Type:	SDRAM
Graphics Bus Interface:	PCI
Resolution Max (Video RAM Std), NI:	1024x768
Resolution Max (Video RAM Max), NI:	1600x1200
Colors Max (Video RAM Std):	16777216
Colors Max (Video RAM Max):	65536
Graphics features:	DDC-2B compliant

Hard Disk
Hard Disk 1:

Number of installed hard disks:	
Hard disk size[1]:	--
Hard disk controller:	Integrated Ultra160 SCSI
Hard disk type:	Open bay
Total possible device types:	
Max internal hard disk capacity:	220.2GB
Average seek time:	--
Average latency:	--
RAID levels supported:	
Hot swappable drive bays:	3
Cache size:	--
Number of platters:	
Platter RPM:	
Burst transfer rate:	
Sustained data trans rate (low; high):	--
Additional storage features:	
Optional hard disk available:	

Memory

Memory (RAM) std/max:	2GB / 16GB
RAM speed:	100MHz
Optional RAM configuration:	
RAM type:	PC1600 DDR SDRAM
RAM slots total (available):	8 DIMM (4 DIMM)

Networking

Network interface:	Ethernet-Integrated
Network speed:	100Mbps, 10Mbps
Network features:	

Power Management

Power supply:	370Watts
Power supply type:	110-220 volt Hot Swap Redundant Auto Restar 2 Std.
Power supply additional:	
Heat emissions:	361W
Sound emissions:	63dB
Cooling system:	6 fans
UPS:	
Power management features4:	

System Management

Adapter:	Remote Supervisor Adapter
Software:	Power-on password Privileged access password Selectable boot Unattended start-up
Features:	32-bit Data/Address Width; Ethernet and Fast Ethernet Compatible Networks; Network Speec of 100Mbps/10Mbps; PCI Interface Bus; RJ11 Connectors; RJ45 Connectors; RS 232 Connectors; RS 485 Connectors; RS-232 Connectors

Processor

Processor (CPU)2:	Intel Xeon MP
Processor internal clock speed2:	2.00GHz
Front Side Bus:	400MHz
Processor manufacturer:	Intel
Math co-processor:	
L1 internal CPU cache:	--
L2 internal CPU cache:	512KB
L2 external CPU cache std:	--
L2 external CPU cache type:	
Upgradable processor:	
Processor upgrade options:	
Processor upgrade method:	Add processor option
BIOS type:	Flash BIOS
Number of processors std/max:	2/4
SMP capable (multiple processors):	Yes
Multi-processor bus (slots/speed):	--
L3 cache:	2MB

Security

AssetCare features:	IBM Director System Management Features an Tools

Security features:	Power-on password Privileged access password Selectable boot Unattended start-up
VPD support:	

Software

Tested operating systems:	Caldera Open UNIX 8.0.0, Caldera OpenLinux Server 3.1.1, Microsoft Windows NT 4.0 Server Microsoft Windows 2000 Advanced Server, Microsoft Windows 2000 Server, Novell Netwar 6.0, Novell NetWare 5.1, Open Server 5.0.6a, Red Hat Linux 7.3, SuSE 7.2, VMware ESX Server v1.5
Operating system provided:	
Communication/networking applications:	
Device drivers/utilities:	
Multimedia applications:	
Productivity applications:	
Other applications provided:	

Standard Features

Pointing device type:	
Standard diskette size:	3.5" 1.44/1.2/0.72MB
Keyboard type standard:	
I20 Compliant:	
Product approvals/certifications4:	NOM 019; TUV-GS; UL-1950; BSMI (Taiwan); C-Tick Mark (AS/NZS 3548 Class A); CE Mark (EN55022 Class A, EN60950, and EN50082-1); CISPR-22 Class A; CSA C22.2 No. 950; FCC Class A - Part 15; ICES-003 Class A (Canada); IEC-60950 Certificate/Report; IEC-950; Japan VCCI, Class A

Warranty

Limited Warranty period and type:	Three year parts and labor Onsite

Weight & Dimentions

Weight:	70lbs
Travel weight:	--
Height:	5.25in
Height with stand:	--
Width:	17.4in
Width with stand:	--
Depth:	27.6in
Operating Temperature (C) (low; high):	10; 35
Relative Humidity (%) (low; high):	8; 80

Other

Recommendation:	

Important Legal Information

Doc 5

Select a country
← Servers
Intel processor-based servers
Rack-optimized
Universal
Blade servers
Storage
Systems Management
Accessories&upgrades
Services
Support
Certification
Education and training
News and awards
Literature
HW/SW Compatibility
Solutions

Shopping help
Warranty info
View cart
Open saved carts
Estimate shipping
Estimate leasing
Order status
Returns policy
Shopping guarantee

Related links:
Home / home office
Small Business
Medium Business

IBM Director 4.1

Intelligent systems management, rock-solid reliability

Overview

IBM Director v4.1 is the newest release of the industry leading client/server workgroup manager. IBM Director's tools provide customers with flexible capabilities to realize maximum system availability and lower IT costs. With IBM Director, IT administrators can view and track the hardware configuration of remote systems in detail and monitor the usage and performance of critical components, such as processors, disks, and memory.

In addition to making available a new version of IBM Director, enhanced extensions to IBM Director will also be available for IBM customers who want advanced capabilities. IBM Director Server Plus Pack consists of five additional tools for advanced server managements to help optimize performance and maximize availability. These tools are tightly integrated with IBM Director for consistent management from a single console.

Take a tour of IBM Director 4.1
Requires Flash player

Purcl
→ Cur use Dire

Additi docun
Inst Con
Sys Gui
→ Dire
→ SNI Dire

Features at a glance

- Self-managing, smart tools -- automated, proactive capabilities that reduce IT costs and maximize uptime.
- Support for non-IBM hardware -- Innovative use of industry standards from CIM to SNMP enables heterogeneous hardware management, protecting your existing IT investment.
- Seamless Integration -- IBM Director protects your investments in other management packages by integrating with and complementing these with more extensive hardware manageability.
- Single-click management GUI -- a convenient user interface delivers the ability to drag and drop tasks to specific systems or groups of systems.
- Integrated, centralized SQL database -- an internal database makes system-related data available, even when the specific system is not directly available.
- Multiple operating system support -- IBM Director smoothly handles a variety of popular operating systems

What's new

IBM Director 4.1 will provide significantly richer and broader systems management capabilities for superior hardware management. Key enhancements in IBM Director 4.1 include:

- Software Distribution Premium Edition is a new optional add-on to IBM Director that enables you to create and distribute software packages to the systems on your network, saving travel and labor costs.
- Command Line Interface support for many IBM Director management tasks
- An easy, single point of deployment and management of new blade servers
- Configuration wizards that streamline implementation and reduce complexity, saving valuable IT time and resources
- Linux support for IBM Director's console and management server, facilitating the use of IBM Director in pure Linux environments
- A new tool called Update Assistant that makes the management and distribution of system updates a breeze
- IBM Director Server Plus Pack, new and enhanced extensions to IBM Director for advanced server management to help optimize performance and maximize availability

availability

IBM Director Agent

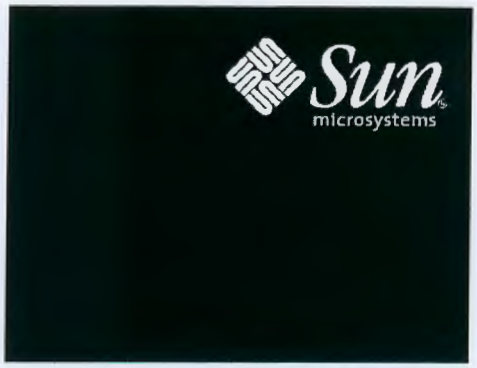
The client-side component of IBM Director is included at no additional charge with the purchase of an IBM system and can be used for added flexibility and ubiquitous remote management.
→ IBM Director Agent

Upward integration

IBM Director's upward integration will complement your existing investments in management packages like Tivoli, HP OpenView, Microsoft SMS and CA Unicenter.
→ IBM Director's upward integration

On the Web | www.sun.com/srs/netconnect

Sun℠ Remote Services Net Connect



A pre-emptive approach to system management

Sun℠ Remote Services (SRS) Net Connect is a collection of system management services designed to help you better control your IT environment. These Web-delivered services give you the ability to self-monitor systems, create performance and trend reports, and receive automatic notification so you can act more quickly when a system event occurs and manage potential issues before they become problems.

Self-monitoring:

> Monitor current system status and view detailed event history on key metrics (see back) promoting better decision making and overall system efficiency

> View system performance and event alerts to isolate problems quickly and decrease Mean Time to System Restoration (MTTR)

> Define and monitor your Sun network storage environment to determine storage needs and increase preparedness

> Review a status summary for new and uncleared alarms, by specific component, for effective problem solving

Availability, Trend, Configuration, Patch Reporting:

> Record system events and performs comparative and change analysis to determine patch status, identify issues and proactively avert future problems

> Collect event data for analysis or root cause, tracking baseline status, improving MTTR and determining gross availability

> Detect recurring system events (trends) that may affect system performance, helping you to forecast future system needs

> Report over-threshold system summary, enabling you to better allocate system resources and achieve high system performance

Event Detection and Notification:

> Notify event alerts through a Web portal for quick and easy discovery

> Deliver event alerts via e-mail, pager or both for immediate response

> Notification of alarms can be turned on or off per monitored variable for customization

Sun Reliability, Availability and Serviceability (RAS) System Analysis (for fee service):

> Provide a detailed analysis of configuration and patch data, and make recommendations for remediation

> Improve change management process through detailed reports prioritized by criticality

> Optimize system health and performance

> Help prevent system issues and downtime

SRS Net Connect helps you:

Improve IT management

Optimize system performance

Detect and resolve problems faster

Access real-time IT operations information

Realize greater value from your IT investments

Facilitate services on Sun systems to lower MTTR

Updated Features:

Hardware Failure monitoring and notification

Heartbeat detection/notification

Availability Reporting

Optional Frame Relay connection

Access control allows setup of multiorganizational user groups

SRS Net Connect 3.0 minimum requirements:

30MB of available disk space

5.8MB average RAM consumption

Sun SPARC® architecture-based system running Solaris™ 2.6 Operation Environment up to and including the Solaris™ 9 Operating Environment

Netscape™ 4.79 or higher for Solaris Operating Environment

Netscape 4.79 or higher or Internet Explorer 5.01 or higher for Intel architecture

SRS Net Connect provides secure, consistent, self-managed services that are easy to install and use. The services utilize a secure Internet-based infrastructure to collect and deliver data to SRS Net Connect's password-protected portal, and require no hardware or firewall changes.

Application Features:

> Internet-Based (Frame relay connection available for fee)

> View SRS Net Connect results on a single common interface through a secure Web portal

> Auto-upgrade — easily and automatically update the SRS Net Connect environment (at your convenience)

> Robust access control and system grouping for user administration

> "Invite" function allows for multiorganizational user groups

> Self-installable and easy to use

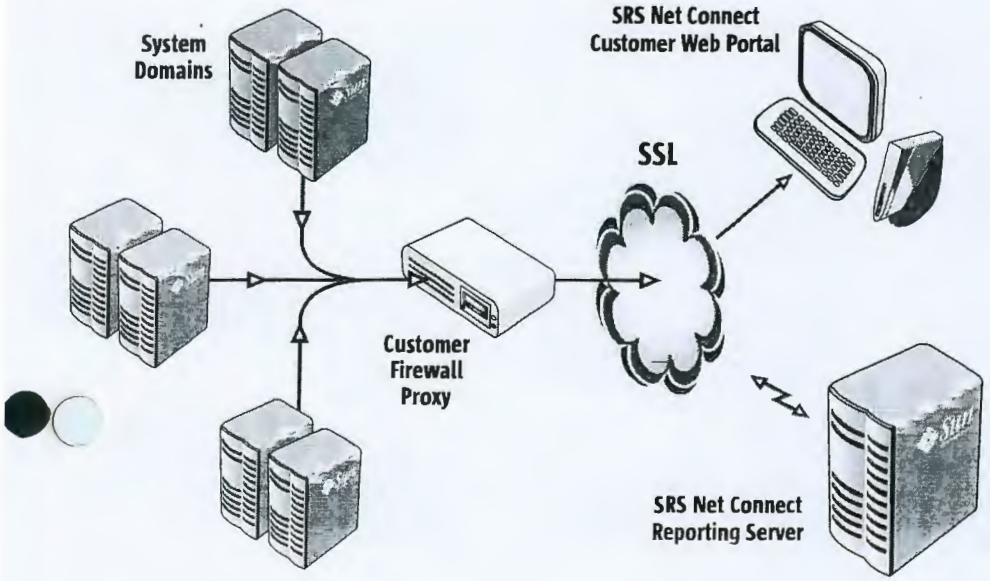
Security:

> Customer firewall proxy is the only connection point to the Internet

> Shared secret exchange between Sun and your systems

> SSL with 128 bit key encryption for all Internet communications

For more information and to download SRS Net Connect, go to **www.sun.com/srs/netconnect.**



Monitoring Hardware Failure variables include:

Temperature

Fan failed

System Board failure

AC Power failure

Corrected ECC

Device media error

Power status lost

CPU offline

And more...

System Performance variables include:

CPU run queue

CPU average utilization

Disk waiting

Memory page scan rate

File system

Disk average service time

Memory buffer cache

Network interface

And more...

Sun Microsystems, Inc. 4150 Network Circle, Santa Clara, CA 95054 USA 1-650-960-1300 or 1-800-555-9sun www.sun.com

Sun microsystems
We make the net work.

SUN

0119

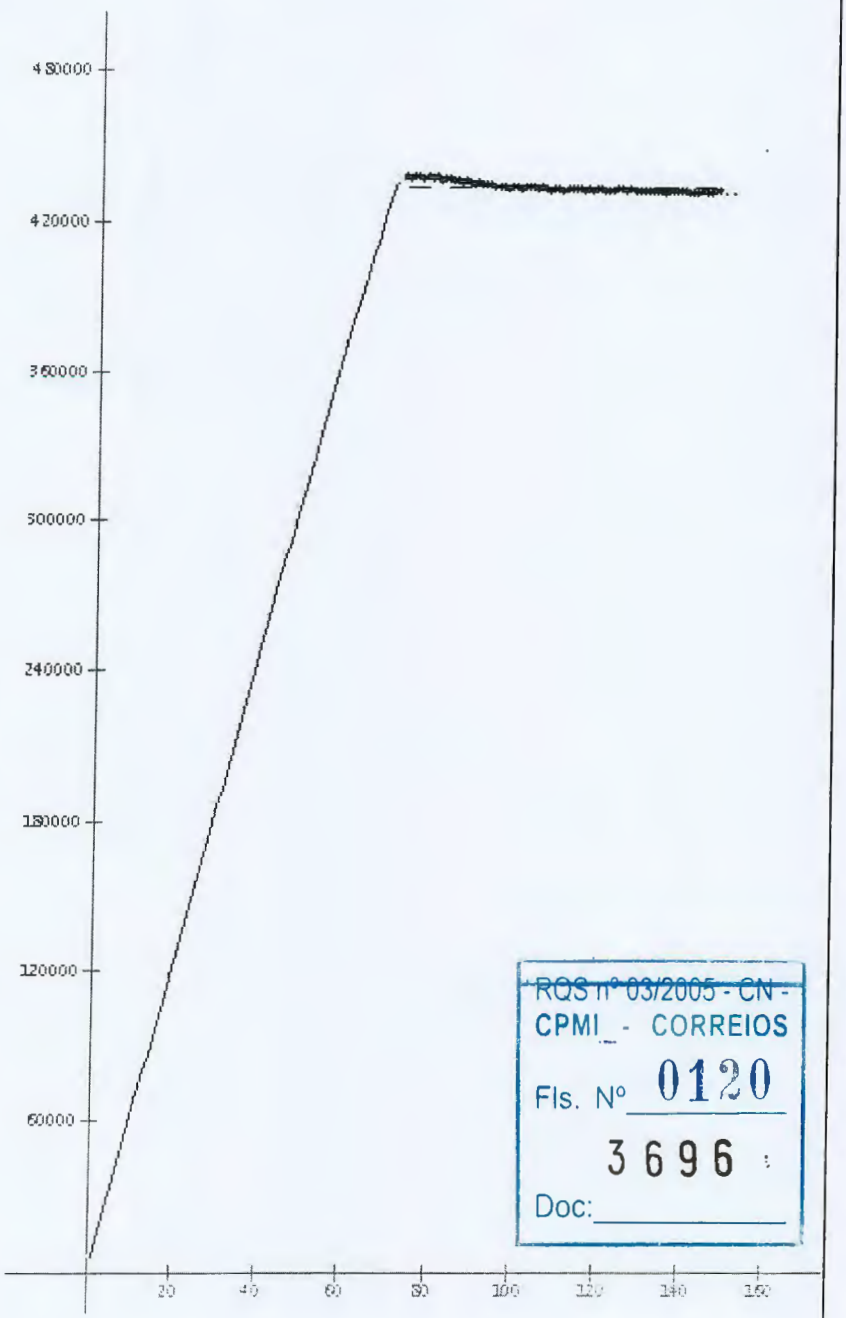
SPECjbb2000

SPECjbb2000 = 433166 ops/s

Sun Microsystems, Inc. Sun Fire 15K

Sun Microsystems, Inc. HotSpot 64-Bit Server VM on Solaris/SPARC, version 1.4.0_01

Warehouses	Ops/s	Incl. in metric
1	6164	
2	12412	
3	18681	
4	24626	
5	30851	
6	37013	
7	43556	
8	49560	
9	56036	
10	61636	
11	68395	
12	73992	
13	80015	
14	86711	
15	93366	
16	99443	
17	105236	
18	110818	
19	118154	
20	124474	
21	129982	
22	136383	
23	142578	
24	148687	
25	155088	
26	161582	
27	167592	
28	173535	
29	180166	
30	187009	
31	193057	
32	199225	
33	205330	
34	211280	



35	217367	
36	223655	
37	230620	
38	236290	
39	242523	
40	248485	
41	254863	
42	261020	
43	268037	
44	274362	
45	279701	
46	285690	
47	291568	
48	298333	
49	304486	
50	310423	
51	316176	
52	322823	
53	328259	
54	334740	
55	341364	
56	346317	
57	353857	
58	359057	
59	365598	
60	371215	
61	377941	
62	382899	
63	389591	
64	395399	
65	400890	
66	407336	
67	412030	
68	417047	
69	423860	
70	428707	
71	433599	
72	436717	
73	436428	
74	437534	*
75	436143	*

77	437089	*
78	436712	*
79	437185	*
80	436265	*
81	437064	*
82	436071	*
83	436479	*
84	436144	*
85	435393	*
86	435699	*
87	435007	*
88	435357	*
89	434565	*
90	434448	*
91	435112	*
92	434269	*
93	434172	*
94	434100	*
95	433548	*
96	433530	*
97	432968	*
98	432906	*
99	433169	*
100	433431	*
101	432476	*
102	433058	*
103	432999	*
104	433053	*
105	432648	*
106	432910	*
107	432423	*
108	431838	*
109	432335	*
110	432470	*
111	431956	*
112	432266	*
113	432379	*
114	432567	*
115	432758	*
116	432084	*
117	432650	*

119	432194	*
120	432111	*
121	431944	*
122	432075	*
123	431878	*
124	432317	*
125	432337	*
126	431955	*
127	432242	*
128	431665	*
129	432037	*
130	431422	*
131	431697	*
132	431588	*
133	431672	*
134	431721	*
135	431147	*
136	431341	*
137	432043	*
138	431690	*
139	431814	*
140	431771	*
141	431299	*
142	431284	*
143	431111	*
144	431606	*
145	431205	*
146	431136	*
147	431605	*
148	431383	*
149	430903	
150	431436	
151	431243	
152	431539	
SPECjbb2000	**(from 74 to 148)**	**433166 ops/s**

SPEC license # 6	**Tested by:** Sun Microsystems, Inc.	**Test date:** Apr 9, 2002

Hardware		**Software**	
Hardware	Sun Microsystems,	**Software Vendor**	Sun Microsystems, Inc.

Vendor	Inc.
Vendor URL	http://www.sun.com
Model	Sun Fire 15K
Processor	UltraSPARC-III Cu
MHz	1050
# of Procs	72
Memory (MB)	294912
Primary cache	32KB(I)+64KB(D)
Secondary cache	8MB(I+D) off chip
Other cache	
Filesystem	UFS
Disks	1 x 18GB SCSI (classes); 1 x 18GB SCSI (OS)
Other hardware	

Vendor URL	http://www.sun.com
Java Precompiler Version	
Java Precompiler Command Line	
Java Precompiler Way Of Excluding Classes	
JVM Version	HotSpot 64-Bit Server VM on Solaris/SPARC, version 1.4
JVM Command Line	java -server -d64 -Xbatch -Xss256k -XX:+UseISM -XX:+AggressiveHeap -classpath ./jbb.jar:./jbb_no_precompile.jar:./check.jar:./rep spec.jbb.JBBmain -propfile SPECjbb.props
JVM Initial Heap Memory (MB)	258048
JVM Maximum Heap Memory (MB)	258048
JVM CLASSPATH	./jbb.jar: ./jbb_no_precompile.jar: ./check.jar: ./reporter.jar
JVM BOOTCLASSPATH	/var/jbb/j2re1.4.0_01/lib/rt.jar: /var/jbb/j2re1.4.0_01/lib/i18n.jar: /var/jbb/j2re1.4.0_01/lib/sunrsasign.jar: /var/jbb/j2re1.4.0_01/lib/jsse.jar: /var/jbb/j2re1.4.0_01/lib/jce.jar: /var/jbb/j2re1.4.0_01/lib/charsets.jar: /var/jbb/j2re1.4.0_01/classes
OS Version	Solaris 8 update 7
System state	normal
Other software	

Test Information	
Tested by	Sun Microsystems, Inc.
SPEC license #	6
Test location	SAE; Beaverton, Oregon
Test date	Apr 9, 2002
H/w available	Aug-2002
JVM available	Jun-2002
OS available	Feb-2002
Other s/w available	

Tuning

Operating system tunings

- /etc/system:
  - autoup=345600
  - tune_t_fsflushr=345600
  - set shmsys:shminfo_shmmax=0xffffffffffffffff
  - set shmsys:shminfo_shmseg=0x800
-
- environment:
  - LD_LIBRARY_PATH=/usr/lib/lwp

Notes

Command line options are described at http://java.sun.com/docs/hotspot

Details of Runs

Warehouses	Thrput	Total heap (MB)		Thread spread %	% > 120s	transaction type	Count	Time (in seconds)	
		Size	Used					total	max
1	6164	250699	33.1	<0.01%	<0.01	new_order	321599	68.9	<0.01
						payment	321599	23.9	.066
						order_status	32160	2.68	<0.01
						delivery	32159	9.26	<0.01
						stock_level	32161	1.00	.091
2	12412	250699	60.5	.731%	<0.01	new_order	647578	139	<0.01
						payment	647578	47.6	<0.01
						order_status	64758	5.19	<0.01
						delivery	64757	19.8	<0.01
						stock_level	64759	18.9	<0.01
3	18681	250699	75.2	1.55%	<0.01	new_order	974765	207	<0.01
						payment	974772	72.1	<0.01
						order_status	97476	8.33	<0.01
						delivery	97475	29.5	<0.01
						stock_level	97477	28.3	<0.01
4	24626	250699	111	1.27%	<0.01	new_order	1284917	276	<0.01
						payment	1284925	96.7	<0.01
						order_status	128493	11.0	<0.01
						delivery	128493	38.7	<0.01
						stock_level	128491	37.2	<0.01
5	30851	250699	117	2.71%	<0.01	new_order	1609692	343	<0.01
						payment	1609688	123	<0.01
						order_status	160969	13.8	<0.01
						delivery	160970	48.6	<0.01
						stock_level	160967	45.8	<0.01
6	37013	250699	163	2.82%	<0.01	new_order	1931223	414	<0.01
						payment	1931207	145	<0.01
						order_status	193123	16.3	<0.01
						delivery	193121	58.2	<0.01
						stock_level	193120	55.4	<0.01
7	43556	250699	160	4.13%	<0.01	new_order	2272622	480	<0.01
						payment	2272620	170	<0.01
						order_status	227262	19.1	<0.01
						delivery	227259	69.1	<0.01
						stock_level	227261	66.0	<0.01
8	49560	250699	217	3.86%	<0.01	new_order	2585903	551	<0.01

						payment	2585883	195	<0.01
						order_status	258587	21.4	<0.01
						delivery	258590	78.0	<0.01
						stock_level	258589	74.5	<0.01
9	56036	250699	200	3.23%	<0.01	new_order	2923819	620	<0.01
						payment	2923818	219	<0.01
						order_status	292385	24.6	<0.01
						delivery	292385	87.5	<0.01
						stock_level	292384	82.9	<0.01
10	61636	250699	264	5.89%	<0.01	new_order	3216052	688	<0.01
						payment	3216060	243	.020
						order_status	321609	26.8	<0.01
						delivery	321604	97.8	<0.01
						stock_level	321607	93.8	<0.01
11	68395	250699	243	5.84%	<0.01	new_order	3568480	755	<0.01
						payment	3568479	271	<0.01
						order_status	356851	29.8	<0.01
						delivery	356848	108	<0.01
						stock_level	356849	102	<0.01
12	73992	250699	315	4.05%	<0.01	new_order	3860579	823	<0.01
						payment	3860580	295	<0.01
						order_status	386055	32.4	<0.01
						delivery	386055	118	<0.01
						stock_level	386061	110	<0.01
13	80015	250699	285	4.98%	<0.01	new_order	4174815	895	<0.01
						payment	4174821	317	<0.01
						order_status	417481	35.0	<0.01
						delivery	417481	127	<0.01
						stock_level	417481	120	<0.01
14	86711	250699	366	6.10%	<0.01	new_order	4524347	962	<0.01
						payment	4524348	343	<0.01
						order_status	452435	37.8	<0.01
						delivery	452434	137	<0.01
						stock_level	452435	130	<0.01
15	93366	250699	329	5.49%	<0.01	new_order	4871514	1028	<0.01
						payment	4871505	369	<0.01
						order_status	487153	41.1	<0.01
						delivery	487152	148	<0.01
						stock_level	487150	139	<0.01
16	99443	250699	421	5.47%	<0.01	new_order	5188694	1097	<0.01
						payment	5188686	392	<0.01

						delivery	518871	158	<0.01
						stock_level	518863	149	<0.01
17	105236	250699	371	4.01%	<0.01	new_order	5491028	1171	.011
						payment	5491030	414	<0.01
						order_status	549103	45.8	<0.01
						delivery	549101	167	<0.01
						stock_level	549103	158	<0.01
18	110818	250699	469	3.04%	<0.01	new_order	5782048	1242	<0.01
						payment	5782042	438	<0.01
						order_status	578200	48.4	<0.01
						delivery	578204	174	<0.01
						stock_level	578202	168	<0.01
19	118154	250699	414	5.86%	.010	new_order	6165164	1307	<0.01
						payment	6165177	465	<0.01
						order_status	616517	51.4	<0.01
						delivery	616518	185	<0.01
						stock_level	616518	175	<0.01
20	124474	250699	526	6.69%	<0.01	new_order	6494900	1372	<0.01
						payment	6494910	491	<0.01
						order_status	649493	53.8	<0.01
						delivery	649489	197	<0.01
						stock_level	649490	185	<0.01
21	129982	250699	450	4.27%	<0.01	new_order	6781921	1443	.026
						payment	6781918	514	<0.01
						order_status	678193	56.5	<0.01
						delivery	678191	205	<0.01
						stock_level	678190	196	<0.01
22	136383	250699	571	8.80%	<0.01	new_order	7115959	1512	<0.01
						payment	7115951	537	<0.01
						order_status	711594	59.3	<0.01
						delivery	711600	216	<0.01
						stock_level	711585	205	<0.01
23	142578	250699	495	9.38%	<0.01	new_order	7439079	1582	<0.01
						payment	7439075	560	<0.01
						order_status	743908	61.1	<0.01
						delivery	743910	227	<0.01
						stock_level	743909	215	<0.01
24	148687	250699	621	5.20%	<0.01	new_order	7757797	1650	<0.01
						payment	7757781	585	<0.01
						order_status	775781	64.6	<0.01
						delivery	775780	237	<0.01

12988

25	155088	250699	539	13.0%	<0.01	new_order	8091678	1713	<0.01
						payment	8091667	612	<0.01
						order_status	809164	67.4	<0.01
						delivery	809164	249	<0.01
						stock_level	809168	233	<0.01
26	161582	250699	676	8.22%	.010	new_order	8431223	1788	<0.01
						payment	8431225	633	<0.01
						order_status	843118	69.1	<0.01
						delivery	843119	257	<0.01
						stock_level	843119	243	<0.01
27	167592	250699	578	6.95%	<0.01	new_order	8744731	1857	<0.01
						payment	8744733	659	<0.01
						order_status	874473	72.8	<0.01
						delivery	874474	267	<0.01
						stock_level	874471	249	<0.01
28	173535	250699	719	5.31%	<0.01	new_order	9054666	1931	<0.01
						payment	9054687	680	<0.01
						order_status	905465	75.0	<0.01
						delivery	905463	275	<0.01
						stock_level	905462	260	<0.01
29	180166	250699	624	9.93%	<0.01	new_order	9400559	1996	<0.01
						payment	9400571	706	<0.01
						order_status	940063	77.8	<0.01
						delivery	940053	286	<0.01
						stock_level	940059	270	<0.01
30	187009	250699	778	7.52%	<0.01	new_order	9757829	2061	<0.01
						payment	9757823	732	<0.01
						order_status	975782	80.4	<0.01
						delivery	975783	297	<0.01
						stock_level	975782	279	<0.01
31	193057	250699	665	7.88%	<0.01	new_order	10073413	2128	<0.01
						payment	10073390	756	<0.01
						order_status	1007336	84.0	<0.01
						delivery	1007337	306	<0.01
						stock_level	1007340	291	<0.01
32	199225	250699	825	8.23%	<0.01	new_order	10395227	2203	<0.01
						payment	10395210	779	<0.01
						order_status	1039524	86.1	<0.01
						delivery	1039515	316	<0.01
						stock_level	1039515	297	<0.01
33	205330	250699	707	9.34%	<0.01	new_order	10713743	2270	<0.01

12987

						order_status	1071377	88.8	<0.01
						delivery	1071371	326	<0.01
						stock_level	1071370	307	<0.01
34	211280	250699	881	8.56%	<0.01	new_order	11023775	2349	<0.01
						payment	11023756	823	<0.01
						order_status	1102379	89.6	<0.01
						delivery	1102377	336	<0.01
						stock_level	1102379	314	<0.01
35	217367	250699	749	6.50%	<0.01	new_order	11341382	2411	<0.01
						payment	11341394	852	<0.01
						order_status	1134133	94.8	<0.01
						delivery	1134140	345	<0.01
						stock_level	1134135	323	<0.01
36	223655	250699	932	7.96%	<0.01	new_order	11669262	2470	<0.01
						payment	11669263	881	<0.01
						order_status	1166925	96.8	<0.01
						delivery	1166931	358	<0.01
						stock_level	1166931	335	<0.01
37	230620	250699	791	6.60%	.010	new_order	12033570	2539	<0.01
						payment	12033543	905	<0.01
						order_status	1203360	99.9	<0.01
						delivery	1203354	368	<0.01
						stock_level	1203356	345	<0.01
38	236290	250699	983	7.39%	<0.01	new_order	12329209	2610	<0.01
						payment	12329211	930	<0.01
						order_status	1232923	102	<0.01
						delivery	1232924	377	<0.01
						stock_level	1232918	354	<0.01
39	242523	250699	834	6.14%	<0.01	new_order	12653989	2679	<0.01
						payment	12654022	951	<0.01
						order_status	1265406	105	<0.01
						delivery	1265405	387	<0.01
						stock_level	1265398	365	<0.01
40	248485	250699	1032	6.25%	.010	new_order	12965711	2752	<0.01
						payment	12965748	975	<0.01
						order_status	1296565	107	<0.01
						delivery	1296575	397	<0.01
						stock_level	1296574	371	<0.01
41	254863	250699	879	6.20%	<0.01	new_order	13298206	2813	<0.01
						payment	13298211	1003	<0.01
						order_status	1329822	110	<0.01

12986

						stock_level	1329821	382	<0.01
42	261020	250699	1085	6.23%	<0.01	new_order	13619369	2888	<0.01
						payment	13619347	1025	<0.01
						order_status	1361937	112	<0.01
						delivery	1361936	417	<0.01
						stock_level	1361939	391	<0.01
43	268037	250699	921	6.41%	<0.01	new_order	13984892	2957	<0.01
						payment	13984884	1051	<0.01
						order_status	1398488	115	<0.01
						delivery	1398483	426	<0.01
						stock_level	1398489	400	<0.01
44	274362	250699	1143	5.97%	<0.01	new_order	14314897	3021	<0.01
						payment	14314903	1075	<0.01
						order_status	1431490	118	<0.01
						delivery	1431484	438	<0.01
						stock_level	1431499	411	<0.01
45	279701	250699	960	7.29%	<0.01	new_order	14594456	3098	<0.01
						payment	14594447	1097	<0.01
						order_status	1459441	121	<0.01
						delivery	1459447	447	<0.01
						stock_level	1459445	415	<0.01
46	285690	250699	1194	5.94%	<0.01	new_order	14906907	3159	<0.01
						payment	14906905	1125	<0.01
						order_status	1490692	124	<0.01
						delivery	1490690	458	.380
						stock_level	1490698	428	<0.01
	291568	250699	1006	6.80%	<0.01	new_order	15212593	3230	<0.01
						payment	15212608	1147	<0.01
						order_status	1521262	126	<0.01
						delivery	1521255	468	<0.01
						stock_level	1521261	438	<0.01
48	298333	250699	1241	6.78%	.010	new_order	15566737	3295	.018
						payment	15566769	1171	.018
						order_status	1556677	128	<0.01
						delivery	1556674	480	.015
						stock_level	1556673	451	<0.01
49	304486	250699	1048	5.97%	.010	new_order	15887793	3362	<0.01
						payment	15887804	1196	<0.01
						order_status	1588781	131	<0.01
						delivery	1588780	492	<0.01
						stock_level	1588775	457	<0.01

12985

50	310423	250699	1294	7.25%	<0.01	payment	16197457	1222	<0.01
						order_status	1619744	133	<0.01
						delivery	1619747	499	<0.01
						stock_level	1619753	470	<0.01
51	316176	250699	1084	5.93%	<0.01	new_order	16497655	3509	<0.01
						payment	16497607	1243	<0.01
						order_status	1649757	136	<0.01
						delivery	1649770	508	<0.01
						stock_level	1649765	474	<0.01
52	322823	250699	1339	5.41%	<0.01	new_order	16843929	3571	<0.01
						payment	16843901	1270	<0.01
						order_status	1684387	140	<0.01
						delivery	1684402	520	<0.01
						stock_level	1684390	485	<0.01
53	328259	250699	1133	7.35%	<0.01	new_order	17127282	3646	<0.01
						payment	17127297	1291	<0.01
						order_status	1712732	142	<0.01
						delivery	1712731	530	<0.01
						stock_level	1712736	492	<0.01
54	334740	250699	1403	6.09%	.010	new_order	17466420	3706	<0.01
						payment	17466431	1318	<0.01
						order_status	1746634	145	<0.01
						delivery	1746648	540	<0.01
						stock_level	1746644	507	<0.01
55	341364	250699	1175	5.37%	<0.01	new_order	17811910	3773	<0.01
						payment	17811911	1344	<0.01
						order_status	1781183	148	<0.01
						delivery	1781184	550	<0.01
						stock_level	1781194	514	<0.01
56	346317	250699	1446	6.16%	.010	new_order	18070511	3851	<0.01
						payment	18070512	1367	<0.01
						order_status	1807052	149	<0.01
						delivery	1807050	560	<0.01
						stock_level	1807053	521	<0.01
57	353857	250699	1212	6.14%	.010	new_order	18463947	3911	<0.01
						payment	18463928	1393	<0.01
						order_status	1846393	153	<0.01
						delivery	1846383	572	<0.01
						stock_level	1846395	533	<0.01
58	359057	250699	1493	7.69%	<0.01	new_order	18734019	3985	<0.01
						payment	18733997	1414	<0.01

0131

12984

						delivery	1873402	581	<0.01
						stock_level	1873404	540	<0.01
59	365598	250699	1260	7.60%	<0.01	new_order	19075294	4057	<0.01
						payment	19075295	1437	<0.01
						order_status	1907532	158	<0.01
						delivery	1907533	590	<0.01
						stock_level	1907526	551	<0.01
60	371215	250699	1548	6.41%	<0.01	new_order	19368850	4118	<0.01
						payment	19368839	1465	<0.01
						order_status	1936882	160	<0.01
						delivery	1936889	602	<0.01
						stock_level	1936879	560	<0.01
61	377941	250699	1304	5.03%	<0.01	new_order	19720151	4185	<0.01
						payment	19720158	1488	<0.01
						order_status	1972013	163	<0.01
						delivery	1972018	612	<0.01
						stock_level	1972008	572	<0.01
62	382899	250699	1596	6.43%	.010	new_order	19979356	4261	<0.01
						payment	19979348	1512	<0.01
						order_status	1997931	166	<0.01
						delivery	1997935	624	<0.01
						stock_level	1997941	575	<0.01
63	389591	250699	1343	6.62%	<0.01	new_order	20328192	4325	<0.01
						payment	20328167	1537	<0.01
						order_status	2032821	168	<0.01
						delivery	2032818	633	.380
						stock_level	2032817	589	<0.01
64	395399	250699	1653	7.02%	<0.01	new_order	20630883	4395	<0.01
						payment	20630883	1560	<0.01
						order_status	2063090	171	<0.01
						delivery	2063077	642	<0.01
						stock_level	2063089	599	<0.01
65	400890	250699	1387	6.67%	<0.01	new_order	20917043	4476	<0.01
						payment	20917065	1581	<0.01
						order_status	2091708	173	<0.01
						delivery	2091701	650	<0.01
						stock_level	2091709	606	<0.01
66	407336	250699	1715	6.97%	<0.01	new_order	21253929	4533	.040
						payment	21253944	1612	.010
						order_status	2125388	176	<0.01
						delivery	2125385	662	.389

12983

67	412030	250699	1430	9.66%	<0.01	new_order	21497961	4612	.381
						payment	21497954	1631	.370
						order_status	2149796	179	<0.01
						delivery	2149798	669	.400
						stock_level	2149794	623	.361
68	417047	250699	1758	8.58%	<0.01	new_order	21760961	4685	.400
						payment	21760978	1653	.390
						order_status	2176090	179	.254
						delivery	2176092	682	.396
						stock_level	2176104	631	.341
69	423860	250699	1465	8.71%	<0.01	new_order	22116088	4753	.090
						payment	22116104	1680	.310
						order_status	2211612	182	<0.01
						delivery	2211598	691	.340
						stock_level	2211611	639	<0.01
70	428707	250699	1803	10.7%	<0.01	new_order	22368984	4826	.390
						payment	22368978	1702	.371
						order_status	2236890	185	<0.01
						delivery	2236893	700	.391
						stock_level	2236894	648	.351
71	433599	250699	1511	9.56%	<0.01	new_order	22624039	4894	.401
						payment	22624068	1727	.380
						order_status	2262410	189	.401
						delivery	2262411	710	.399
						stock_level	2262409	656	.371
72	436717	250699	1855	11.6%	<0.01	new_order	22786942	4964	.401
						payment	22786907	1745	.400
						order_status	2278694	190	.400
						delivery	2278691	724	.399
						stock_level	2278696	669	.401
73	436428	250699	1556	9.76%	<0.01	new_order	22771860	5021	.655
						payment	22771904	1774	.800
						order_status	2277187	194	.400
						delivery	2277182	745	.401
						stock_level	2277194	674	.400
74	437534	250699	1905	9.57%	<0.01	new_order	22828606	5098	.401
						payment	22828617	1793	.401
						order_status	2282859	196	.401
						delivery	2282856	757	.441
						stock_level	2282865	679	.401
75	436143	250699	1594	8.00%	<0.01	new_order	22755860	5160	.521

						order_status	2275596	195	.390
						delivery	2275581	787	.490
						stock_level	2275582	690	.401
76	437219	250699	1946	9.73%	<0.01	new_order	22812199	5208	.401
						payment	22812213	1838	.550
						order_status	2281224	198	.401
						delivery	2281214	814	.401
						stock_level	2281221	698	.402
77	437089	250699	1637	9.07%	<0.01	new_order	22805760	5269	.401
						payment	22805785	1859	.737
						order_status	2280577	203	.400
						delivery	2280578	837	.408
						stock_level	2280573	704	.401
78	436712	250699	1999	11.3%	<0.01	new_order	22786709	5340	.691
						payment	22786692	1885	.635
						order_status	2278666	204	.400
						delivery	2278670	845	.401
						stock_level	2278674	712	.401
79	437185	250699	1667	10.2%	<0.01	new_order	22811169	5385	.401
						payment	22811211	1905	.545
						order_status	2281130	205	.400
						delivery	2281111	870	.723
						stock_level	2281125	734	.401
80	436265	250699	2031	9.87%	<0.01	new_order	22763538	5466	.458
						payment	22763561	1915	.686
						order_status	2276360	208	.401
						delivery	2276350	903	.411
						stock_level	2276356	728	.401
81	437064	250699	1709	12.0%	<0.01	new_order	22804091	5508	.489
						payment	22804107	1940	.708
						order_status	2280399	219	.401
						delivery	2280406	930	.800
						stock_level	2280409	737	.401
82	436071	250699	2074	10.0%	<0.01	new_order	22753631	5585	.659
						payment	22753621	1948	.642
						order_status	2275368	215	.401
						delivery	2275360	952	.702
						stock_level	2275368	748	.401
83	436479	250699	1751	9.81%	<0.01	new_order	22774329	5594	.401
						payment	22774307	1957	.791
						order_status	2277430	215	.551

						stock_level	2277435	747	.401
84	436144	250699	2125	11.6%	<0.01	new_order	22757050	5698	.795
						payment	22757078	2005	.687
						order_status	2275706	217	.400
						delivery	2275695	1005	.800
						stock_level	2275702	756	.401
85	435393	250699	1796	10.5%	<0.01	new_order	22717099	5744	.800
						payment	22717134	2043	.660
						order_status	2271711	224	.401
						delivery	2271722	1026	.801
						stock_level	2271720	766	.401
86	435699	250699	2176	14.2%	<0.01	new_order	22733460	5810	.424
						payment	22733447	2051	.591
						order_status	2273339	215	.401
						delivery	2273346	1068	1.20
						stock_level	2273343	779	.401
87	435007	250699	1828	11.2%	<0.01	new_order	22697869	5854	.524
						payment	22697924	2046	.694
						order_status	2269790	223	.401
						delivery	2269791	1124	.799
						stock_level	2269789	778	.402
88	435357	250699	2218	12.3%	<0.01	new_order	22715782	5958	.409
						payment	22715812	2077	.675
						order_status	2271584	222	.401
						delivery	2271584	1106	1.02
						stock_level	2271574	781	.401
	434565	250699	1865	12.4%	<0.01	new_order	22674879	5991	.666
						payment	22674859	2143	.798
						order_status	2267479	224	.400
						delivery	2267492	1120	.803
						stock_level	2267482	793	.401
90	434448	250699	2246	15.6%	<0.01	new_order	22668712	6056	.692
						payment	22668727	2131	.701
						order_status	2266874	229	.411
						delivery	2266879	1153	.799
						stock_level	2266869	809	.401
91	435112	250699	1906	11.5%	<0.01	new_order	22703178	6117	.617
						payment	22703212	2147	.606
						order_status	2270310	237	.401
						delivery	2270312	1201	.929
						stock_level	2270318	797	.801

92	434269	250699	2299	12.7%	<0.01	payment	22658258	2167	.599
						order_status	2265820	236	.782
						delivery	2265829	1282	.860
						stock_level	2265834	819	.401
93	434172	250699	1943	14.2%	<0.01	new_order	22653180	6232	.642
						payment	22653196	2184	.800
						order_status	2265324	232	.401
						delivery	2265324	1257	.801
						stock_level	2265324	825	.401
94	434100	250699	2332	16.7%	.010	new_order	22650980	6291	.615
						payment	22650973	2211	.699
						order_status	2265094	233	.401
						delivery	2265093	1290	1.08
						stock_level	2265087	822	.401
95	433548	250699	1978	13.9%	<0.01	new_order	22621785	6331	.800
						payment	22621791	2222	.802
						order_status	2262181	244	.440
						delivery	2262189	1340	.801
						stock_level	2262183	825	.401
96	433530	250699	2374	15.0%	<0.01	new_order	22620652	6382	.409
						payment	22620601	2266	.681
						order_status	2262063	242	.401
						delivery	2262063	1334	.801
						stock_level	2262066	850	.401
97	432968	250699	2018	16.0%	<0.01	new_order	22591305	6444	.800
						payment	22591315	2271	.749
						order_status	2259127	245	.401
						delivery	2259129	1378	1.20
						stock_level	2259136	856	.401
98	432906	250699	2428	16.1%	<0.01	new_order	22588509	6438	.500
						payment	22588478	2243	.799
						order_status	2258846	244	.400
						delivery	2258844	1539	1.17
						stock_level	2258856	847	.401
99	433169	250699	2057	17.2%	≤0.01	new_order	22601421	6540	.476
						payment	22601449	2302	.799
						order_status	2260144	255	.401
						delivery	2260154	1459	1.57
						stock_level	2260140	867	.401
100	433431	250699	2461	13.8%	<0.01	new_order	22615125	6610	.521
						payment	22615125	2343	.642

						delivery	2261504	1446	.801
						stock_level	2261524	876	.402
101	432476	250699	2089	15.1%	<0.01	new_order	22565285	6645	.791
						payment	22565284	2341	.797
						order_status	2256534	248	.401
						delivery	2256518	1549	1.20
						stock_level	2256546	872	.401
102	433058	250699	2502	15.3%	<0.01	new_order	22596232	6687	.405
						payment	22596202	2369	.748
						order_status	2259624	254	.401
						delivery	2259621	1593	1.04
						stock_level	2259612	884	.401
103	432999	250699	2136	13.0%	<0.01	new_order	22592958	6781	.800
						payment	22592963	2376	.793
						order_status	2259291	254	.401
						delivery	2259309	1561	1.20
						stock_level	2259301	910	.402
104	433053	250699	2562	18.5%	<0.01	new_order	22595989	6859	.751
						payment	22595961	2392	.634
						order_status	2259596	272	.401
						delivery	2259603	1557	1.60
						stock_level	2259594	914	.401
105	432648	250699	2168	17.0%	<0.01	new_order	22574436	6879	.800
						payment	22574424	2415	.794
						order_status	2257444	262	.401
						delivery	2257440	1653	1.24
						stock_level	2257440	911	.401
106	432910	250699	2587	18.1%	<0.01	new_order	22588133	6930	.611
						payment	22588149	2443	.642
						order_status	2258806	275	.401
						delivery	2258813	1678	1.20
						stock_level	2258805	912	.491
107	432423	250699	2207	15.3%	<0.01	new_order	22562125	6973	.431
						payment	22562109	2488	.648
						order_status	2256220	273	.450
						delivery	2256216	1700	1.20
						stock_level	2256209	927	.402
108	431838	250699	2642	17.6%	<0.01	new_order	22531069	7064	.429
						payment	22531037	2481	.675
						order_status	2253115	265	.401
						delivery	2253098	1701	1.20

12178

109	432335	250699	2243	18.7%	<0.01	new_order	22557163	7124	.800
						payment	22557160	2495	.799
						order_status	2255719	272	.401
						delivery	2255712	1752	1.20
						stock_level	2255715	943	.402
110	432470	250699	2676	22.6%	.010	new_order	22565911	7083	.706
						payment	22565919	2502	.797
						order_status	2256592	281	.401
						delivery	2256595	1902	1.59
						stock_level	2256590	929	.402
111	431956	250699	2282	19.9%	<0.01	new_order	22538175	7032	.634
						payment	22538146	2507	.800
						order_status	2253819	278	.401
						delivery	2253819	2079	1.20
						stock_level	2253809	929	.402
112	432266	250699	2710	14.4%	<0.01	new_order	22555114	7231	.801
						payment	22555078	2558	.795
						order_status	2255511	284	.421
						delivery	2255498	1912	1.60
						stock_level	2255493	961	.401
113	432379	250699	2324	15.1%	<0.01	new_order	22561014	7253	2.52
						payment	22560976	2584	.790
						order_status	2256086	273	.411
						delivery	2256102	1991	1.60
						stock_level	2256079	963	2.00
114	432567	250699	2747	16.1%	<0.01	new_order	22570791	7349	.793
						payment	22570785	2599	.667
						order_status	2257085	280	.646
						delivery	2257071	1977	1.20
						stock_level	2257084	974	.411
115	432758	250699	2357	16.4%	<0.01	new_order	22580579	7373	2.53
						payment	22580544	2586	2.00
						order_status	2258052	294	.403
						delivery	2258028	2044	1.60
						stock_level	2258058	987	.402
116	432084	250699	2789	15.7%		new_order	22544995	7428	2.45
						payment	22545009	2627	2.00
						order_status	2254498	289	.401
						delivery	2254498	2055	1.59
						stock_level	2254497	992	.411
117	432650	250699	2397	17.6%	<0.01	new_order	22574348	7448	2.23

12977

						order_status	2257444	285	.794
						delivery	2257444	2138	2.00
						stock_level	2257435	1001	.401
118	431677	250699	2831	13.1%	<0.01	new_order	22523204	7470	.550
						payment	22523193	2668	.807
						order_status	2252336	289	.401
						delivery	2252320	2203	1.83
						stock_level	2252329	1001	.411
119	432194	250699	2437	14.8%	<0.01	new_order	22550931	7642	2.00
						payment	22550913	2695	.998
						order_status	2255094	292	1.78
						delivery	2255098	2105	1.59
						stock_level	2255092	1009	2.00
120	432111	250699	2853	12.3%	<0.01	new_order	22546415	7617	.796
						payment	22546400	2689	.804
						order_status	2254652	304	.401
						delivery	2254639	2259	1.69
						stock_level	2254633	1011	.401
121	431944	250699	2479	14.0%	<0.01	new_order	22537536	7685	.800
						payment	22537514	2714	.799
						order_status	2253750	290	.578
						delivery	2253753	2295	1.60
						stock_level	2253763	1003	.521
122	432075	250699	2888	16.8%	<0.01	new_order	22543817	7681	2.58
						payment	22543766	2698	1.82
						order_status	2254375	293	.401
						delivery	2254381	2417	1.55
						stock_level	2254377	1020	.401
123	431878	250699	2515	13.4%	<0.01	new_order	22534293	7815	2.39
						payment	22534273	2748	.795
						order_status	2253439	307	.403
						delivery	2253422	2309	1.68
						stock_level	2253441	1030	2.19
124	432317	250699	2933	15.2%	<0.01	new_order	22557172	7796	2.50
						payment	22557173	2744	.799
						order_status	2255719	299	.401
						delivery	2255712	2480	1.60
						stock_level	2255721	1037	.410
125	432337	250699	2551	18.2%	<0.01	new_order	22557110	7816	2.36
						payment	22557073	2757	2.30
						order_status	2255698	294	.677

12976
E

						stock_level	2255714	1036	2.21
126	431955	250699	2969	13.5%	<0.01	new_order	22538691	7885	2.55
						payment	22538682	2781	2.00
						order_status	2253859	302	.797
						delivery	2253876	2554	2.39
						stock_level	2253869	1038	2.00
127	432242	250699	2588	16.1%	<0.01	new_order	22553068	7906	2.26
						payment	22553079	2816	.860
						order_status	2255302	312	.404
						delivery	2255299	2592	2.59
						stock_level	2255306	1047	.401
128	431665	250699	3020	17.4%	<0.01	new_order	22522415	7819	2.43
						payment	22522425	2795	2.52
						order_status	2252242	299	.401
						delivery	2252246	2873	2.00
						stock_level	2252240	1025	2.00
129	432037	250699	2629	14.8%	<0.01	new_order	22542025	8031	.787
						payment	22542003	2881	2.00
						order_status	2254192	312	.531
						delivery	2254200	2628	2.00
						stock_level	2254196	1060	.402
130	431422	250699	3056	16.2%	<0.01	new_order	22509911	8018	2.51
						payment	22509937	2854	.968
						order_status	2250992	309	.411
						delivery	2250986	2773	1.76
						stock_level	2251003	1073	2.00
[illegible]	431697	250699	2664	14.7%	<0.01	new_order	22523501	8171	2.19
						payment	22523551	2906	2.00
						order_status	2252346	322	.796
						delivery	2252363	2668	1.60
						stock_level	2252358	1088	.402
132	431588	250699	3087	18.4%	<0.01	new_order	22519542	8175	2.00
						payment	22519519	2873	2.37
						order_status	2251951	330	2.00
						delivery	2251948	2828	2.30
						stock_level	2251951	1080	2.43
133	431672	250699	2704	16.0%	<0.01	new_order	22522943	8224	2.28
						payment	22522969	2898	2.40
						order_status	2252292	321	.401
						delivery	2252289	2853	2.40
						stock_level	2252287	1100	2.00

12975

134	431721	250699	3131	16.7%	<0.01	payment	22525284	2890	2.41
						order_status	2252526	323	2.54
						delivery	2252534	3102	2.00
						stock_level	2252539	1049	2.00
135	431147	250699	2745	15.3%	<0.01	new_order	22495939	8138	2.49
						payment	22495918	2892	2.48
						order_status	2249586	322	.401
						delivery	2249612	3224	2.52
						stock_level	2249601	1080	1.82
136	431341	250699	3161	16.9%	<0.01	new_order	22506079	8327	2.59
						payment	22506080	2950	2.48
						order_status	2250601	321	.797
						delivery	2250606	3030	2.36
						stock_level	2250617	1104	2.29
137	432043	250699	2788	15.4%	<0.01	new_order	22542654	8396	2.59
						payment	22542667	2923	2.09
						order_status	2254267	315	1.69
						delivery	2254261	3114	2.37
						stock_level	2254280	1099	2.56
138	431690	250699	3205	15.1%	<0.01	new_order	22524499	8420	2.57
						payment	22524470	3033	2.32
						order_status	2252437	319	.643
						delivery	2252444	3069	2.57
						stock_level	2252440	1127	2.46
139	431814	250699	2817	15.7%	<0.01	new_order	22530001	8455	2.59
						payment	22529987	2999	2.54
						order_status	2253006	323	.978
						delivery	2252982	3191	2.28
						stock_level	2252989	1106	2.00
140	431771	250699	3242	17.4%	<0.01	new_order	22528315	8354	2.28
						payment	22528325	3000	2.32
						order_status	2252834	323	2.32
						delivery	2252838	3457	2.10
						stock_level	2252835	1088	2.55
141	431299	250699	2857	17.1%	<0.01	new_order	22502913	8507	2.58
						payment	22502941	3036	2.34
						order_status	2250298	332	.401
						delivery	2250287	3339	2.07
						stock_level	2250291	1121	.741
142	431284	250699	3276	19.1%	<0.01	new_order	22503499	8396	2.55
						payment	22503478	2985	2.26

12974

						delivery	2250354	3687	2.11
						stock_level	2250348	1084	2.42
143	431111	250699	2889	18.5%	<0.01	new_order	22494260	8663	2.57
						payment	22494248	3054	2.24
						order_status	2249433	338	.630
						delivery	2249423	3381	2.40
						stock_level	2249419	1146	2.54
144	431606	250699	3315	16.6%	<0.01	new_order	22518962	8635	2.61
						payment	22518953	3061	2.48
						order_status	2251881	340	2.00
						delivery	2251905	3516	2.40
						stock_level	2251888	1118	1.84
145	431205	250699	2934	14.9%	<0.01	new_order	22499684	8592	2.58
						payment	22499700	3020	2.59
						order_status	2249968	330	2.23
						delivery	2249980	3751	2.25
						stock_level	2249963	1110	2.00
146	431136	250699	3348	17.6%	<0.01	new_order	22494609	8796	2.53
						payment	22494623	3101	2.91
						order_status	2249476	357	.797
						delivery	2249456	3465	2.91
						stock_level	2249461	1158	2.44
147	431605	250699	2965	16.4%	<0.01	new_order	22520376	8869	2.72
						payment	22520386	3160	2.85
						order_status	2252031	332	1.20
						delivery	2252040	3478	2.59
						stock_level	2252036	1174	2.80
148	431383	250699	3400	18.1%	<0.01	new_order	22508992	8901	2.85
						payment	22508998	3120	2.53
						order_status	2250899	341	2.23
						delivery	2250905	3594	2.52
						stock_level	2250890	1190	2.52
149	430903	250699	3004	19.1%	<0.01	new_order	22483029	8827	3.14
						payment	22482994	3145	2.75
						order_status	2248299	352	2.00
						delivery	2248293	3776	2.81
						stock_level	2248302	1160	2.31
150	431436	250699	3431	22.9%	<0.01	new_order	22510840	8896	2.95
						payment	22510776	3139	2.92
						order_status	2251084	342	2.42
						delivery	2251097	3811	2.84

2913

151	431243	250699	3050	18.9%	<0.01	new_order	22500583	8984	3.00
						payment	22500592	3193	2.96
						order_status	2250060	352	2.41
						delivery	2250069	3750	3.10
						stock_level	2250061	1187	2.57
152	431539	250699	3472	18.5%	<0.01	new_order	22516201	9069	3.07
						payment	22516186	3218	2.85
						order_status	2251612	358	2.70
						delivery	2251615	3727	2.90
						stock_level	2251618	1211	2.85

SPECjbb2000 Version: [SPECjbb2000 1.02, December 14, 2001]

Doc (2A)

Sun microsystems

Now your Sun systems can take full advantage of next-generation GigaSwift Ethernet technology with a network interface card designed for copper cable applications.

Sun™ GigaSwift Ethernet UTP Adapter

HIGHLIGHTS

- Sun-developed GigaSwift Ethernet ASIC delivers 1-Gbps performance
- Supports Cat 5 UTP unshielded twisted pair copper media
- Enjoy high-bandwidth services like voice, video, and data at an affordable cost
- Increased bandwidth provides efficient, high-speed backups of large data files
- Creates an end-to-end, Gigabit Ethernet pipe to move large files for usage and backup
- Delivers Gigabit-speed network computing for EAD/CAM workstations and other high-performance simulation applications

Designed to provide next-generation, high-performance services by bringing your Sun servers and workstations up to speed with the Sun™ GigaSwift Ethernet UTP Adapter. Utilizing a single port, the adapter provides high bandwidth, server-to-server or server-to-switch connections, through copper media, at Gigabit speed—an order of magnitude faster than Fast Ethernet. By reducing CPU processing loads with packet parsing, hardware checksum generation and interrupt coalescing, server efficiency is increased, alleviating network congestion on the corporate computer backbone and enhancing performance. Because the Sun GigaSwift Ethernet UTP Adapter complies with IEEE 802.3 standards, existing infrastructure, applications, and expertise can be retained when upgrading portions of the network to GigaSwift Ethernet technology. This interoperability protects your investment while helping to enable a smooth migration and lower total cost of ownership. Developed by Sun, the adapter offers a high level of functionality and reliability.

Purchase these products from the Sun Store, sun.com/store or contact an authorized Sun reseller near you.

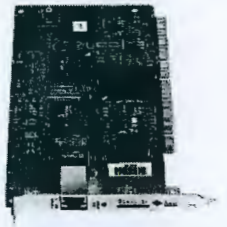
SUN GIGASWIFT ETHERNET UTP ADAPTER

FEATURES

- 1000BASE-T Gigabit performance
- Fully compliant with IEEE 802.3ab standards
- Supports IEEE 802.1Q VLAN
- Supports IEEE 802.1P/802.1D Priority Tagging
- Sun-developed high-performance ASIC

BENEFITS

- Increased productivity and cost savings through high network throughput
- Low cost of ownership and investment protection through open system and interoperability
- Increased network security and cost savings through departmental network segmentation to relieve network congestion
- Increased network reliability and cost savings through support for Quality of Service for mission-critical traffic service
- Sun quality and performance



UTP Adapter, front

UTP Adapter, back

SUN GIGASWIFT ETHERNET UTP ADAPTER SPECIFICATIONS

PCI BUS

	32/64 bit, 33/66 MHz
	Single slot universal
	5V or 3.3V DC
	Half length

OPERATING ENVIRONMENTS SUPPORTED

	Solaris™ 2.6 and later releases

STANDARDS COMPLIANCE

	IEEE 802.3ab Gigabit Ethernet Standards
	IEEE 802.1Q VLAN
	IEEE 802.1P/802.1D Priority Tagging/Quality of Service

ENVIRONMENTAL

Operating temperature	0° C to 55° C
Storage temperature	-40° C to 85° C
Relative humidity	0% to 95%, noncondensing
Shock and vibration	Operating shock: 2.5 G, 11 msec., 1/2 sine
	Nonoperating shock: 18 G, 11 msec., 1/2 sine, 6/face
	Operating vibration: 0.25 G, 5 to 500 Hz
	Nonoperating vibration: 0.6 G, 5 to 500 Hz
Dimensions	17.5 cm x 10.6 cm (6.9 in. x 4.2 in.)

CONNECTIONS

	RJ 45 UTP connector for Cat 5 copper cabling 4-pair

POWER CONSUMPTION

	Typical 12 Watts (2.4A at 5V)
	Max 15 Watts (3.0A at 5V)

OPERATING DISTANCE

	Up to 100 meters

HEADQUARTERS SUN MICROSYSTEMS, INC., 901 SAN ANTONIO ROAD, PALO ALTO, CA 94303-4900 USA
PHONE: 650 960-1300 OR 800 555-9SUN INTERNET: www.sun.com

Sun microsystems

take it to the n[th]

SALES OFFICES

AFRICA (NORTH, WEST AND CENTRAL): +9714-3366333 • ARGENTINA: +5411-4317-5600 • AUSTRALIA: +61-2-9844-5000 • AUSTRIA: +43-1-60563-0 • BELGIUM: +32-2-704-8000 • BRAZIL: +55-11-5187-2100 • CANADA: +905-477-6745 • CHILE: +56-2-3724500 • COLOMBIA: +571-629-2323 • COMMONWEALTH OF INDEPENDENT STATES: +7-502-935-8411 • CZECH REPUBLIC: +420-2-3300-9311 • DENMARK: +45 4556 5000 • EGYPT: +202-570-9442 • ESTONIA: +372-6-308-900 • FINLAND: +358-9-525-561 • FRANCE: +33-01-30-67-50-00 • GERMANY: +49-89-46008-0 • GREECE: +30-1-618-8111 • HUNGARY: +36-1-202-4415 • ICELAND: +354-563-3010 • INDIA: +91-80-5599595 • IRELAND: +353-1-8055-666 • ISRAEL: +972-9-9513465 • ITALY: +39-039-60551 • JAPAN: +81-3-5717-5000 • KAZAKHSTAN: +7-3272-466774 • KOREA: +822-3469-0114 • LATVIA: +371-750-3700 • LITHUANIA: +370-729-8468 • LUXEMBOURG: +352-49 11 33 1 • MALAYSIA: +603-264-9988 • MEXICO: +52-5-258-6100 • THE NETHERLANDS: +00-31-33-45-15-000 • NEW ZEALAND: +64-4-499-2344 • NORWAY: +47-2202-3900 • PEOPLE'S REPUBLIC OF CHINA: BEIJING: +86-10-6803-5588; CHENGDU: +86-28-619-9333; GUANGZHOU: +86-20-8755-5900; SHANGHAI: +86-21-6466-1228; HONG KONG: +852-2202-6688 • POLAND: +48-22-8747800 • PORTUGAL: +351-21-4134000 • RUSSIA: +7-502-935-8411 SINGAPORE: +65-438-1888 • SLOVAK REPUBLIC: +421-7-4342 94 85 • SOUTH AFRICA: +2711-805-4305 • SPAIN: +34-91-596-9900 • SWEDEN: +46-8-631-10-00 • SWITZERLAND: GERMAN: 41-1-908-90-00; FRENCH: 41-22-999-0444 • TAIWAN: +886-2-2514-0567 • THAILAND: +662-636-1555 TURKEY: +90-212-335 22-00 • UNITED ARAB EMIRATES: +9714-3366333 • UNITED KINGDOM: +44-1-276-20444 • UNITED STATES: +1-800-555-9SUN OR +1-650-960-1300 • VENEZUELA: +58-2-905-3800 • WORLDWIDE HEADQUARTERS: +1-800-555-9SUN OR +1-650-960-1300

Doc 2

On the Web | www.sun.com/storage

Sun StorEdge™ 2 Gb PCI Single and Dual Fibre Channel Network Host Bus Adapter (HBA)

Product Brief

The Sun StorEdge™ 2 Gb PCI Single and Dual Fibre Channel Network Host Bus Adapter (HBA) has been optimized for peak performance and real-world scalability in storage area networks (SANs). Engineered for maximum bandwidth, our HBA eliminates host bus bottlenecks that may impede the high-performance of 2 Gb Fibre Channel and creates a balanced solution. With support for multiple protocols — SCSI, IP, and FC-Tape — our HBA is optimized for high-speed data movement and system management, providing the flexibility needed to run complex storage networks. Sun StorEdge™ Traffic Manager software helps dramatically simplify administration by providing superior SAN-wide failover and load balancing between HBAs to improve availability and address storage growth without adding complexity.

Sun StorEdge Complete Storage Solutions — providing you with comprehensive hardware, software, and services to solve your business challenges enterprise-wide.

High data transfer rate
Supports up to 400 MB/sec Fibre Channel data transfer rates in Full Duplex mode.

Choice of models
Single and Multi channel models.

Hands-off management
Automatically negotiates Fibre Channel bit rate (1 or 2 Gb).

Complete compatibility
Backwards compatible with standard 33 and 66 MHz PCI.

Specifications

Fibre Channel chip	QLogic ISP2312A (single-port card) QLogic ISP2342A (dual-port card)
RAM (per Fibre Channel port)	256 KB
Onboard intelligence	Single chip engine includes enhanced RISC processor, Fibre Channel Protocol manager, PCI DMA controller, 2 Gb transceivers, and on-chip frame buffers.
Topology	FC-AL, Point-to-Point, Fabric
Fabric support	F-Port
Class of service	Class 3
Transfers	Full Duplex in point-to-point and fabric topologies.
Protocols	SCSI, FCP2 (FC-Tape), IP
Host bus	Conforms to PCI X Specification 1.0 and PCI Local Bus Specification 2.2.
FC data transfers	Up to 400 MB/sec per channel with Full Duplex.

Power Consumption	
Single-channel PCI	< 6 Watts
Dual-channel PCI	< 12 Watts
Form Factor	
Standard half card PCI	6.875" x 4.200"
3U compact PCI	6.600" x 2.536"
Environment	
Operating	0° C to 55° C (32° F to 131° F) 5% to 90% relative humidity, noncondensing
Nonoperating	-20° C to 65° C (-40° F to 149° F) 0% to 95% relative humidity, noncondensing
Host Software	
Software drivers	PCI: Sun StorEdge Network Foundation Software 6.0

145

1297
3

The versatile, high-speed adapter for reliable LAN and storage connectivity.

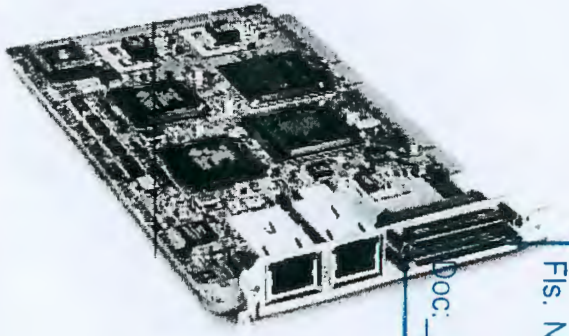
Sun™ Dual Fast Ethernet + Dual SCSI PCI Adapter

HIGHLIGHTS

- Provides two independent FastEthernet ports (dual RJ-45) and two independent 80-MB/sec. Ultra SCSI-2 ports (dual VHDCI) on a single 32/64-bit, 33/66-MHz PCI card
- Supports single-ended and low-voltage differential signaling for use of longer cables
- Auto-negotiation capability allows immediate connection to existing 10-Mb/sec. Ethernet or migration to 100-Mb/sec. FastEthernet
- Supports load balancing for RX packets among multiple CPUs
- Features dynamic reconfiguration, redundancy, and failover support for high availability
- Provides built-in bootable drivers (Solaris™ 8 Operating Environment, update 7 only)
- Supports 3.3-V or 5-V PCI slots (universal)
- Features low CPU utilization for efficient use of server resources and bandwidth
- Compliant with IEEE 802.3u for interoperability
- Supports infinite burst capabilities (on UltraSPARC™ III processor-based servers only)

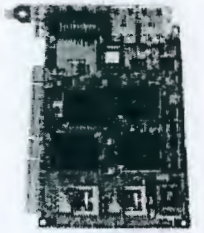
Purchase these products from the Sun™ Store, sun.com/store or contact an authorized Sun reseller near you.

Today's enterprise and Internet data center environments demand high-speed, high-density, affordable solutions for attaching to both LAN environments and storage devices. And Sun meets that demand with the Sun™ Dual Fast Ethernet + Dual SCSI PCI adapter. The adapter features four ports on a single, full-size PCI card—two FastEthernet ports for LAN connectivity and two Ultra SCSI-2 ports for attaching to SCSI-2 compliant peripherals—which saves valuable slots and lowers cost of ownership by simplifying service and support. Plus, the Sun Dual Fast Ethernet + Dual SCSI PCI adapter supports universal PCI powering environments, features 64-bit ASICs for improved bus operation, and accommodates single-ended and low-voltage differential signaling—for an extremely versatile solution. And its auto-negotiation capabilities provide backward compatibility with 10-BaseT Ethernet environments, for outstanding investment protection.

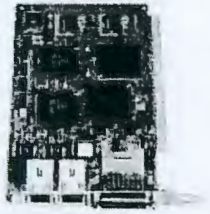


SUN DUAL FAST ETHERNET + DUAL SCSI PCI ADAPTER

Enterprises and Internet data centers alike look to Sun to provide high-performance, versatile, highly reliable networking solutions. The Sun Dual Fast Ethernet + Dual SCSI PCI adapter delivers two FastEthernet ports and two SCSI ports on a single PCI card—for reliable performance with minimal downtime and lower total cost of ownership.



Back



Front

SUN DUAL FAST ETHERNET + DUAL SCSI PCI ADAPTER SPECIFICATIONS

PERFORMANCE

PCI clock	Maximum 33/66 MHz
PCI data burst transfer rate	Up to 64-byte bursts
SCSI synchronous transfer rate	80 MB/sec.
SCSI asynchronous transfer rate	Maximum 12 MB/sec. (16-bit) Maximum 6 MB/sec. (8-bit)
Transfer size	Maximum 4 GB
PCI data/address lines	AD31-0 or AD63-0
PCI modes	Master/slave
SCSI interface	Single-ended (SE) Low Voltage Differential (LVD)
SCSI bus parity	Yes
SCSI 8-bit bus devices	Yes
SCSI 16-bit bus devices	Yes
10-BaseT transfer rate	Up to 10 Mb/sec.
100-BaseT transfer rate	Up to 100 Mb/sec.

HARDWARE SUPPORTED

Servers	
Sun Ultra™	30, 60, 80
Sun Enterprise™	220R, 420R, 250, 450, 2800, 4800, 6800, E10K, E15K
Sun Blade™	100, 1000
Sun Fire™	4800, 4810, 6800
StorEdge™	S1
Peripherals	All Sun-supported SCSI-2 devices

SOFTWARE SUPPORTED

Operating environment	Solaris Operating Environment 8, update 7 and higher
Firmware	OpenBoot™ PROM 3.0 and higher
Diagnostic	SunVTS™ 4.4 and higher

POWER REQUIREMENTS

Power consumption	Maximum 10 W
Voltage	3.3 V and 5 V

DIMENSIONS AND WEIGHT

Length	175 mm (6.8 in.)
Width	107 mm (4.2 in.)

HEADQUARTERS SUN MICROSYSTEMS, INC., 901 SAN ANTONIO ROAD, PALO ALTO, CA 94303-4900 USA
PHONE: 650 960-1300 OR 800 555-9SUN INTERNET: www.sun.com

take it to the n[th]

SALES OFFICES

AFRICA (NORTH, WEST AND CENTRAL): +9714 3366333 • ARGENTINA: +5411-4317-5600 • AUSTRALIA: +61-2-9844-5000 • AUSTRIA: +43-1-60563-0 • BELGIUM: +32-2-704-8000 • BRAZIL: +55-11-5187-2100 • CANADA: +905-477-6745 • CHILE: +56-2-3724500 • COLOMBIA: +571-629-2323 • COMMONWEALTH OF INDEPENDENT STATES: +7-502-935-8411 • CZECH REPUBLIC: +420-2-3300-9311 • DENMARK: +45 4556 5000 • EGYPT: +202 570-9442 • ESTONIA: +372-6-308-900 • FINLAND: +358-9-525-561 • FRANCE: +33-01-30-67-50-00 • GERMANY: +49-89-46008-0 • GREECE: +301-618-8111 • HUNGARY: +36-1-202-4415 • ICELAND: +354-563-3010 • INDIA: +91-80-5589595 • IRELAND: +353-1-8055-666 • ISRAEL: +972-9-9710500 • ITALY: +39-039-60551 • JAPAN: +81-3-5717-5000 • KAZAKHSTAN: +7-3272-466774 • KOREA: +822-2193-5114 • LATVIA: +371-750-3700 • LITHUANIA: +370-729-8468 • LUXEMBOURG: +352-49 11 33 1 • MALAYSIA: +603-264 9988 • MEXICO: +52-5-258-6100 • THE NETHERLANDS: +00-31-33-45 15 000 • NEW ZEALAND: +64-4-499-2344 • NORWAY: +47 23 36 96 00 PEOPLE'S REPUBLIC OF CHINA: BEIJING: +86-10-6803-5588; CHENGDU: +86-28-619-9333; GUANGZHOU: +86-20-8755-5900; SHANGHAI: +86-21-6466-1228; HONG KONG: +852-2202-6688 • POLAND: +48-22-8747800 • PORTUGAL: +351-21-4134000 • RUSSIA: +7-502-935-8411 SINGAPORE: +65 438-1888 • SLOVAK REPUBLIC: +421-7-4342 94 85 • SOUTH AFRICA: +2711-805-4305 • SPAIN: +34-91-596-9900 • SWEDEN: +46-8-631-10-00 • SWITZERLAND: GERMAN: 41-1-908-90-00; FRENCH: 41-22-999-0444 • TAIWAN: +886-2-2514-0567 • THAILAND: +662-636-1555 TURKEY: +90-212-335-22-00 • UNITED ARAB EMIRATES: +9714 3366333 • UNITED KINGDOM: +44-1-276-20444 • UNITED STATES: +1-800-555-9SUN OR +1-650-960-1300 • VENEZUELA: +58-2-905-3800 • WORLDWIDE HEADQUARTERS: +1-800-555-9SUN OR +1-650-960-1300

SUN SERVERS

Family Comparison Chart

Servers

- Entry-Level Servers
- Midframe & Midrange Servers
- High-End Servers
- Server Appliances
- NEBS-Certified Servers

Servers Related:

- Server Comparison
- Success Stories
- Solutions
- Documentation
- White Papers
- Support & Service
- Server Upgrades
- Awards & Reviews

See Also:

- Storage
- Sun BluePrints
- Press Releases

Sun Fire 12K and 15K Servers
Enhanced performance and manageability
» More

Product Specifications	Sun Fire V1280	Sun Fire 3800	Sun Fire 4800	Sun Fire 6800	Sun Fire 12K	Sun Fire 15K
CPUs	4-12	2-8	2-12	2-24	Up to 52	Up to 106
Processor			UltraSPARC III			
Clock speed	900 MHz		900 Mhz, 1.05 GHz or 1.2 GHz			
Uniboard CPU/Memory Boards	N/A	1 or 2	Up to 3	Up to 6	Up to 9	Up to 18
I/O Slots (cPCI/PCI)	6 cPCI	12 cPCI	16 PCI or 8 hot-swappable cPCI	32 PCI or 16 hot-swappable cPCI	36 PCI	72 PCI
Maximum Memory per domain	96 GB	64 GB	96 GB	192 GB	288 GB	576 GB
Maximum Storage (all Sun Fire data center servers support external storage)	17.5 TB	35 TB	35 TB	77 TB	120 TB	250 TB
Sustained System Bandwidth			9.6 GB/sec		21.6 GB/sec	43.2 GB/sec
Hot Swap	CPU, Memory, Power Supplies, Disks	CPU, Memory, Uniboard CPU/Memory Boards, Compact PCI cards (3800-6800), Power Supplies, Fans. In addition, the Sun Fire 12K/15K supports hot-swap PCI cards and MaxCPU Boards.				
Common Components	CPU, Memory, System Controller, Fireplane Switch	CPU, Memory, Uniboard CPU/Memory Boards, Compact PCI card (3800-6800), PCI (4800-15K), System Controller (4800-6800), Fireplane Switch (4800-6800), I/O Assemblies (4800-6800)CPU, Memory, Uniboard CPU/Memory Boards, Compact PCI card (3800-6800), PCI (4800-15K), System Controller (4800-6800), Fireplane Switch (4800-6800), I/O Assemblies (4800-6800)				
Redundant	Power Supplies		Full Hardware Redundancy			

Redundant Components	Power Supplies, Sun Fireplane, Switches, Power Cords, Data Memory Paths	Full Hardware Redundancy			
Availability Features	Dynamic Reconfiguration of CPU/Memory boards, hot CPU upgrades, redundant Sun Fireplane Interconnect, redundant network connections, hot swap disks, smart fans, 2N redundant hot swap power supplies, hardened Operating System Kernel, hardened I/O drivers, systems configuration card, proactive self diagnostics, end-to-end data integrity, including ECC, and cluster support.	Full hardware redundancy, Dynamic System Domains, Dynamic reconfiguration, Hot CPU Upgrades, online upgrades, concurrent maintenance, end-to- end ECC protection, redundant network connections, redundant storage connections, kernel hot patching, hardened operating system kernel, live operating system upgrades, journaling file system, hardened I/O drivers, and cluster support		Full hardware redundancy; Hot CPU Upgrades; Online upgrades; Journaling file system; Concurrent maintenance; Full data integrity; Redundant network connections; Redundant storage connections; Hardened operating system kernel; Hardened I/O drivers
Domains	N/A	Up to 2 fault-isolated Dynamic System Domains	Up to 4 fault-isolated Dynamic Sytem Domains	Up to 9 fault-isolated Dynamic System Domains	Up to 18 fault-isolated Dynamic System Domains
Operating Environment	Solaris 8 02/02 Operating Environment (or later)	Solaris 8 4/01 Operating Environment (or later)		Solaris 8 10/01 Operating Environment (or later)	
System Management	Sun Management Center 3.0 software, Solaris Management Console	Sun Management Center 3.0 software			

Warranty	1 year, on-Site H/W Service (8am-5pm, M-F), next business day Hardware Response Time, Telephone Support (8am-5pm, M-F)	1 year, on-Site H/W Service (8am-5pm, M-F), 4-Hr Hardware Response Time, Telephone Support (8am-8pm, M-F)	1 year, on-Site H/W Service (24x7x365), 4-Hr Hardware Response Time, Telephone Support (24x7x365)	1 year, on-Site H/W Service (24x7x365); 4-hr Hardware Response Time; Telephone Support (24x7x365); Software Warranty: 90 Days (material defects only)	
Installation	N/A	Serverstart Installation includes up to two (2) domains.		ServerStart installation includes up to 9 domains	ServerStart installation includes up to 18 domains

1. This page meets my need. disagree ○ ○ ○ ○ ○ ○ agree

2. This page was easy to find. disagree ○ ○ ○ ○ ○ ○ agree

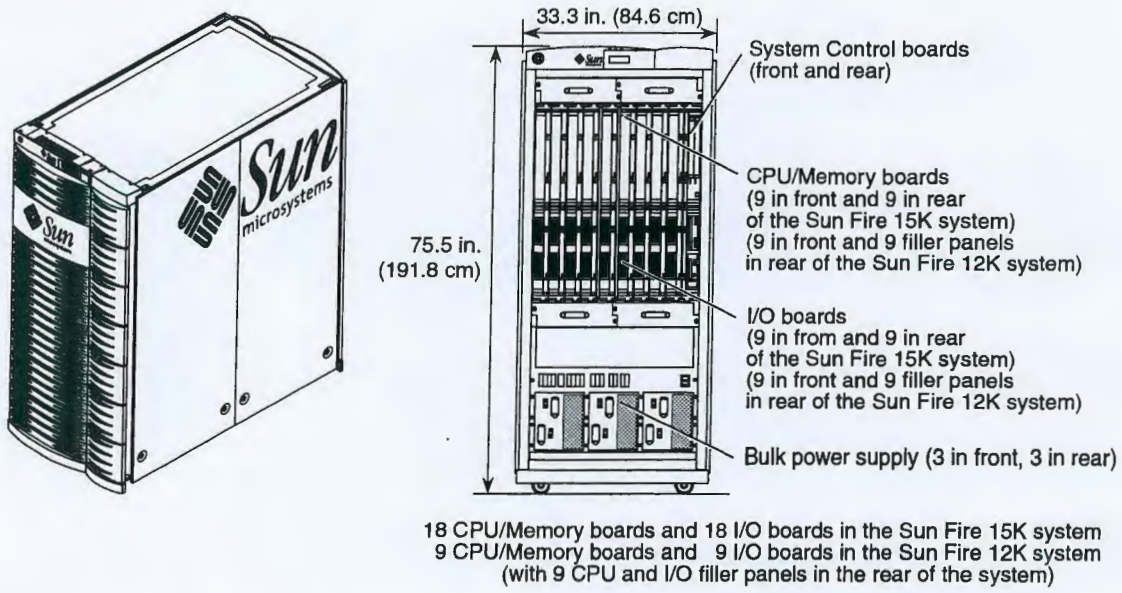


FIGURE 1-1 Sun Fire 15K/12K Systems

The Sun Fire 15K/12K systems are essentially the same. The Sun Fire 15K system has the capacity for 18 CPU/Memory boards and 18 I/O boards. The Sun Fire 12K system has the capacity for nine CPU/Memory boards and nine I/O boards. Each system contains two System Control boards (one main and one spare).

1.1 System Boards

1.1.1 CPU/Memory Boards

The CPU/Memory board holds four CPUs. Each CPU has an associated memory subsystem of eight DIMMs, so memory bandwidth and capacity are both scaled up as CPUs are added. The memory capacity of the board is 32 Gbytes using a 1-Gbyte DIMM. The maximum memory bandwidth inside a board is 9.6 Gbytes per second. The CPU/Memory board has a 4.8 Gbyte per second connection to the rest of the system.

1.1.2 I/O Boards

The common Sun Fire 15K/12K systems hot-swap PCI assembly architecture has two I/O controllers. Each controller provides one 66/33-MHz PCI (peripheral component interconnect) bus and one 33-MHz PCI bus for a total of two of each speed on the I/O board. Therefore, each I/O assembly has four hot-swap component PCI slots. A Sun Fire I/O board has a 2.4 Gbyte per second connection to the rest of the system.

1.1.3 System Controller

The system controller is the heart of the Sun Fire 15K/12K systems availability and serviceability technology. It configures the system, coordinates the boot process, sets up the dynamic system domains, monitors the system environmental sensors, and handles error detection, diagnosis, and recovery. Two System Control boards are configured into the system to provide redundancy and automatic failover in the event that one board fails.

1.1.4 Peripherals

The Sun Fire 15K/12K systems cabinet does not have room for peripherals, with the exception of the system controller peripherals (DVD-ROM, digital audio tape (DAT) drive, and hard drive). However, more peripheral devices can be configured in additional peripheral expansion racks.

Doc Ac

12964
E

System Architecture

SMS architecture is best described as distributed client-server. `init`(1M) starts (and restarts as necessary) one process: `ssd`(1M). `ssd` is responsible for monitoring all other SMS processes and restarting them as necessary. See FIGURE 3-1.

The Sun Fire 15K/12K platform, the SC, and other workstations communicate over Ethernet. You perform SMS operations by entering commands on the SC console after remotely logging in to the SC from another workstation on the local area network. You must log in as a user with the appropriate platform or domain privileges if you want to perform SMS operations (such as monitoring and controlling the platform).

Note – If SMS is stopped on the main SC and the other SC is powered off, the domains gracefully shutdown and the platform is powered down. If the remaining SC is simply powered off without a shutdown of SMS, SMS won't have time to power off the platform and the domains will crash.

Dual system controllers are supported within the Sun Fire 15K/12K platform. One SC is designated as the primary or main system controller, and the other is designated as the spare system controller. If the main SC fails, the failover capability automatically switches to the spare SC as described in "SC Failover" on page 155.

Most domain configurable units are active components and you need to check the system state before powering off any DCU.

Note – Circuit breakers must be on whenever a board is present, including expander boards, whether or not the board is powered on.

For details, see "Power Control" on page 128.

SMS Administration Environment

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0152
3696
Doc:

Administration tasks on the Sun Fire 15K/12K system are secured by group privilege requirements. Upon installation, SMS installs the following 39 UNIX groups to the `/etc/group` file.

- `platadmn` - Platform administrator
- `platoper` - Platform operator

0152

- `platsvc` - Platform service
- `dmn[`*A...R*`]admn` - domain [*domain_id* | *domain_tag*] administrator (18)
- `dmn[`*A...R*`]rcfg` - domain [*domain_id* | *domain_tag*] configurator (18)

`smsconfig`(1M) allows an administrator to add, remove, and list members of platform and domain groups as well as set platform and domain directory privileges using the `-a`, `-r`, and `-l` options.

`smsconfig` also can configure SMS to use alternate group names including NIS managed groups using the `-g` option. Group information entries can come from any of the sources for groups specified in the `/etc/nsswitch.conf` file (refer to `nsswitch.conf`(4)). For instance, if domain A was known by its domain tag as the "Production Domain," an administrator could create a NIS group with the same name and configure SMS to use this group as the domain A administrator group instead of the default, `dmnaadmn`. For more information, refer to the *System Management Services (SMS) 1.3 Installation Guide*, "Administration Privileges" on page 15, and refer to the `smsconfig` man page.

Network Connections for Administrators

The nature of the Sun Fire 15K/12K physical architecture, with an embedded system controller, as well as the supported administrative model (with multiple administrative privileges, and hence multiple administrators) dictates that an administrator utilize a remote network connection from a workstation to access SMS command interfaces to manage the Sun Fire 15K/12K system.

Caution – Shutting down a remote workstation while a tip session is active into a Sun Fire 15K/12K SC will bring both SCs down to the OpenBoot OK prompt. This will not affect the domains and after powering the remote system back on you can restore the SCs by typing go at the OK prompt; however, you should end all tip sessions before shutting down a remote workstation.

Since the administrators provide information to verify their identity (passwords) and might possibly need to display sensitive data, it is important that the remote network connection be secure. Physical separation of the administrative networks provides some security on the Sun Fire 15K/12K system. Multiple external physical network connections are available on each SC. SMS software supports up to two external network communities.

For more information on Sun Fire 15K/12K networks, see "Management Network Services" on page 141. For more information on securing the Sun Fire 15K/12K system see "Security Options" on page 14.

CHAPTER 2

Dynamic System Domains

The Sun Fire 15K/12K systems contain dynamic domains. These domains are described in the following sections.

The Sun Fire 15K system can be dynamically subdivided into as many as 18 dynamic system domains. The Sun Fire 12K system can be subdivided into as many as 9 dynamic system domains. Each domain has a separate boot disk (to execute a specific instance of the Solaris operating environment) as well as separate disk storage, network interfaces, and I/O interfaces. CPU boards and I/O boards can be separately added and removed from running domains.

Domains are used for server consolidation to run separate parts of a solution, such as an application server, a web server, and a database server. The domains are hardware-protected from hardware or software faults in other domains.

2.1 Domain Configurability

Each of the system boards (slot 0 and slot 1 boards) can be independently added to, or removed from, a running domain. This enables CPU and memory resources to be moved from one domain to another without disturbing the disk storage and network connections. In the Sun Fire 15K system, each domain must have an I/O board; therefore, there is a maximum of 18 domains. In the Sun Fire 12K system, each domain must have an I/O board; therefore, there is a maximum of 9 domains.

2.2 Domain Protection

Primary domain protection is accomplished in the address extender queue (AXQ) ASICs by checking each transaction for domain validity when a transaction is first detected. In the Sun Fire 15K system, the system data interface (SDI) chips can also screen data transfer requests for valid destinations (to as many as 36 system boards). In addition, each Sun Fireplane interconnect arbiter (data, address, response) screens requests to as many as 18 expanders. In the Sun Fire 12K system, the SDI chips can screen data transfer requests for valid destinations (to as many as 18 system boards). Each Sun Fireplane interconnect arbiter (data, address, response) screens requests to as many as 9 expanders.This is a double check on the other domain protection mechanisms, which are in the AXQ and the SDI chips.

If a transgression error is detected in the AXQ, the AXQ treats the error operation like a request to nonexistent memory. It reissues the request without asserting a mapped coherency protocol signal, causing a Solaris operating environment switch execution from one process to another. A transgression error in the Sun Fireplane interconnect causes a domainstop of the transgressing domains because this error must indicate a failure of the primary protection mechanism.

2.3 Domain Fault Isolation

Domains are protected against software or hardware faults in other domains. If there is a fault in the processor or memory hardware that is assigned to a particular domain, only that one domain will be affected. If there is a fault in hardware that is shared between multiple domains, only those domains that share the hardware are affected.

As an example of hardware shared between two domains, consider a system which is configured to have a CPU/Memory board in one domain and its associated I/O board in another domain. The logic on a split expander board is shared between those two domains. A fault in a split expander or its control wiring to the Sun Fireplane interconnect causes a failure only in those two domains. A fault in globally shared hardware, such as the system clock generator or Sun Fireplane interconnect chips, causes a failure in all domains.

Fatal errors, such as a parity error in control wiring or a faulty ASIC, causes a *domainstop*. The steering signals from the expander boards to the arbiter chips of the Sun Fireplane interconnect are parity protected. If there is a parity error, the multiple copies of the Sun Fireplane interconnect arbiter could get out of sync. Therefore, this type of parity error causes an immediate *domainstop* of the domain.

1.4 Dynamic System Domains

Each domain in the Sun Fire 15K/12K systems include one or more CPU/Memory boards and one or more I/O boards. Each domain runs its own instance of the Solaris operating environment and has its own peripherals and network connections. Domains can be reconfigured without interrupting the operation of other domains. Domains can be used for:

- Testing new applications
- Making operating system updates
- Supporting various departments
- Removing and reinstalling boards for repair or upgrade

As an example, the Sun Fire 15K system is divided into three domains. Here is one example of partitioning a fully populated system into three domains to handle three types of functions:

- Domain 1 is set up to run online transaction processing (OLTP). It is a 32-CPU domain containing eight boards of four CPUs each.
- Domain 2 is set up to run decision support software (DSS). It is also a 32-CPU domain containing eight boards of four CPUs each.
- Domain 3 is set up as a domain for developers. It is a two-board domain, each board with four CPUs.

Boards can be automatically migrated between domains as the load change demands.

The Sun Fire 15K system can have up to 18 domains. The Sun Fire 12K system can have up to 9 domains. Domains are isolated from each other by the interconnect application-specific integrated circuits (ASICs).

Doc 7

12959

System Architecture

SMS architecture is best described as distributed client-server. `init`(1M) starts (and restarts as necessary) one process: `ssd`(1M). `ssd` is responsible for monitoring all other SMS processes and restarting them as necessary. See FIGURE 3-1.

The Sun Fire 15K/12K platform, the SC, and other workstations communicate over Ethernet. You perform SMS operations by entering commands on the SC console after remotely logging in to the SC from another workstation on the local area network. You must log in as a user with the appropriate platform or domain privileges if you want to perform SMS operations (such as monitoring and controlling the platform).

Note – If SMS is stopped on the main SC and the other SC is powered off, the domains gracefully shutdown and the platform is powered down. If the remaining SC is simply powered off without a shutdown of SMS, SMS won't have time to power off the platform and the domains will crash.

Dual system controllers are supported within the Sun Fire 15K/12K platform. One SC is designated as the primary or main system controller, and the other is designated as the spare system controller. If the main SC fails, the failover capability automatically switches to the spare SC as described in "SC Failover" on page 155.

Most domain configurable units are active components and you need to check the system state before powering off any DCU.

Note – Circuit breakers must be on whenever a board is present, including expander boards, whether or not the board is powered on.

For details, see "Power Control" on page 128.

SMS Administration Environment

Administration tasks on the Sun Fire 15K/12K system are secured by group privilege requirements. Upon installation, SMS installs the following 39 UNIX groups to the `/etc/group` file.

- `platadmn` - Platform administrator
- `platoper` - Platform operator

- `platsvc` - Platform service
- `dmn`[*A...R*]`admn` - domain [*domain_id* | *domain_tag*] administrator (18)
- `dmn`[*A...R*]`rcfg` - domain [*domain_id* | *domain_tag*] configurator (18)

`smsconfig`(1M) allows an administrator to add, remove, and list members of platform and domain groups as well as set platform and domain directory privileges using the `-a`, `-r`, and `-l` options.

`smsconfig` also can configure SMS to use alternate group names including NIS managed groups using the `-g` option. Group information entries can come from any of the sources for groups specified in the `/etc/nsswitch.conf` file (refer to `nsswitch.conf`(4)). For instance, if domain A was known by its domain tag as the "Production Domain," an administrator could create a NIS group with the same name and configure SMS to use this group as the domain A administrator group instead of the default, `dmnaadmn`. For more information, refer to the *System Management Services (SMS) 1.3 Installation Guide*, "Administration Privileges" on page 15, and refer to the `smsconfig` man page.

Network Connections for Administrators

The nature of the Sun Fire 15K/12K physical architecture, with an embedded system controller, as well as the supported administrative model (with multiple administrative privileges, and hence multiple administrators) dictates that an administrator utilize a remote network connection from a workstation to access SMS command interfaces to manage the Sun Fire 15K/12K system.

Caution – Shutting down a remote workstation while a tip session is active into a Sun Fire 15K/12K SC will bring both SCs down to the OpenBoot OK prompt. This will not affect the domains and after powering the remote system back on you can restore the SCs by typing go at the OK prompt; however, you should end all tip sessions before shutting down a remote workstation.

Since the administrators provide information to verify their identity (passwords) and might possibly need to display sensitive data, it is important that the remote network connection be secure. Physical separation of the administrative networks provides some security on the Sun Fire 15K/12K system. Multiple external physical network connections are available on each SC. SMS software supports up to two external network communities.

For more information on Sun Fire 15K/12K networks, see "Management Network Services" on page 141. For more information on securing the Sun Fire 15K/12K system see "Security Options" on page 14.

ultimate net worker

Sun Fire™ V480 Server

THE AFFORDABLE, RACK-OPTIMIZED SERVER THAT OFFERS EXCEPTIONAL PROCESSING POWER IN A COMPACT FOOTPRINT.

SUN FIRE™ V480 SERVER

The Sun Fire™ V480 server is designed to deliver compute density and enterprise-class RAS features at an affordable price. Its space-efficient, rack-optimized 5RU, 24-inch-depth enclosure provides excellent value per rack unit and contains up to four 900-MHz UltraSPARC® III Cu processors, each with 8 MB e-cache (L2), up to 32 GB of memory, integrated dual 10/100/1000-Mb/sec. Ethernet, and the Sun Fireplane Interconnect operating at 9.6 GB/sec. The Sun Fire V480 server features N+1 power supplies with separate power cords, so a fully configured system can run on one power supply; the second power supply is for redundancy purposes. In addition, hot-plug disks and hot-swap power supplies enable online maintenance and repair to further enhance system availability. Outstanding scalability, performance, and enterprise class RAS features make the Sun Fire V480 server an excellent Web, e-commerce, or EDA server. Remote System Control (RSC) reduces overall system management costs by providing monitoring and control from remote locations via Ethernet, serial, and modem connections.

SPECIFICATIONS

PROCESSOR OPTIONS

Processor	900-MHz UltraSPARC® III Cu
Architecture	Superscalar SPARC 9
Processor modules	One or two dual-processor/memory modules
Cache (on chip)	64-KB data and 32-KB instruction
Secondary (L2)	8-MB external

MAIN MEMORY

A system maximum of 32 GB when configured with four processors

STANDARD/INTEGRATED INTERFACES

Network	Two 10/100/1000-Mb/sec. Ethernet
I/O	FC-AL disk controller, two USB ports
Serial	RJ45 serial port
Expansion capability	Six PCI slots compliant with PCI specification Revision 2.1: two at 66 MHz, 64 bits wide, 3.3 volts; four at 33 MHz, 64 bits wide, 5 volts

MASS STORAGE AND MEDIA

Host adapters	Internal IDE to support the internal DVD
Internal disk	Two 3.5-in. X 1.0-in. 10,000 RPM FC-AL disks, 36-GB (73-GB drives are also supported)
External disk	Sun StorEdge™ MultiPack systems Sun StorEdge A1000 Sun StorEdge D1000 Sun StorEdge A3500 Sun StorEdge A5100/A5200 Sun StorEdge T3 Sun StorEdge D2 Sun StorEdge S1 Sun StorEdge 3900/6900 Sun StorEdge 9900
External tape systems	SCSI tape devices via a SCSI host bus adapter: Sun StorEdge 12-GB DDS-3 UniPack Sun StorEdge DDS-3 FlexiPack Sun StorEdge DDS-3 Autoloader FlexiPack Sun StorEdge 20-GB DDS-4 UniPack Sun StorEdge DLT8000 FlexiPack Sun StorEdge L9 tape autoloader Sun StorEdge L20 tape library family Sun StorEdge L180 tape library Sun StorEdge L700 tape library (Utilization of the Sun StorEdge L180 and L700 tape libraries may be limited by the number of SCSI host bus adapters and buses available for connection to the server.)

SOFTWARE

Operating system	Solaris™ 8 2/02 or later
Languages	C, C++, FORTRAN, Java
Networking	ONC, NFS, TCP/IP, SunLink™ OSI, MHS, IPX/SPX
System and network management	Sun™ Management Center, Sun Remote System Control, Sun Cluster, Solaris PC Netlink, Solaris Management Console, Solstice JumpStart™, Solaris WebStart, Solaris Web Start Wizards, Solstice AdminSuite™, Solstice DiskSuite™, Solstice Backup™, and other Solstice™ products

CONSOLE OPTIONS

Monitor	Optional, Sun monitors from 1995 onward (17-, FP18-, 19-, 20-, 21-, and 24-inch)
Frame buffer	Sun PGX64 8/24-bit
Keyboard and mouse	USB keyboard and mouse
PCI I/O options	Gigabit Ethernet, 10/100-Mb/sec. Ethernet, FC-AL, Quad FastEthernet, token ring, FDDI, ATM-155, ATM-622, high-speed serial, Ultra™ SCSI with 10/100-Mb/sec. Ethernet, dual-channel single-ended Ultra SCSI, dual-channel differential Ultra SCSI

POWER SUPPLIES

One required, two for redundancy, each with independent power cord

Maximum AC input	1440 W per power supply
Maximum DC output	1184 W per power supply

ENVIRONMENT

AC power	100–240 VAC, 47–63 HZ, 0.895 KVA
Operating	5° C to 35° C (41° F to 95° F) 20% to 80% relative temperature humidity, noncondensing, 27° C maximum wet bulb
Nonoperating	-20° C to 60° C (-4° F to 140° F) 5% to 95% relative temperature humidity, noncondensing

REGULATIONS

Meets or exceeds the following requirements:

Safety	UL 1950, CB Scheme IEC 950 (CE mark), CSA C22.2 950 (from UL), TUV EN 60950
RFI/EMI	Class A: Australia/New Zealand AS/NZ 3548, Industry Canada ICES-003, European Community EN55022/CISPR22, Japan VCCI, Taiwan CNS 13438, and US FCC 47CFR15.B
Immunity	EN55024, EN61000-4-2, EN61000-4-3, EN61000-4-4, EN61000-4-5, EN61000-4-6, EN61000-4-8, EN61000-4-11, IEC 61000-3-2, and IEC 61000-3-3
X-ray	U.S. DHHS 21CFR Subchapter J, PTB German X-ray Decree

DIMENSIONS AND WEIGHT

Height	5U, 222 mm (8.75 in.)
Width	446 mm (17.5 in.)
Depth	610 mm (24.0 in.)
Weight	35.8 kg (79 lb.) (minimum) 44 kg (97 lb.) (fully configured)
Rack	Fits into a standard 19-inch-wide rack mount kit that complies with EIA-310-D-1992 standard, or a 72-inch height Sun StorEdge rack, which will support seven Sun Fire V480 servers.

UPGRADES

Upgrades are available for SPARC® server and Sun Enterprise™ systems. Contact your local Sun sales representative for details.

WARRANTY

Hardware support	3 years
Software install	90 days
Call response	8 hours
Delivery	Second business day, on-site

Sun Fire 280R

Sun Fire V480

Sun Fire V880

HEADQUARTERS SUN MICROSYSTEMS, INC., 901 SAN ANTONIO ROAD, PALO ALTO, CA 94303-4900 USA

PHONE: 650 960-1300 or 800-555-9SUN INTERNET: www.sun.com

Sun microsystems

take it to the n[th]

SALES OFFICES

AFRICA (NORTH, WEST AND CENTRAL): +9714-3366333 • ARGENTINA: +5411-4317-5600 • AUSTRALIA: +61-2-9844-5000 • AUSTRIA: +43-1-60563-0 • BELGIUM: +32-2-704-8000 • BRAZIL: +55-11-5187-2100 • CANADA: +905-477-6745 • CHILE: +56-2-3724500 • COLOMBIA: +571-629-2323 • COMMONWEALTH OF INDEPENDENT STATES: +7-502-935-8411 CZECH REPUBLIC: +420-2-3300-9311 • DENMARK: +45 4556 5000 • EGYPT +202-570-9442 • ESTONIA: +372-6-308-900 • FINLAND: +358-9-525-561 • FRANCE: +33-134-03-00-00 • GERMANY: +49-89-46008-0 • GREECE: +30-1-618-8111 • HUNGARY: +36-1-489-8900 • ICELAND: +354-563-3010 • INDIA: BANGALORE: +91-80-2298989/2295454; NEW DELHI: +91-11-6106000; MUMBAI: +91-22-2018141 • IRELAND: +353-1-8055-666 • ISRAEL: +972-9-9710500 • ITALY: +39-039-60551 • JAPAN: +81-3-5717-5000 • KAZAKHSTAN: +7-3272-466774 • KOREA: +822-2193-5114 LATVIA: +371-750-3700 • LITHUANIA: +370-729-8468 • LUXEMBOURG: +352-49 11 33 1 • MALAYSIA: +603-21161888 MEXICO: +52-5-258-6100 • THE NETHERLANDS:+00-31-33-45-15-000 • NEW ZEALAND: AUCKLAND: +64-9-976-6800; WELLINGTON: +64-4-462-0780 • NORWAY: +47 23 36 96 00 • PEOPLE'S REPUBLIC OF CHINA: BEIJING: +86-10-6803-5588; CHENGDU: +86-28-619-9333; GUANGZHOU: +86-20-8755-5900; SHANGHAI: +86-21-6466-1228; HONG KONG: +852-2202-6688 • POLAND: +48-22-8747800 • PORTUGAL:+351-21-4134000 • RUSSIA: +7-502-935-8411 • SINGAPORE: +65-438-1888 • SLOVAK REPUBLIC: +421-2-4342-94-85 • SOUTH AFRICA: +2711-805-4305 • SPAIN: +34-91-596-9900 • SWEDEN: +46-8-631-10-00 • SWITZERLAND: GERMAN: 41-1-908-90-00; FRENCH: 41-22-999-0444 • TAIWAN: +886-2-8732-9933 • THAILAND: +662-344-6888 • TURKEY: +90-212-335-22-00 • UNITED ARAB EMIRATES: +9714-3366333 • UNITED KINGDOM: +44-1-276-20444 • UNITED STATES: +1-800-555-9SUN OR +1-650-960-1300 • VENEZUELA: +58-2-905-3800 • OR ONLINE AT SUN.COM/STORE

05/02

Doc 8a

Sun™ Rack 900

Highly flexible rack mount system.

Key feature highlights

Easily personalized for your particular needs, with numerous building blocks and upgrade options.

Base building block options including a newly designed power distribution system using zero rack units, a locking front door, cable management, and rack mount kits to accommodate current and future Sun products with an industry-standard 19-inch width.

Accommodates Sun servers, storage, and qualified third-party products.

Zero rack unit power distribution system allows sophisticated power management without taking up valuable product space.

Vertical Cable Management Bracket contributes to increased security and better resource management.

Enjoy more options in your resource deployment.

With constantly changing data center space and resource requirements, information technology (IT) managers need greater flexibility in deploying their resources. Designed with a building block approach that maximizes resource allocation opportunities, the Sun™ Rack 900 provides a wide variety of options. Offering greater space utilization, flexibility, and manageability, the Sun Rack 900 can be incorporated into a full spectrum of environments – from the largest data centers to small deployment situations.

Building blocks for flexibility.

The Sun Rack 900 offers the flexibility of a building-block approach to maximize resource allocation opportunities, with three power options to meet your specific needs. If your data center is already fitted to provide power to the rack, you can order the rack without power. The second option is the newly designed Power Distribution System (PDS), which consists of two independently powered sequencers and two power outlet strips each with 24 outlets (48 total). The Sun Rack 900 PDS does not use any RUs of valuable product

Sun™ Rack 900 System Specifications

space, and you have use of the total 38 RUs for your current and future Sun servers and storage systems, as well as qualified third-party products.

For supported products, please see http://sun.com/servers/rack

Sun Rack 900 Dimensions

Height: 74 in	188 cm
Width: 23.5 in	59.7 cm
Depth: 35.4 in	90 cm
Weight: 360 pounds	163.3 kg
Usable rack units: 38	

Operating Range	Power Distribution System (PDS)
Nominal Voltage	200, 208, 220, 230, or 240 VAC
Operating Voltage	Single Phase 180-240 VAC
Frequency	47-63 Hz
Current	32A (2X 16A) maximum 2N Redundant Systems 64A (4X-16A) maximum Non-Redundant Systems* N+1 Redundant Systems*
AC Power Plug	NEMA L6-20P Domestic IEC 309 16A 3 Position International
AC Power Receptacle	NEMA L6-20R Domestic IEC 309 16A 3 Position International
Power Cords Required	4

* These configurations will not survive the loss of an AC input unless systems are redundant.

Base Sun Rack 900 cabinet includes:

- Rear door, locking
- Frame with casters
- RETMA rails, M6 thread
- Top panel
- Side panels (2)
- Anti-tilt bar assembly
- Power strip bracket and cabling
- Vertical cable management bracket
- Sequencer box bracket (2)
- Ship kit

The front and rear doors of the cabinet give data center technicians immediate access to products, and cable management arms keep cables organized for easy tracing.

For more information on the Sun Rack 900 rack mount system, please go to www.sun.com/servers/rack

Sun Microsystems, Inc. 901 San Antonio Road, Palo Alto, CA 94303-4900 USA **Phone** 800 786-7638 or +1 512 434-1577 **Web** sun.com

Sun microsystems
We make the net work.

0162

STORAGE MANAGEMENT SOFTWARE

VERITAS File System

VERITAS File System

» In the Spotlight

Storage Related:

» White Papers
» Success Stories
» Press Releases

Print

VERITAS File System software is a powerful, quick-recovery journaling file system that is designed to provide high performance and easy management for mission-critical applications. The software augments UNIX® file management with high availability, data throughput, and up-to-date structural integrity.

Contact Me | Get the Software

VERITAS File System is a high-performance, quick-recovery, journaling file system. It helps provide the performance and manageability mission-critical applications require. VxFS provides scalable performance and capacity to meet the demands of increased user loads and client/server environments.

Highlights

Key Applications:
VERITAS File System 3.2 (VxFS) software augments UNIX® file management and provides scalable performance and capacity to meet the demands of increased user loads and client/server environments.

Key Specifications:
VERITAS File System has online management capabilities, such as defragmentation and flexible file system sizes. The software helps enable online backups and fast recovery times: The journaling file system means no file system checks are required.

Key Benefits:
Is designed to provide fast recoverability, high availability, high performance and scalability. Centralized management in heterogeneous environments.

Key Related Hardware:
- Sun StorEdge A5200
- Sun StorEdge T3 Array for the Enterprise
- Sun StorEdge T3 Array for the Workgroup

Key Industries:
VxFS is suitable for virtually any mission-critical site that needs high availability, robust data access, and fast recovery.

Requirements:

- Solaris 2.6, 7, or 8 Operating Environments.

1. This page meets my need. disagree ○ ○ ○ ○ ○ ○ ○ agree
2. This page was easy to find. disagree ○ ○ ○ ○ ○ ○ ○ agree

Doc 10

1295

```
#to mount          to fsck             point        type pass at boot options
#
fd                 -                   /dev/fd      fd   -    no      -
/proc              -                   /proc        proc -    no      -
/dev/dsk/c0t0d0s1  -                   -            swap -    no      -
/dev/dsk/c0t0d0s0  /dev/rdsk/c0t0d0s0  /            ufs  1    no      -
/dev/dsk/c0t0d0s6  /dev/rdsk/c0t0d0s6  /usr         ufs  1    no      -
/dev/dsk/c0t0d0s5  /dev/rdsk/c0t0d0s5  /datab       ufs  2    yes     -
/dev/dsk/c0t0d0s7  /dev/rdsk/c0t0d0s7  /export/home ufs  2    yes     -
swap               -                   /tmp         tmpfs -   yes     -
```

▼ How to Determine the Number of Tapes Needed for a Full Backup

1. **Become superuser or assume an equivalent role.**
2. **Estimate the size of the backup in bytes.**

   `# ufsdump S` *file-system*

   The `S` displays the estimated number of bytes that are needed to do the backup.
3. **Divide the estimated size by the capacity of the tape to see how many tapes you need.**

   For a list of tape capacities, see Table 46–5.

Example—Determining Number of Tapes

In this example, the file system of 489,472 bytes easily fits on a 150-Mbyte tape.

```
# ufsdump S /export/home
489472
```


Backing Up a File System

The following are general guidelines for performing backups:

- Use single-user mode or unmount the file system, unless you are creating a snapshot of a file system. For information about UFS snapshots, see Chapter 48.
- Be aware that the backing up of file systems when there are directory-level operations (such as creating, removing, and renaming files) and file-level activity occurring means that some data will not be included in the backup.
- You can run the `ufsdump` command from a single system and remotely back up groups of systems across the network through remote shell or remote login, and direct the output to the system on which the tape drive is located. (Typically, the

0165

tape drive is located on the system from which you run the `ufsdump` command, but it does not have to be.)

Another way to back up files to a remote drive is to pipe the output from the `ufsdump` command to the `dd` command. For information about using the `dd` command, see Chapter 51.

- If you are doing remote backups across the network, the system with the tape drive must have entries in its `/.rhosts` file for each client that will be using the drive. Also, the system that initiates the backup must be included in the `/.rhosts` file on each system that it will back up.
- To specify a remote tape device on a system, use the naming convention that matches the OS release of the system with the remote tape drive. For example, use the `/dev/rst0` device for a remote drive on a system that is running the SunOS 4.1.1 release or compatible versions. Use the `/dev/rmt/0` device for a system running the Solaris 9 release or compatible versions.

Note – Use the `nisbackup` command to back up a NIS+ master server. For information on using this command, see *System Administration Guide: Naming and Directory Services (FNS and NIS+)*.

▼ How to Backup a File System to Tape

The following steps provide the general steps for backing up file systems using the `ufsdump` command. The examples show specific uses of options and arguments.

1. **Become superuser or assume an equivalent role.**
2. **Bring the system to run level S (single-user mode).**

   ```
   # shutdown -g30 -y
   ```

3. **(Optional) Check the file system for consistency.**

   ```
   # fsck -m /dev/rdsk/device-name
   ```

   The `fsck -m` command checks for the consistency of file systems. For example, power failures can leave files in an inconsistent state. For more information on the `fsck` command, see Chapter 43.

4. **If you need to back up file systems to a remote tape drive:**

   a. **On the system to which the tape drive is attached (the tape server), add the following entry to its `/.rhosts` file.**

      host `root`

      The *host* entry specifies the name of the system on which you will run the `ufsdump` command to perform the backup.

Task	Description	Instructions
	Restore files interactively - Use this method when you are unsure of the file names because you can browse the media contents and select individual files and directories.	"How to Restore Files Interactively" on page 677
	Restore files non-interactively - Using this method is probably faster if you already know the few file names to be restored.	"How to Restore Specific Files Non-Interactively" on page 679
	Restore a file system – Use this method when you get a new disk drive or as part of a recovery procedure.	"How to Restore a Complete File System" on page 681
Restore the root (/) or /usr file systems	Restoring the root (/) or /usr file systems involves booting the system from a local CD or the network.	"How to Restore the root (/) and /usr File Systems" on page 684

Preparing to Restore Files and File Systems

The `ufsrestore` command copies files to disk, relative to the current working directory, from backups that were created by using the `ufsdump` command. You can use the `ufsrestore` command to reload an entire file system hierarchy from a level 0 dump and incremental dumps that follow it or to restore one or more single files from any backup tape. If the `ufsrestore` command is run as superuser, files are restored with their original owner, last modification time, and mode (permissions).

Before you start to restore files or file systems, you need to know the following:

- The tapes (or diskettes) you need
- The raw device name on which you want to restore the file system
- The type of tape device you will use
- The device name (local or remote) for the tape drive

Determining the File System Name

If you have properly labeled your backup tapes, you should be able to use the file system name (`/dev/rdsk/`*device-name*) from the tape label. For more information, see "How to Find File System Names" on page 656.

Determining the Type of Tape Device You Need

You must use a tape device that is compatible with the backup media to restore the files. The format of the backup media determines which drive you must use to restore files. For example, if your backup media is 8-mm tape, you must use an 8-mm tape drive to restore the files.

Determining the Tape Device Name

You might have specified the tape device name (`/dev/rmt/`*n*) as part of the backup tape label information. If you are using the same drive to restore a backup tape, you can use the device name from the label. For more information on media devices and device names, see Chapter 52.

Restoring Files and File Systems

When you back up files and directories, you save them relative to the file system in which they belong. When you restore files and directories, the `ufsrestore` command re-creates the file hierarchy in the current working directory.

For example, files backed up from the `/export/doc/books` directory (where `/export` is the file system), are saved relative to `/export`. In other words, the `book1` file in the `books` directory is saved as `./doc/books/book1` on the tape. Later on, if you restored the `./doc/books/book1` file to the `/var/tmp` directory, the file would be restored to `/var/tmp/doc/books/book1`.

When you restore individual files and directories, it is a good idea to restore them to a temporary location, such as the `/var/tmp` directory. After you verify them, you can move the files to their proper locations. You can restore individual files and directories to their original locations. If you do so, be sure you are not overwriting newer files with older versions from the backup tape.

To avoid conflicts with other users, you might want to create and change to a subdirectory, such as the`/var/tmp/restore` file, in which to restore the files.

If you are restoring a hierarchy, you should restore the files in a temporary directory on the same file system where the files will reside. So, you can use the `mv` command to move the entire hierarchy where it belongs after it is restored.

SUN FIRE™ V480 SERVER

The Sun Fire™ V480 server is designed to deliver compute density and enterprise-class RAS features at an affordable price. Its space-efficient, rack-optimized 5RU, 24-inch-depth enclosure provides excellent value per rack unit and contains up to four 900-MHz UltraSPARC® III Cu processors, each with 8 MB e-cache (L2), up to 32 GB of memory, integrated dual 10/100/1000-Mb/sec. Ethernet, and the Sun Fireplane Interconnect operating at 9.6 GB/sec. The Sun Fire V480 server features N+1 power supplies with separate power cords, so a fully configured system can run on one power supply; the second power supply is for redundancy purposes. In addition, hot-plug disks and hot-swap power supplies enable online maintenance and repair to further enhance system availability. Outstanding scalability, performance, and enterprise class RAS features make the Sun Fire V480 server an excellent Web, e-commerce, or EDA server. Remote System Control (RSC) reduces overall system management costs by providing monitoring and control from remote locations via Ethernet, serial, and modem connections.

SPECIFICATIONS

PROCESSOR OPTIONS

Processor	900-MHz UltraSPARC® III Cu
Architecture	Superscalar SPARC 9
Processor modules	One or two dual-processor/memory modules
Cache (on chip)	64-KB data and 32-KB instruction
Secondary (L2)	8-MB external

MAIN MEMORY

A system maximum of 32 GB when configured with four processors

STANDARD/INTEGRATED INTERFACES

Network	Two 10/100/1000-Mb/sec. Ethernet
I/O	FC-AL disk controller, two USB ports
Serial	RJ45 serial port
Expansion capability	Six PCI slots compliant with PCI specification Revision 2.1: two at 66 MHz, 64 bits wide, 3.3 volts; four at 33 MHz, 64 bits wide, 5 volts

MASS STORAGE AND MEDIA

Host adapters	Internal IDE to support the internal DVD
Internal disk	Two 3.5-in. X 1.0-in. 10,000 RPM FC-AL disks, 36-GB (73-GB drives are also supported)
External disk	Sun StorEdge™ MultiPack systems Sun StorEdge A1000 Sun StorEdge D1000 Sun StorEdge A3500 Sun StorEdge A5100/A5200 Sun StorEdge T3 Sun StorEdge D2 Sun StorEdge S1 Sun StorEdge 3900/6900 Sun StorEdge 9900
External tape systems	SCSI tape devices via a SCSI host bus adapter: Sun StorEdge 12-GB DDS-3 UniPack Sun StorEdge DDS-3 FlexiPack Sun StorEdge DDS-3 Autoloader FlexiPack Sun StorEdge 20-GB DDS-4 UniPack Sun StorEdge DLT8000 FlexiPack Sun StorEdge L9 tape autoloader Sun StorEdge L20 tape library family Sun StorEdge L180 tape library Sun StorEdge L700 tape library (Utilization of the Sun StorEdge L180 and L700 tape libraries may be limited by the number of SCSI host bus adapters and buses available for connection to the server.)

SOFTWARE

Operating system	Solaris™ 8 2/02 or later
Languages	C, C++, FORTRAN, Java
Networking	ONC™, NFS, TCP/IP, SunLink™ OSI, MHS, IPX™/SPX
System and network management	Sun™ Management Center, Sun Remote System Control, Sun Cluster, Solaris PC Netlink, Solaris Management Console, Solstice JumpStart™, Solaris WebStart, Solaris Web Start Wizards, Solstice AdminSuite™, Solstice DiskSuite™, Solstice Backup™, and other Solstice™ products

CONSOLE OPTIONS

Monitor	Optional, Sun monitors from 1995 onward (17-, FP18-, 19-, 20-, 21-, and 24-inch)
Frame buffer	Sun PGX64 8/24-bit
Keyboard and mouse	USB keyboard and mouse
PCI I/O options	Gigabit Ethernet, 10/100-Mb/sec. Ethernet, FC-AL, Quad FastEthernet, token ring, FDDI, ATM-155, ATM-622, high-speed serial, Ultra™ SCSI with 10/100-Mb/sec. Ethernet, dual-channel single-ended Ultra SCSI, dual-channel differential Ultra SCSI

POWER SUPPLIES

One required, two for redundancy, each with independent power cord

Maximum AC input	1440 W per power supply
Maximum DC output	1184 W per power supply

ENVIRONMENT

AC power	100–240 VAC, 47–63 HZ, 0.895 KVA
Operating	5° C to 35° C (41° F to 95° F) 20% to 80% relative temperature humidity, noncondensing, 27° C maximum wet bulb
Nonoperating	-20° C to 60° C (-4° F to 140° F) 5% to 95% relative temperature humidity, noncondensing

REGULATIONS

Meets or exceeds the following requirements:

Safety	UL 1950, CB Scheme IEC 950 (CE mark), CSA C22.2 950 (from UL), TUV EN 60950
RFI/EMI	Class A: Australia/New Zealand AS/NZ 3548, Industry Canada ICES-003, European Community EN55022/CISPR22, Japan VCCI, Taiwan CNS 13438, and US FCC 47CFR15.B
Immunity	EN55024, EN61000-4-2, EN61000-4-3, EN61000-4-4, EN61000-4-5, EN61000-4-6, EN61000-4-8, EN61000-4-11, IEC 61000-3-2, and IEC 61000-3-3
X-ray	U.S. DHHS 21CFR Subchapter J, PTB German X-ray Decree

DIMENSIONS AND WEIGHT

Height	5U, 222 mm (8.75 in.)
Width	446 mm (17.5 in.)
Depth	610 mm (24.0 in.)
Weight	35.8 kg (79 lb.) (minimum) 44 kg (97 lb.) (fully configured)
Rack	Fits into a standard 19-inch-wide rack mount kit that complies with EIA-310-D-1992 standard, or a 72-inch height Sun StorEdge rack, which will support seven Sun Fire V480 servers.

UPGRADES

Upgrades are available for SPARC® server and Sun Enterprise™ systems. Contact your local Sun sales representative for details.

WARRANTY

Hardware support	3 years
Software install	90 days
Call response	8 hours
Delivery	Second business day, on-site

Sun Fire 280R

Sun Fire V480

Sun Fire V880

HEADQUARTERS SUN MICROSYSTEMS, INC. 901 SAN ANTONIO ROAD, PALO ALTO, CA 94303-4900 USA
PHONE: 650 960-1300 or 800 555-9SUN INTERNET: www.sun.com

Sun microsystems

take it to the n[th]

SALES OFFICES

AFRICA (NORTH, WEST AND CENTRAL): +9714-3366333 • ARGENTINA: +5411-4317-5600 • AUSTRALIA: +61-2-9844-5000 • AUSTRIA: +43-1-60563-0 • BELGIUM: +32-2-704-8000 • BRAZIL: +55-11-5187-2100 • CANADA: +905-477-6745 • CHILE: +56-2-3724500 • COLOMBIA: +571-629-2323 • COMMONWEALTH OF INDEPENDENT STATES: +7-502-935-8411 • CZECH REPUBLIC: +420-2-3300-9311 • DENMARK: +45 4556 5000 • EGYPT +202-570-9442 • ESTONIA: +372-6-308-900 • FINLAND: +358-9-525-561 • FRANCE: +33-134-03-00-00 • GERMANY: +49-89-46008-0 • GREECE: +30-1-618-8111 • HUNGARY: +36-1-489-8900 • ICELAND: +354-563-3010 • INDIA: BANGALORE: +91-80-2298989/2295454; NEW DELHI: +91-11-6106000; MUMBAI: +91-22-2018141 • IRELAND: +353-1-8055-666 • ISRAEL: +972-9-9710500 • ITALY: +39-039-60551 • JAPAN: +81-3-5717-5000 • KAZAKHSTAN: +7-3272-466774 • KOREA: +822-2193-5114 LATVIA: +371-750-3700 • LITHUANIA: +370-729-8468 • LUXEMBOURG: +352-49 11 33 1 • MALAYSIA: +603-21161888 MEXICO: +52-5-258-6100 • THE NETHERLANDS:+00-31-33-45-15-000 • NEW ZEALAND: AUCKLAND: +64-9-976-6800; WELLINGTON: +64-4-462-0780 • NORWAY: +47 23 36 96 00 • PEOPLE'S REPUBLIC OF CHINA: BEIJING: +86-10-6803-5588; CHENGDU: +86-28-619-9333; GUANGZHOU: +86-20-8755-5900; SHANGHAI: +86-21-6466-1228; HONG KONG: +852-2202-6688 • POLAND: +48-22-8747800 • PORTUGAL:+351-21-4134000 • RUSSIA: +7-502-935-8411 • SINGAPORE: +65-438-1888 • SLOVAK REPUBLIC: +421-2-4342-94-85 • SOUTH AFRICA: +2711-805-4305 • SPAIN: +34-91-596-9900 • SWEDEN: +46-8-631-10-00 • SWITZERLAND: GERMAN: 41-1-908-90-00; FRENCH: 41-22-999-0444 • TAIWAN: +886-2-8732-9933 • THAILAND: +662-344-6888 • TURKEY: +90-212-335-22-00 • UNITED ARAB EMIRATES: +9714-3366333 • UNITED KINGDOM: +44-1-276-20444 • UNITED STATES: +1-800-555-9SUN OR +1-650-960-1300 • VENEZUELA: +58-2-905-3800 • OR ONLINE AT SUN.COM/STORE

05/02

Document ID: ID41665
Synopsis: Sun[TM] GigaSwift Gigabit Ethernet Adapters - Further Information

Description To

Document Body To

GigaSwift Gigabit Ethernet Further Information

- Gigabit Ethernet is the IEEE standard for Ethernet with 1000 Mbit/s.
- Full Duplex operation allows simultaneous traffic in each direction, so the aggregate bandwidth is 2GBit/s.
- GigaSwift is the third generation of Sun gigabit ethernet products.
- It operates on both, fiber and copper cable.
- GigaSwift supports VLANs, it can decode VLAN tagged packets
- Older products are Gigabit Ethernet 1.x (vge) and Gigabit Ethernet 2.x/3.x (ge).
- Purpose
  - provide a "big pipe" for server connections to many clients or to backup systems.
  - provide services to different VLANS over one interface. GigaSwift can decode VLAN tagged packets.
  - Hardware TCP/UDP checksum generation, packet parsing and interrupt coalescing reduce CPU processing for increased server efficiency
  - Additionally, the SunSwitch is available.
- Common Standards
  - IP Versions 4 and 6
  - IEEE 802.1d - Quality of Service
  - IEEE 802.1p - Priority Tagging
  - IEEE 802.1q - VLAN Tagging
  - IEEE 802.3ab - 1000Base-TX over Category 5 UTP copper cable.
  - IEEE 802.3u - Fast Ethernet including Autonegotiation (100Mbit/s)
  - IEEE 802.3z - 1000Base-SX overFiber
  - IEEE 802.3x - Ethernet Flow Control (sender and receiver side)
  - Hardware Details

0170

- UTP NIC
  - Dynamic Reconfiguration and redundancy/failover support
  - 6.8inch x 4.2 inch short card
  - Load balancing for received packets among multiple CPUs
  - Does not support 1000 Mbit/s half duplex support (normally not needed)
  - Hardware TCP/UDP checksum generation, packet parsing and interrupt coalescing reduce CPU processing for increased server efficiency
  - Sun developed ASIC and Adapter
  - Standards our NIC applies to
    - IEEE 802.3ab (UTP NIC), 802.3z (Fiber NIC), 802.3u, 802.3x, 802.1q, 802.1p, 802.1d
    - special SNMP MIB
    - IPv4 and IPv6 support
    - PCI 2.2 33/66 MHz, 32 or 64 bit bus master

- Abbreviations/Acronyms
  - IEEE - Institute of Electrical and Electronics Engineers, Inc., standardizes Ethernet
  - Jumbo Frame - An Ethernet frame which is larger than 1518 bytes (9K bytes).
  - NIC - Network Interface Card
  - VLAN - Virtual LAN, the ability to have several independent net segments within one hardware.
  - LAN - Local Area Network, network which is geographically limited (typically to a 1 km radius, e.g. within a building)

Versions

- Hardware
  - Available Hardware Versions

Table 1. Hardware

Version	Mkt Part#	Part#	Comment
1.0	X1150A	501-5902	PCI copper UTP Adapter
1.0	X1151A		PCI Multimode Fiber Adapter
1.0	X1261A	501-5523	cPCI 3U Multimode Fiber Adapter

1.0	X2222A	501-5727	100 Mbit/s dual UTP/SCSI PCI Combo
1.0	A37	501-5819	SunFire V480 On-board 1000 Mbit/s

- How to Determine Hardware Version prtconf -pv | grep SUNW,pci-ce

- Software
  - Packages
    - SUNWced - Sun GigaSwift Ethernet Adapter (32-bit Driver)
    - SUNWcedx - Sun GigaSwift Ethernet Adapter (64-bit Driver)
    - SUNWcedu - Sun GigaSwift Ethernet Adapter Driver Headers
    - SUNWcem - Sun GigaSwift Ethernet Adapter Driver Man Pages
    - SUNWcea - Sun GigaSwift Ethernet Adapter Driver 32 bit adb Macros
    - SUNWceax - Sun GigaSwift Ethernet Adapter Driver 64 bit adb Macros
    - SUNWvld - VLAN utility routines (32-bit, for 5.8)
    - SUNWvldx - VLAN utility routines (64-bit, for 5.8)
    - SUNWvldx - VLAN utility headers (for 5.8)
  - How to Determine Product Version Number: pkginfo -l SUNWced | grep VERSION
  - How to Determine Driver Version Number: modinfo | grep CE or strings /kernel/drv/ce | grep CE or strings /platform/sun4u/kernel/drv/ce | grep CE

- Driver Versions Table

Table 2. Driver Versions

Version	Comment/Availability
1.87	GigaSwift 1.0 CD Part# 704-7117-10 (Jan.01)
1.105	Solaris 8 4/01
1.109	Solaris 8 10/01, GigaSwift 1.0u1 CD (Nov.01)
1.115	Solaris 9 FCS

Compatibility

- Hardware Compatibility

Table 3. Hardware Compatibility

supported Architecture	max # of cards		Comment			
	UTP	Fiber	cPCI	Combo		

Ultra 5,10	1	1		systems without graphic card
Ultra 60, E250	1	1		
Ultra 80	1	2		
E 220R	2	1		
E280R, E420, E450	2	2		
3x00-6x00	2	4		Use shielded UTP cable
E10K	TBD	X		
Netra 20	X			
Netra t1		X		
Netra t 112x	1	1		
Netra t 140x, AC/DC200	1			
Blade 100	1	1		
Blade 1000	2	2		
V480	X	X		
V880	4	4		
F 3800			4	cPCI X1261A, only
F 48x0,6800	X	X	4	
F12k,15k	6	X		

Key:
X - supported, max Number of cards not yet defined.
recommended CPU power:
500MHz per adapter, with a minimum of one 167MHz to handle interrupts. For max throughpu

- Software Compatibility Matrix A complete list of patches can be found on sunsolve.sun.com

Table 4. Software Compatibility

	Product Version
O/S	1.0
4.x	N/S
2.4	N/S
2.5	N/S
2.5.1	N/S
2.6	112327-NN
7*32	112327-NN
7*64	112327-NN
8	111883-NN
9	xxxxxx-NN

Key:
N/S - Product not supported on this OS
N/P - No patch applicable for this OS
N/A - Not Available
7*32 - Solaris 7 - 32 bit kernel

```
7*64 - Solaris 7 - 64 bit kernel
xxxxxx-NN means there is no patch for this version yet
```

Installation/Configuration Details

- Cabling
  - Fiber cable: Multimode Fiber 62.5um (max 260m) or 50um (max 550m), SC connector Part numbers: 2m - 537-1004, 5m - 537-1020, 15m 537-1006
  - Copper cable: Category 5, tested for Gigabit connections, max 100m, RJ45 connector
- Configuration Files Location
  - /etc/hostname.ce<instance number> - IPv4 address and interface config
  - /etc/hostname6.ce<instance number> - IPv6 address and interface config, Solaris 8
  - /etc/hostname.ce<vlan-tag><instance number> - VLAN interface config, IPv4 (for 5.8)
  - /etc/hostname6.ce<vlan-tag><instance number> - VLAN interface config, IPv6 (for 5.8)
  - /kernel/drv/ce.conf - can be used for Operational Mode parameter settings
  - /etc/system - can be used for Operational Mode parameter settings
  - /etc/path_to_inst - automatically generated to map hardware and driver
- Important configuration commands (short overview)
  - ifconfig - configure IP interface online
  - eeprom local-mac-address?=true - use unique onboard ethernet address
  - /usr/sbin/ndd -set /dev/ce - change Operational Mode parameters online
- More config tips
  - Use S68net-tune script to change Operational Mode parameters.
- Config file examples
  - /etc/system can NOT be used
  - /etc/path_to_inst is generated on boot -r to map hardware and driver

    path

    ```
    # grep ce /etc/path_to_inst
    "/pci@1f,2000/pci@1/network@0" 0 "ce"
    ```

  - /etc/hostname.ce<vlan-tag><instance number> - VLAN interface config

- VLAN packages are available for SunOS 5.8, only
- The hostname in this file should be found in /etc/hosts
- The VLAN tag must be the same on the link partner side (switch, other system)

```
                    instance # (last 3 digits, value=0 -> uses ce0 interface)
                    |||
/etc/hostname.ce123000
                      |||
                      VLAN tag (digit 4 and higher, value=123)
```

VLAN

```
# cat /etc/hostname.ce1000
lab058-enet11
# grep lab058-enet11 /etc/hosts
172.16.24.58    lab058-enet11
lab058# ifconfig ce1000
```

- Configure Ethernet Flow Control (802.3x)
  - Check out User's Guide Chapter 4, Configuring Driver Parameter - Flow Control Parameters.
  - use ndd command to enable sending and receiving of pause frames

NDD

```
# ndd -set /dev/ce adv_pause_cap 1
# ndd -set /dev/ce adv_autoneg_cap 0
```

  - enable sending and receiving of pause frames on the other side (switch)

Pause Frames

```
cat5500> (enable) set port flowcontrol 8/5 send on      (Example for a Cisco Catalys
Port 8/5 flow control send administration status set to on
(port will send flowcontrol to far end)
cat5500> (enable) set port flowcontrol 8/5 receive on
Port 8/5 flow control receive administration status set to on
(port will require far end to send flowcontrol)
```


  - check (on both sides) if setting was successful and is used

Setting

```
# kstat -p ce | grep link | grep pause
ce:0:ce0:link_asmpause  0
ce:0:ce0:link_pause     1
```

  - if setting was not successful, try to unplug/replug the cable or to disable/enable autonegotiation.
  - Use boot script to set parameters while booting.

FAQ

1. What can I do when the link does not come up?
   - Check Operational Mode settings (see below) and Hardware, see Troubleshooting)
2. How do I see the actual Operational Mode settings ?
   - Check link_ parameters of netstat -k ce[your_interface.number]
     - link_up - 0 down, 1 up
     - link_speed - speed in Mbit/s
     - link_duplex - 1 half duplex, 2 full duplex, 0 down

     This parameters must show the same values on both sides. If not, Autonegotiation does not work.

What can I do when Autonegotiation does not work ?

   - You can disable Autonegotiation and set the correct Operational Mode values yourself on both sides. This is called "Forced Mode".

4. How do I disable Autonegotiation ?
   - Use S68net-tune script to change Operational Mode parameters or ndd -set /dev/ce, see Troubleshooting
5. Is it OK if all MAC addresses are the same ?
   - In most modern networks, this will cause problems. (packet loss, low performance) To avoid this set eeprom local-mac-address\?=true and reboot.

6. The Link does not come up or has problems when connected to Cisco switch
   - Some Cisco switches (e.g. Catalyst 6500) have Autonegotiation disabled by default. This is not according to the IEEE 802.3z standard. To get the connection running, set both sides either to forced 1000 Mbit/s Full Duplex or enable Autonegotiation on the switch.
7. Does ce support Jumbo Frames ?
   - This feature can be implemented in the ce driver on request within a Sun Professional Services project. Such a driver will not be supported through the usual support channels.
8. Can I boot over gigabit ethernet?
   - Yes. Use the ce device path to boot. Autonegotiation to the link partner (switch) must be enabled and working, since you can not play with operational modes of the NIC in boot prom. To boot correctly, the SUNWce* packages must be installed on the boot server. That means, the boot image as well as the install base directory must contain the ge driver.

Driver

```
{0} ok show-nets
```

```
a) /pci@1f,4000/pci@2/network@0
...
q) NO SELECTION
Enter Selection, q to quit: a
a) /pci@1f,4000/pci@2/network@0 has been selected.
Type ^Y ( Control-Y ) to insert it in the command line...
{0} ok boot /pci@1f,4000/pci@2/network@0
.......
```

1. How do I see the Operational Mode settings ?
   - The driver distinguishes between 4 types of settings :
     - **"advertized"** - configurable Operational Mode parameters, will be used on next negotiation. Use show_ce.sh or ndd /dev/ce to read this driver parameters. To select the interface you want to check, use ndd -set /dev/ce instance [your_interface.number] The parameter names begin with adv_
     - **"capabilities"** - the hardware capabilities. The settings can be read with netstat -k ce [your_interface.number]. The parameter names begin with cap_.
     - **"link partner capabilities"** - the settings as the link partner reported them. Invalid when Autonegotiation was off on one side. The settings can be read with netstat -k ce [your_interface.number] The parameter names begin with lp_cap_.
     - **"actual mode"** - the actual used parameters. link_ parameters of netstat -k ce [your_interface.number]
2. How can I find out the current PCI bus speed ?
   - Type /usr/platform/[platform]/sbin and locate SUNW,pci-ce

Bus Speed

```
...
========================= IO Cards =========================
     Bus   Freq
Brd  Type  MHz   Slot  Name                          Model
---  ----  ----  -- -  ----------------------  -----------
SYS   PCI    66     2   pciclass,020000  SUNW,pci-ce
```


Information Gathering

Things to get:	Comment:
Do you suspect a problem concerning Gigabit Ethernet or IP ?	If IP, the GBE part may not k
network topology plan	What is connected to what? (c
The other side: link partner	e.g. Sun, repeater, switch (t
Sun System (*)	machine type
card version ? (*)	try prtconf -pv | grep SUNW,p
Software Version (*)	pkginfo -l SUNWced | grep VER

Are recommended patches installed ? (*)	
connection completely down or is some traffic possible ?	
Did it work once ?	YES - Are there changes in S NO - Is it an installation/c
Are there error messages ? (*)/var/adm/messages, /var/log/syslog	
Does netstat -k ce[if#] show any errors ? (*)	ierrors oerrors late_coll
Config Files: /etc/hostname.ce*(*), /kernel/drv/ce.conf, /etc/system	
IP config (*)	ifconfig -a; netstat -rvpn

Things to try:

Unique MAC addresses? (*)	in most cases eeprom local-m
Operational Mode configuration (*)	See FAQ
Operational Mode config of the link partner	See FAQ
Snoop suspected interface	e.g. snoop -d ce[if#] -o ce.
What do the LEDs on the Board show ?	
hardware test	See Troubleshooting

- information needed to assign to the next level of support:
  - Short failure description including error or warning messages
  - Short customer situation including timeframes and business impact
  - Platform, part# and revision of NIC, used SBUSor PCI slot (if obtainable)
  - Special commands (see above, if no explorer is available)
  - Special commands (see above, information is not collected by explorer)
  - Explorer output (or path to location)
  - Product gather output (or path to location)
  - Network overview (detailed sketch, cable lengths

- Where is a test machine connected (e.g. a "slow" client) ?
- Short description of your measures to find and solve the problem before the handover
- Use handover template to assign to next level

Installation/De-installation

- Installation
  - Hardware
    - Cabling:
      - Copper: max. 100m Category 5 (or better) Unshielded Twisted Pair (UTP), RJ-45 Plug.
      - Fiber: Multimode Fiber: max 260 62.5u or max 500m 50u, SC-Plug
  - Software
    - sample install log
- De-Installation
  - remove the packets, delete the config files, remove entries from /etc/hosts, etc., remove the card(s)

Troubleshooting

- Troubleshooting Info
  - Check LED state
    - PCI cards:

Table 5. PCI cards

Label	Colour	Meaning	Source
LINK QUALITY	Purple	Gigabit link quality good	PHY
1000X	Green	Link 1Gbit/s up	PHY
100X	Green	Link 100Mbit/s up	PHY
10X	Green	Link 10Mbit/s up	PHY
FDX	Green	Full Duplex Mode	PHY
FDX	Off	Half Duplex Mode	PHY
TX	Green	PHY Transmitting Data	PHY
RX	Green	PHY Receiving Data	PHY
TXM	Green	MAC Transmitting Data	MAC
RXM	Green	MAC Receiving Data	MAC

- compact PCI cards:

Table 6. PCI Cards

Label	Colour	Meaning	Source
HOT SWAP	Blue	Hot swap possible	

- Check Hardware on BootProm (if the Cable is connected properly)

BootProm

```
{0} ok setenv auto-boot? false necessary, if it was set to true
{0} ok reset all
{0} ok show-nets
a) /pci@1f,4000/pf@5
b) /pci@1f,4000/network@1,1
c) /pci@1f,4000/pci@2/network@0
q) NO SELECTION
Enter Selection, q to quit: c
/pci@1f,4000/pci@2/network@0 has been selected.
Type ^Y ( Control-Y ) to insert it in the command line.
e.g. ok nvalias mydev ^Y
         for creating devalias mydev for
/pci@1f,4000/pci@2/network@0
{0} ok test /pci@1f,4000/pci@2/network@0 (you can use ^Y for the path)
Testing /pci@1f,4000/pci@2/network@0
Internal loopback test -- succeeded.
Link is  -- up
{0} ok watch-net /pci@1f,4000/pci@2/network@0
Internal loopback test -- succeeded
Transceiver check  -- passed
Looking for Ethernet Packets.
'.' is a Good Packet.  'X' is a Bad Packet.
Type any key to stop.
.......^C
{0} ok setenv auto-boot? true necessary, if it was set to true before
{0} ok
```

- Error Messages
  - /var/adm/messages : WARNING: ce0: xcvr addr:0x01 - link down - physical connection cut, link partner down or Autonegotiation failed

- Traces/Commands
  - netstat -k ge0 shows error statistics counters. Check the most important ones:
    - ierrors - should be smaller than 1% of ipackets
    - oerrors - should be smaller than 1% of opackets
    - late_collisions - Wrong Operational Mode settings or illegal network diameter
    - crc_err, code_violations - Corrupted incomig packets, should be smaller than 1% of ipackets
    - code_violations - Corrupted incomig packets, should be smaller than 1% of ipackets
  - Force Operational Mode when Autonegotiation fails: To select the interface you want to change,

use ndd -set /dev/ce instance [your_interface.number]. Then ndd -set /dev/ce to set the "advertized" (adv_) values. link_master must be 0 on one side and 1 on the other. Switches use 1, default for our card is 0.

Interface number

```
example: forced 1000 Mbit/s on an UTP
# ndd -set /dev/ce instance 0  <-- settings for ce0
# ndd -set /dev/ce link_master 0  <-- for switch connection
# ndd -set /dev/ce adv_1000fdx_cap 1
# ndd -set /dev/ce adv_1000hdx_cap 0
# ndd -set /dev/ce adv_100fdx_cap 0
# ndd -set /dev/ce adv_100hdx_cap 0
# ndd -set /dev/ce adv_10fdx_cap 0
# ndd -set /dev/ce adv_10hdx_cap 0
# ndd -set /dev/ce adv_autoneg_cap 0
```

Sometimes you must unplug and replug the connector to initialize Autonegotiation.

Performance

- Performance Tuning Hints
  - use a 66MHz, 64 bit PCI slot.
  - Select a slot that does not share bus bandwidth with other slots.
  - 4x 300 MHz CPUs needed for maximum performance.
  - For PCI performance, use Solaris 2.6 5/98 or later.
- Test Results
  - Tolly Group Test on a e6.5k/400MHz stated:
    - 940 Mbit/s unidirectional traffic, download (Solaris 8)
    - 925 Mbit/s unidirectional traffic, download (Solaris 7)
    - 848 Mbit/s bidirectional traffic (Solaris 7)
  - Performance should be measured with several ttcp streams.

References

- Manuals
  - Platform Notes: Sun GigaSwift Ethernet on docs.sun.com
- Other Important Links
  - GigaSwift on www.sun.com
  - Product Photos

CISCO SYSTEMS

12933 E

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.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0183
Doc: 3696

7) A Cisco do Brasil recomenda, para o Edital 050/2003 da Empresa de Correios e Telégrafos, o uso o sistema operacional Pix OS versão 6.2 para os firewalls Cisco Pix 535 e Pix 525.

8) O firewall Cisco Pix 525 com a versão do sistema operacional Pix OS 6.2 possui capacidade de processamento superior a 350 Mbps em texto claro.

9) O sistema de detecção de intrusão IDS 4250 permite a detecção de ataques que utilizam recursos de detecção Whisker anti-IDS.

10) O sistema de detecção de intrusão IDS 4250 permite a detecção de Probin Attacks através das assinaturas de ataques do tipo Probe, como por exemplo Finger Probe, Apache/mod_ssl Worm Probe, SATAN Probe e Backdoor Probes em portas TCP ou UDP.

Atenciosamente,

CONFERIDO POR

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 DE
001-SERGIO FUMIAKI TSUJIOKA
SAO PAULO, 23 DE JULHO DE 2003.
EM TESTEMUNHO DA VERDADE
MARCIO ROBERTO TROFINO-ESC. AUTORIZ.
Total Custas:*******2,07
Car.:133123 DOC.S/V.ECONOMICO
Selo:1063AA054804

Marcio Roberto Trofino
Escrevente Autorizado

Colégio Notarial do Brasil SP
FIRMA 1
1063AA054804

0184

Comprovação das Especificações Exigidas no Edital 050/2003

3. Conectividade da rede

23/07/03

NEC

12931 E

Comprovação das Especificações Exigidas no Edital 050/2003

3.1. Switch tipo 1 (Layer-3 GE)

23/07/03

0185

Switch Tipo 1	
c6000_ds.pdf	Cisco Catalyst 6500 Series Switch
c60ge_ds.pdf	Cisco Catalyst 6500 Series Gigabit Ethernet Modules
01overvw.pdf	Product Overview - Hot-swapping Supervisor Engines na Switching Modules
overview.pdf	CSM Feature Set Description
intro.pdf	Product Overview
supe_ds.pdf	Cisco Catalyst 6500 Supervisor Engines 1A and 2
buffe_wp.pdf	Buffers, Queues, and Thresholds on Cisco Catalyst 6500 Series Ethernet Modules

Data Sheet

Cisco Catalyst **6500** Series Switch

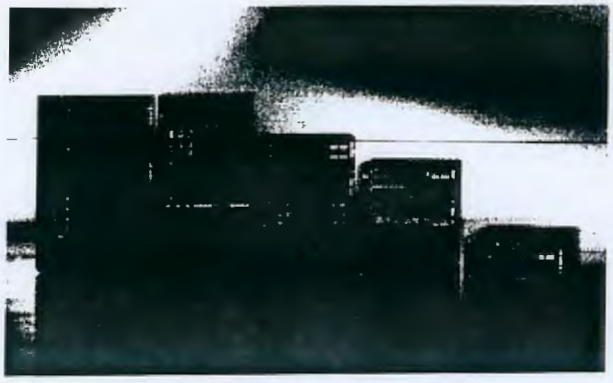
The Catalyst 6500 Series sets the new standard for IP communications and application delivery in enterprise campus and service provider networks by maximizing user productivity and enhancing operational control while providing unprecedented investment protection. As Cisco's premier intelligent multilayer 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



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

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

- 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

Table 1 Catalyst 6500 Series at a Glance

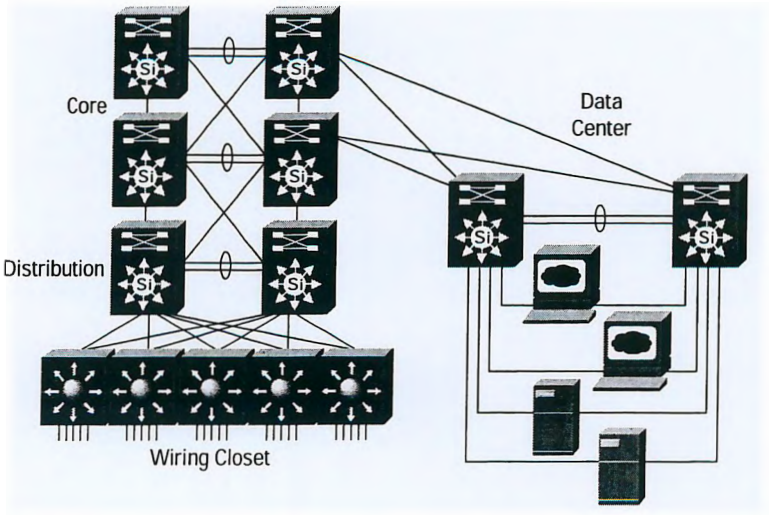
Feature	Catalyst 6500 Series
Operating System	Catalyst OS (CatOS) Cisco IOS CatOS/IOS Hybrid Configuration
Redundant Supervisors	Yes, with stateful failover
Redundant Components	Power supplies (1+1) Switch fabric (1+1) Replaceable clock Replaceable fan tray
High Availability Features	Gateway Load Balancing 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

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.

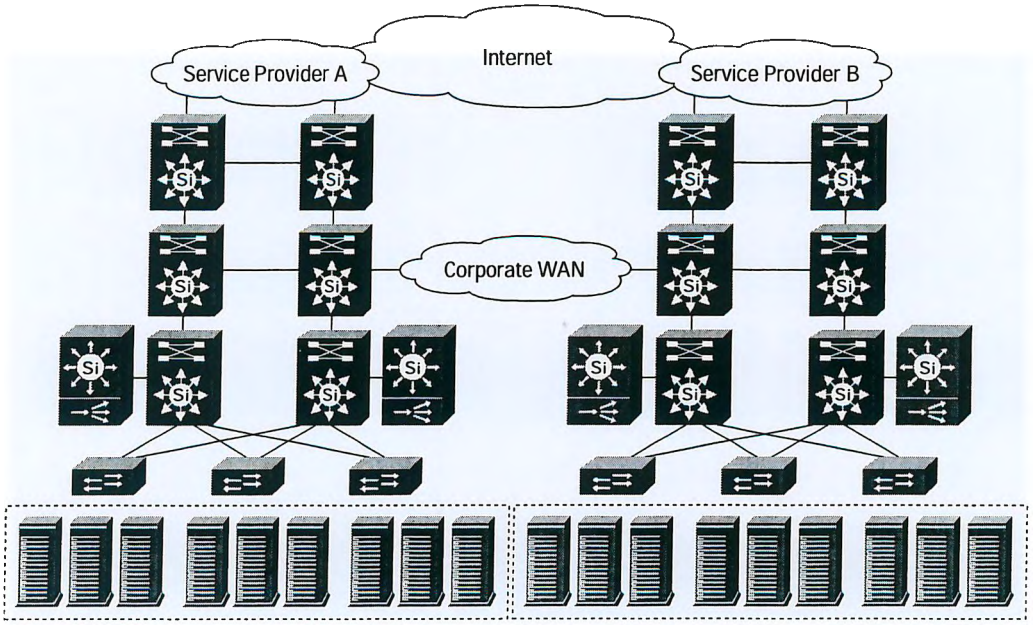
- *Campus networks*—Features 10/100 and 10/100/1000 autosensing modules that provide inline power for the wiring closet, along with robust high availability, security, and manageability features; world-class networking software; high-performance Gigabit and 10 Gigabit interface modules; and network management for the distribution and core

Figure 2
Deployment Scenarios for Catalyst 6500 Series Switches in Campus Networks



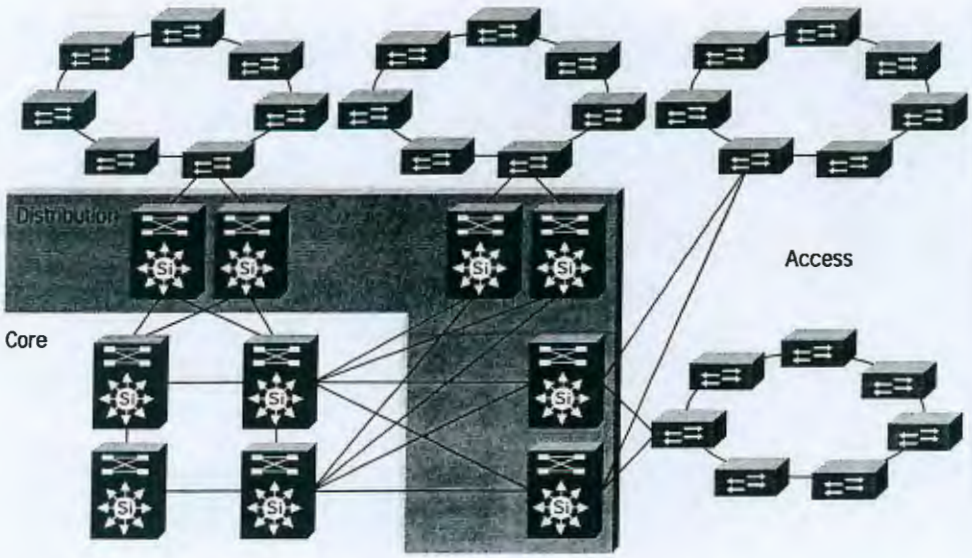
- [*ISP network*—Provides robust high-availability, security, and manageability features; world-class networking software; high-performance Gigabit and 10 Gigabit interface modules; and network management for the most demanding service provider networking environments requiring Multiprotocol Label Switching (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



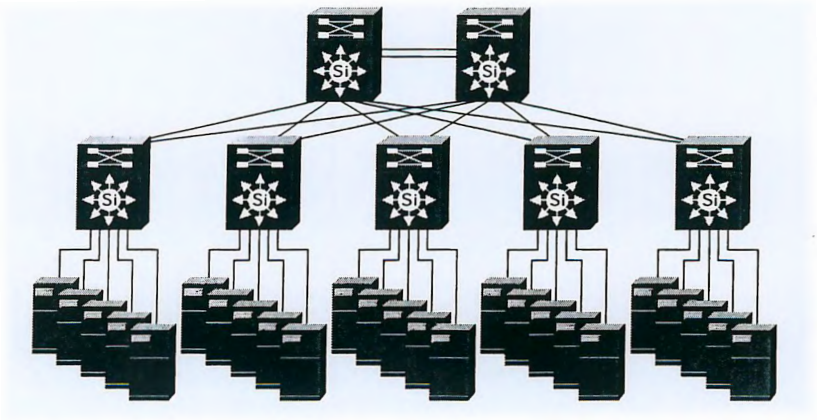
- *Metro edge*—Features edge-, distribution-, and core-layer interfaces for point-to-point and multipoint Ethernet services for metro and inter-metro network deployments with the following features:
  - High-performance 10-Gigabit Ethernet uplinks
  - 802.1Q tunneling
  - Ethernet over MPLS (EoMPLS)
  - 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



- *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



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

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.

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

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

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

- *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.

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.

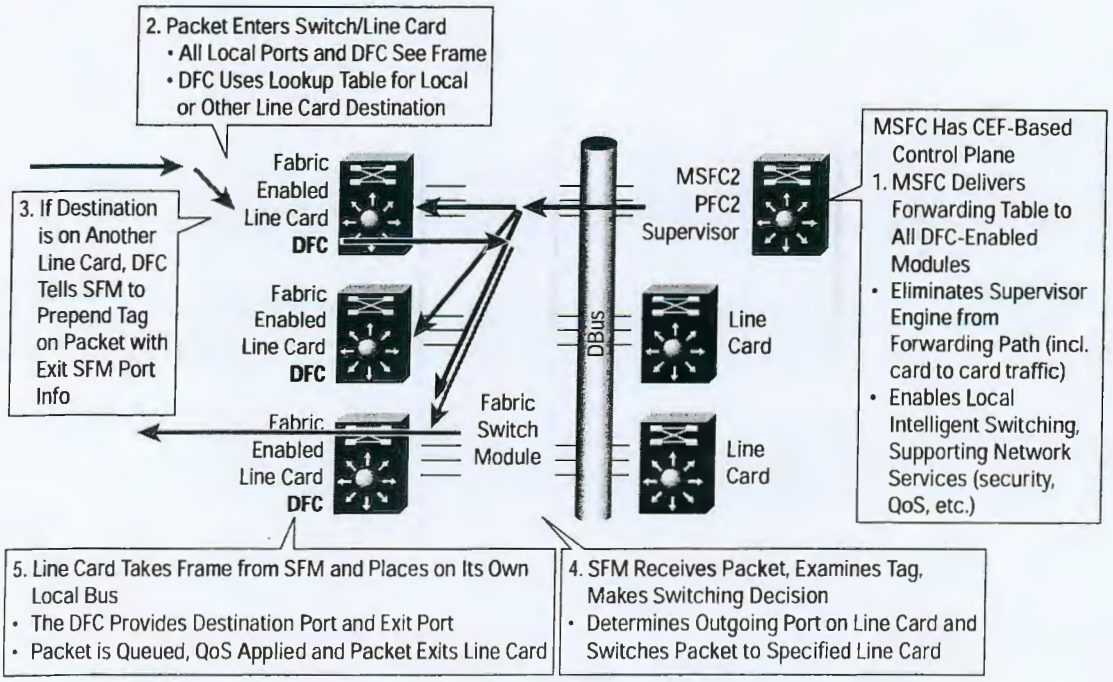
How Distributed Cisco Express Forwarding (dCEF) Works

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.

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.

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.

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.

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.

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

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

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

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

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 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

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

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

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

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

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)

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

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

MH/LW4273 0403

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:

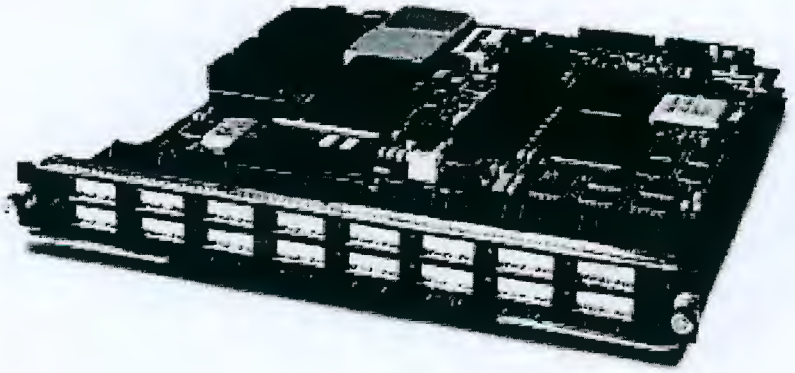
- Flexible configurations for any deployment—Provide flexible port densities, media choices, and performance speeds for any deployment requirement
- Choice of media and connector type—Available in multimode fiber or single-mode fiber using MT-RJ and modular GBIC and SFP optics supporting station-to-station 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

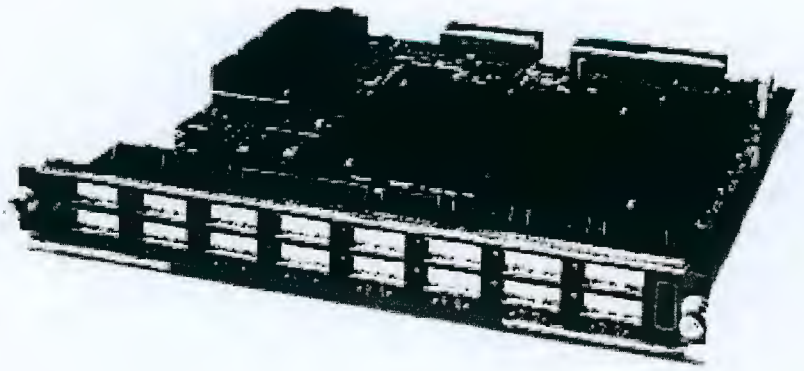
- High port densities—From 8 up to 16 ports per module, up to 256 ports per system
- Scalable and predictable performance—Provide a selection of switch fabric connections and throughput: 32 Gbps bandwidth/15 Mpps (Classic interface modules), 256 Gbps bandwidth/30 Mpps (CEF256 interface modules), and 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

- 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



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

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.

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

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

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

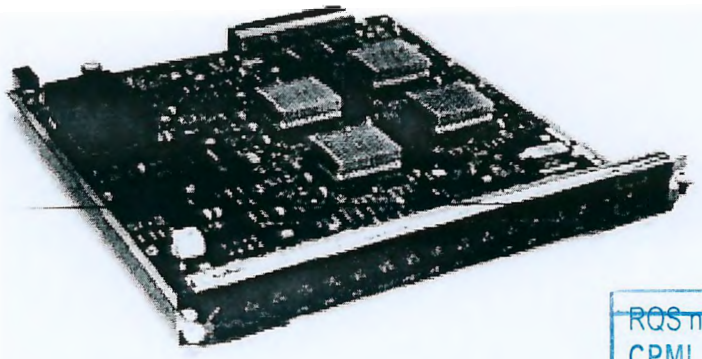
Distributed forwarding upgrade—None; Classic interface modules cannot be upgraded for distributed forwarding

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



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

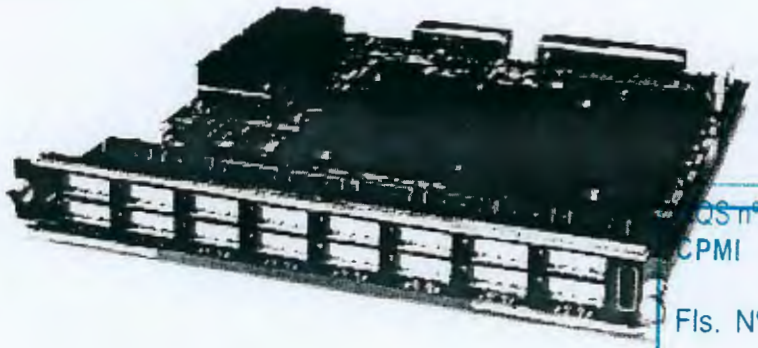
Port densities—192 ports: Catalyst 6513 chassis; 128 ports: Catalyst 6509 chassis

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 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

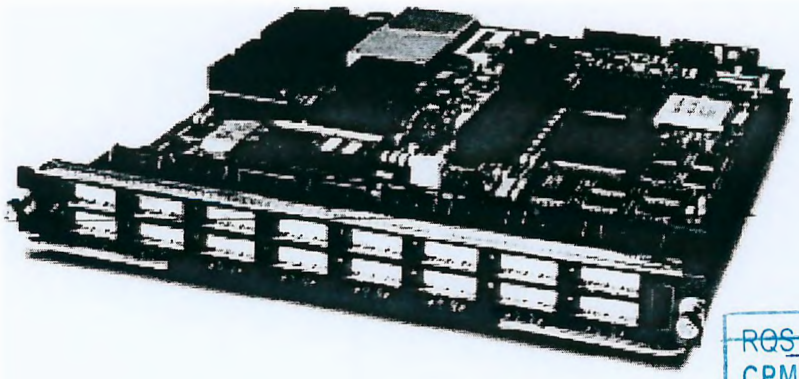
Distributed forwarding—Include a DFC when operating with Supervisor Engine 2 or a DFC3 when operating with Supervisor Engine 720

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



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	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

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)

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

- 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.

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

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

MH/LW4213 0403

CHAPTER 1

Product Overview

The Catalyst 6000 family switches facilitate the migration from traditional shared-hub LANs to large-scale, fully integrated internetworks. These switches provide switched connections to individual workstations, servers, LAN segments, backbones, or other switches using a variety of media.

This chapter consists of these sections:

Supervisor Engine Software

The supervisor engine software is factory-installed on every supervisor engine. Some modules (such as ATM modules) require an additional factory-installed software image.

The Catalyst 6000 family switches share a command-line interface (CLI) with which you can configure modules and ports on the switches. For more information, see Chapter 2, "Command-Line Interfaces." For descriptions of the available CLI commands, refer to the *Catalyst 6000 Family Command Reference* publication.

Supported Software Features

The Catalyst 6000 family switches support these software features:

Spanning Tree Protocol

The Spanning Tree Protocol (STP) allows you to create fault-tolerant internetworks that ensure an active, loop-free data path between all nodes in the network. STP uses an algorithm to calculate the best loop-free path throughout a switched network.

The Catalyst 6000 family switches support the following spanning tree enhancements:

- Spanning tree PortFast—PortFast allows a port with a directly attached host to transition to the forwarding state immediately, bypassing the listening and learning states. Additionally, PortFast BPDU guard provides a method for preventing loops by moving a nontrunking port into an errdisable state when a BPDU is received on that port. The PortFast BPDU guard option allows for fast convergence in a network while also preventing loops from occurring.
- Spanning tree UplinkFast—UplinkFast provides fast convergence after a spanning tree topology change and achieves load balancing between redundant links using uplink groups. Uplink groups provide an alternate path in case the currently forwarding link fails. UplinkFast decreases spanning tree convergence time for switches that experience a direct link failure.
- Spanning tree BackboneFast—BackboneFast reduces the time needed for the spanning tree to converge after experiencing a topology change caused by an indirect link failure. BackboneFast decreases spanning tree convergence time for any switch that experiences an indirect link failure.

For information on configuring STP, see Chapter 6, "Configuring Spanning Tree." For information on configuring the STP enhancements, see Chapter 7, "Configuring Spanning Tree PortFast, UplinkFast, and BackboneFast."

VLANs

A VLAN is an administratively defined broadcast domain that enhances performance by limiting traffic; it allows the transmission of traffic among stations that belong to it and blocks traffic from other stations in other VLANs. VLANs can provide security barriers (firewalls) between end stations on different VLANs within the same switch. Only end stations within the VLAN receive packets that are unicast, broadcast, or multicast (flooded).

These VLAN-related features are also supported on the switches:

- VLAN Trunk Protocol (VTP)—VTP maintains VLAN naming consistency and connectivity between all devices in the VTP management domain. When you add new VLANs on a switch, VTP distributes this information automatically to all the devices in the management domain. VTP is transmitted on all trunk connections, including ISL, 802.1Q, and ATM LAN Emulation (LANE). You can have redundancy in a domain by using multiple VTP servers, through which you can maintain and modify the global VLAN information. Only a few VTP servers are required in a large network.

- GARP VLAN Registration Protocol (GVRP)—GVRP is an industry-standard VLAN management protocol specified in IEEE 802.1p for use in IEEE 802.1Q environments.

For information on configuring VTP, see Chapter 8, "Configuring VTP." For information on configuring VLANs, see Chapter 9, "Configuring VLANs." For information on configuring GVRP, see Chapter 11, "Configuring GVRP."

VLAN Trunks

You can extend VLANs from one switch to another, or from a switch to a router, using VLAN trunks. To verify the trunking capabilities of a particular port, see the hardware documentation for your switch or use the **show port capabilities** command.

You can split VLAN traffic between parallel trunks. By setting spanning tree parameters on a per-VLAN basis, you can define which VLANs are active on a trunk and which use the trunk as a backup if the primary trunk fails.

For information on configuring trunks, see the following sections:

- For information on configuring ISL and 802.1Q Ethernet VLAN trunks, see Chapter 10, "Configuring Ethernet VLAN Trunks."
- For information on configuring ATM LANE, refer to the *ATM Software Configuration and Command Reference—Catalyst 5000 Family and Catalyst 6000 Family Switches* publication.

EtherChannel Port Bundles

EtherChannel port bundles allow you to create high-bandwidth connections between two switches or a switch and a router by grouping multiple ports into a single logical transmission path.

For information on configuring EtherChannel, see Chapter 5, "Configuring EtherChannel."

Network Security

The Catalyst 6000 family switches support these network security features:

- Local, RADIUS, TACACS+, and Kerberos authentication—You can control access to the switch using any combination of these authentication methods. For information on configuring authentication, see Chapter 15, "Switch Access: Using Authentication, Authorization and Accounting."
- Secure port filtering—You can block input to an Ethernet, Fast Ethernet, or Gigabit Ethernet port when the MAC address of a station attempting to access the port is different from the configured or learned MAC address. For information on secure port filtering, see Chapter 29, "Configuring Port Security."
- IP permit list—You can restrict incoming Telnet and SNMP access to a limited list of IP addresses. For information on the IP permit list, see Chapter 28, "Configuring IP Permit List."

Network Management

The Catalyst 6000 family switches offer network management and control through the CLI or through alternative methods, such as CWSI and SNMP. The switch software supports these network management features:

- SNMP—This protocol facilitates the exchange of management information between network devices. Catalyst 6000 family switches support these SNMP types and enhancements:
  - SNMP—Simple Network Management Protocol, a Full Internet Standard
  - SNMP v2C—Community-based administrative framework for Version 2 of SNMP
  - SNMP v3—Community-based administrative framework for Version 3 of SNMP
  - SNMP trap message enhancements—Additional information with certain SNMP trap messages, including spanning tree topology change and configuration change notifications.

  For information on SNMP, see Chapter 30, "Configuring SNMP."
- Remote Monitoring (RMON)—This protocol allows network monitors and console systems to exchange network monitoring data. The following RMON enhancements are supported:
  - Extended RMON alarms—RMON alarms for all MIB objects supported by the Catalyst 6000 family switch SNMP agent.
  - RMON2 configuration group—The RMON2 configuration group trap destinations MIB defined in RFC 2021. When you generate a trap, it is sent to all the hosts configured in the sysTrapReceiverTable and the trapDestTable, and is registered at the given User Datagram Protocol (UDP) port.

  For information on RMON, see Chapter 31, "Configuring RMON."
- Switched Port Analyzer (SPAN)—SPAN allows you to monitor traffic on any port for analysis by a network analyzer or RMON probe. Remote SPAN (RSPAN) allows you to remotely monitor any port or VLAN from any other switch in the network. For information on SPAN and RSPAN, see Chapter 32, "Configuring SPAN and RSPAN."
- System message logs—You can redirect system error messages and output from asynchronous events such as an interface transition, to a virtual terminal, internal buffers, or a UNIX host running a syslog server. The syslog format is compatible with 4.3 BSD UNIX. For information on system message logging, see Chapter 21, "Configuring System Message Logging."
- Switch TopN reports—This feature allows you to generate a report showing metrics for port utilization, broadcasts, multicasts, unicasts, and errors. Reports are available through either SNMP or the CLI. The Switch TopN Reports utility cannot be used to generate reports on the Multilayer Switch Feature Card (MSFC), Multilayer Switch Module (MSM), or ATM ports. For information on switch TopN reports, see Chapter 33, "Using Switch TopN Reports."

For a list of MIBs supported on the Catalyst 6000 family switches, see the "Supported MIBs" section on page 1-8. For additional information, refer to the "*Enterprise MIB User Quick Reference*," on Cisco Connection Online (http://www.cisco.com).

Multicast Services

Multicasting saves bandwidth by forcing the network to replicate packets only when necessary and by allowing hosts to join and leave groups dynamically. These multicast services are supported:

- Internet Group Management Protocol (IGMP) snooping—IGMP snooping manages multicast traffic. The switch software examines IP multicast packets and makes forwarding decisions based on their content. Multicast traffic is forwarded only to ports with attached hosts interested in receiving the multicast traffic. IGMP snooping is supported only with specific hardware.
- GARP Multicast Registration Protocol (GMRP)—GMRP is an industry-standard multicast group membership protocol specified in 802.1p.
- Router Group Management Protocol (RGMP)—Multicast routers receive all multicast data traffic unless they are configured to do otherwise. RGMP enables a switch to reduce network congestion by forwarding multicast data traffic to only those routers that are configured to receive it.

For information on configuring multicast services, see Chapter 34, "Configuring Multicast Services."

Broadcast Suppression

Broadcast suppression controls excessive broadcast traffic in the network. You can limit the number of broadcasts from switch ports to prevent congestion caused by broadcast storms. For information on configuring broadcast suppression, see Chapter 26, "Configuring Broadcast Suppression."

Administrative Features

These administrative features are supported:

- Multiple default IP gateways—You can configure up to three default IP gateways to provide redundancy. In the event that the primary gateway is not reachable, the switch uses the secondary default IP gateways in the order in which they were configured. For information on configuring default gateways, see Chapter 3, "Configuring the Switch IP Address and Default Gateway."
- Domain Name System (DNS)—This protocol resolves IP addresses to host names. In addition, a Catalyst 6000 family switch populates the system name string based on the switch IP address-to-host name mapping in DNS. For information on configuring default gateways, see Chapter 22, "Configuring DNS."
- Cisco Discovery Protocol (CDP)—This protocol discovers and learns information about neighboring Cisco devices on the network. Network management applications can use CDP to retrieve the device type and SNMP-agent address of neighboring devices so the applications can send SNMP queries to neighboring devices. For information on configuring default gateways, see Chapter 23, "Configuring CDP."
- Network Time Protocol (NTP)—This protocol time-synchronizes switches by downloading the system time from an NTP server. Synchronization allows events to be correlated when system logs are created and other time-specific events occur. For information on configuring default gateways, see Chapter 25, "Configuring NTP."

InterVLAN Routing

InterVLAN routing allows network devices in different VLANs to communicate with one another. There are two ways to do interVLAN routing on Catalyst 6000 family switches:

- MSM—For information on configuring interVLAN routing using the MSM, refer to the *Multilayer Switch Module Installation and Configuration Note.*
- MSFC—For information on configuring interVLAN routing using the MSFC, refer to the *Catalyst 6000 Family Multilayer Switch Feature Card and Policy Feature Card Configuration Guide.*

Multilayer Switching and NetFlow Data Export

Multilayer Switching (MLS) scales Layer 3 performance to high-performance link speeds by extending the MLS concept introduced in Cisco IOS software to LAN switching hardware. MLS requires a Catalyst 6000 family switch with an MSFC. NetFlow Data Export allows you to export MLS flow information to an RMON probe for analysis.

Three MLS feature sets are supported:

- IP unicast MLS
- IP multicast MLS
- IPX unicast MLS

For more information, refer to the *Catalyst 6000 Family Multilayer Switch Feature Card and Policy Feature Card Configuration Guide.*

Access Control Lists

Supported access control lists (ACLs) are as follows:

- IOS ACLs require the MSFC
- VLAN ACLs (VACLs) require the Policy Feature Card (PFC)
- Quality of service (QOS) ACLs require the MSFC and PFC

For information on configuring these ACLs, refer to the *Catalyst 6000 Family Multilayer Switch Feature Card and Policy Feature Card Configuration Guide.*

Quality of Service

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.

QoS uses classification, marking, policing, and scheduling to transmit traffic from the switch in a predictable manner. For information on configuring QoS, see Chapter 35, "Configuring Quality of Service."

Redundant Supervisor Operation

Catalyst 6000 family switches support an optional redundant supervisor engine. You can install two supervisor engines in slots 1 and 2 of the chassis. When the switch powers up, the supervisor engine that comes up first enters active mode, while the second supervisor engine enters standby mode.

Both supervisor engines must have the same feature cards:

- L2 Switching Engine I WS-F6020 or L2 Switching Engine II WS-F6020A
- MSFC
- PFC

All network management functions occur on the active supervisor engine. The console port on the standby supervisor engine is inactive. The uplink ports on the standby supervisor engine are active and can be used as normal switch ports.

If the active supervisor engine detects a major problem, it resets itself and the standby supervisor engine seamlessly becomes the active supervisor engine.

For information on how supervisor engine redundancy works, see Chapter 16, "Configuring Redundant Supervisor Engines."

Voice-Over-IP

Telephony systems built on an IP network instead of the traditional circuit-switched Private Branch Exchange (PBX) are called IP PBX systems. For information on how to configure your Catalyst 6000 family switch for Voice-over-IP networking, see Chapter 36, "Configuring a Voice-over-IP Network."

Supported Internet Protocols

The Catalyst 6000 family switches support these standard Internet protocols:

- Address Resolution Protocol (ARP)—Determines the destination MAC address of a host using its known IP address.
- Bootstrap Protocol (BOOTP)—Allows the switch (BOOTP client) to retrieve its IP address from a BOOTP server. BOOTP uses connectionless transport layer User Datagram Protocol (UDP).
- Dynamic Host Configuration Protocol (DHCP)—Provides a mechanism for allocating IP addresses dynamically so that addresses can be reused when hosts no longer need them.
- Internet Control Message Protocol (ICMP)—Allows hosts to send error or control messages to other hosts. ICMP is a required part of IP. For example, the **ping** command uses ICMP echo requests to test if a destination is alive and reachable.
- IP—Sends IP datagram packets between nodes on the Internet. IP is a protocol suite.
- ping—Tests the accessibility of a remote site by sending an ICMP echo request and waiting for a reply.
- Reverse Address Resolution Protocol (RARP)—Determines an IP address knowing only a MAC address. For example, BOOTP, DHCP, and RARP broadcast requests are used to get IP addresses from a BOOTP, DHCP, or RARP server.
- SLIP—Allows IP communications over the administrative interface. SLIP is a version of TCP/IP that runs over serial links.

- SNMP—Processes requests for network management stations and reports exception conditions when they occur. These agents require access to information stored in a MIB. (For more information, see the "Network Management" section on page 1-3.)
- TCP—Transports full-duplex, connection-oriented, end-to-end packets running on top of IP. For example, Telnet uses the TCP/IP protocol suite.
- Telnet—Allows remote access to the administrative interface of a switch over the network (in band). Telnet is a terminal emulation protocol.
- Trivial File Transfer Protocol (TFTP)—Downloads software updates and configuration files to workgroup switch products.
- UDP—Allows an application (such as an SNMP agent) on one system to send a datagram to an application (a network management station using SNMP) on another system. UDP uses IP to deliver datagrams. UDP/IP protocol suites are used by TFTP and SNMP.

Supported MIBs

Catalyst 6000 family switches support these standard and private MIBs:

- BRIDGE-MIB (RFC 1493)
- CISCO-CDP-MIB
- CISCO-COPS-CLIENT-MIB
- CISCO-ENTITY-FRU-CONTROL-MIB
- CISCO-ENTITY-SENSOR-MIB
- CISCO-FLASH-MIB
- CISCO-IMAGE-MIB
- CISCO-MEMORY-POOL-MIB
- CISCO-PAGP-MIB
- CISCO-PIB-MIB
- CISCO-PROCESS-MIB
- CISCO-QOS-MIB
- CISCO-RMON-CONFIG-MIB
- CISCO-RSVP-MIB
- CISCO-STACK-MIB
- CISCO-STP-EXTENSIONS-MIB
- CISCO-SWITCH-ENGINE-MIB
- CISCO-SYSLOG-MIB
- CISCO-VLAN-BRIDGE-MIB
- CISCO-VLAN-MEMBERSHIP-MIB
- CISCO-VTP-MIB
- ENTITY-MIB
- ETHERLIKE-MIB
- HC-RMON-MIB.my

- IF-MIB (RFC 1573)
- RFC 1213 (MIB II)
- RMON MIB (RFC 1757)
- RMON2-MIB (probeInformationGroup, trapDestTable from RFC 2021)
- SMON-MIB

For information about MIBs, refer to:
http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml.

Hot Swapping Supervisor Engines and Switching Modules

You can remove and replace redundant supervisor engines and switching modules without powering down the switch. This feature is known as *hot swapping*.

When you remove or insert a switching module while the switch is powered on and operating, the switch does the following:

1. Determines if there is sufficient power for the module.
2. Scans the backplane for configuration changes.
3. Initializes all newly inserted switching modules, notes any removed modules, and places them in the administratively shutdown state.
4. Places any previously configured interfaces on the switching module back to the state they were in when they were removed. Any newly inserted interfaces are put in the administratively shutdown state, as if they were present (but unconfigured) at boot time. If you insert a similar switching-module type into a slot, its ports are configured and brought online up to the port count of the original switching module.

The switch runs diagnostic tests on any new interfaces. If the test passes, the switch is operating normally. If the new switching module is faulty, the switch resumes normal operation but leaves the new interface disabled.

If the diagnostic test fails, the switch crashes, which usually indicates that the new switching module has a problem in the bus and should be removed.

When you install two supervisor engines, hot swapping allows you to remove and replace one of the supervisor engines without turning off the system power.

Caution To avoid erroneous failure messages, note the current configuration of all interfaces before you remove or replace another switching module, and allow at least 15 seconds for the system to reinitialize after a module has been removed or replaced.

Table 1-2 CSM Feature Set Description (continued)

Features
XML configuration interface
SNMP
GSLB (Global Server Load Balancing)
Resource usage display
Idle timeout for unidirectional flows
STE integration for SSL load balancing
HTTP method parsing
Regular expression scalability improvements
Real server names
Non-TCP connection redundancy
FT show command enhancements
IOS SLB FWLB interoperation (IP reverse-sticky)
Slowpath performance improvements
Multiple CSMs in a chassis
CSM and IOS-SLB functioning simultaneously in a chassis
HTTP 1.1 persistence (all GETs to the same server)
Full HTTP 1.1 persistence (GETs balanced to multiple servers)
Fully configurable NAT
Server initiated connections
Route health injection
Load-balancing Algorithms
Round-robin
Weighted round-robin (WRR)
Least connections
Weighted least connections
URL hashing
Source IP hashing (configurable mask)
Destination IP hashing (configurable mask)
Source and Destination IP hashing (configurable mask)
Configurable pending connection timeout
Load Balancing Supported
Server load balancing (TCP, UDP, or generic IP protocols)
Firewall load balancing

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

CHAPTER 1

Overview

The Catalyst 6500 series Content Switching Module (CSM) provides high-performance server load balancing (SLB) among groups of servers, firewalls, caches, VPN termination devices, and other network devices, based on Layer 3 as well as Layer 4 through Layer 7 packet information. Server farms are groups of load balanced devices.

Server farms that are represented as virtual servers can improve scalability and availability of services for your network. You can add new servers and remove failed or existing servers at any time without affecting the virtual server's availability.

Clients connect to the CSM directing their requests to the virtual IP (VIP) address of the virtual server. When a client initiates a connection to the virtual server, the CSM chooses a real server (a physical device that is assigned to a server farm) for the connection based on configured load-balancing algorithms and policies (access rules). Policies manage traffic by defining where to send client connections.

Sticky connections limit traffic to individual servers by allowing multiple connections from the same client to *stick* to the same real server using source IP addresses, source IP subnets, cookies, and the secure socket layer (SSL) or by redirecting these connections using Hypertext Transfer Protocol (HTTP) redirect messages.

Caution The WS-X6066-SLB-APC Content Switching Module is not fabric enabled.

These sections describe the CSM:

Features

The CSM provides these enhanced features:

- More than one CSM can run in a Catalyst 6500 series switch chassis, and CSMs can run concurrently with Cisco IOS server load balancing (SLB).
- CSM fault-tolerance support allows two CSM modules (in the same or in different chassis) to be configured in the active and standby modes.

- The sticky database and connection table also can be replicated from active to standby to minimize any service disruption.
- CSM firewall load balancing allows you to scale firewall protection. Multiple firewall farms and DMZs are supported.
- A configurable pending-connection timeout feature is available. Pending-connection timeout sets the response time for terminating connections if a switch is flooded with traffic. This feature is used to prevent denial of service (DOS) attacks. Pending connections are configurable on a per virtual server basis.
- The CSM supports 255 VLANs (including the client VLANs, server VLANs and one fault tolerant VLAN used for redundant pairs of CSMs).
- The minimum time between health probes has been reduced to 2 seconds, starting from release 2.1(1).
- Sample scripts are available for reference to support the TCL (Toolkit Command Language) feature. The filename is: c6slb-script.3-1-1a.tcl. This file is located with the CSM Release 3.1(1a) software image at this URL:

Table 1-1 lists the new CSM features in this release.

Table 1-1 New CSM Feature Set Description

New Features New in this Release	Description
VIP connection watermarks	Allow you to limit the number of connections going through a particular virtual server.
Sorry server (backup serverfarm)	Allows you to specify one or more backup servers for use when all primary servers are disabled or out-of-service.
Optional port for health probes	Sets an explicit server port for a probe.
IP reassembly	Attempts reassembly of UDP fragments, even if the first fragment is not received first.
TCL (Toolkit Command Language) scripting	Supports more flexible health probe functionality using administrator-created probe scripts.
XML configuration interface	Allows programmatic configuration of the CSM by a network management device.
SNMP	Does support the CISCO-SLB-MIB and CISCO-SLB-EXT-MIB.
GSLB	Enables global server load balancing.
Resource usage display	Displays resource usage.
Idle timeout for unidirectional flows	Allows uni-directional timeouts for RTSP and other streaming protocols.
SSL termination engine (STE) integration for secure socket layer (SSL) load balancing	Ensures the SSL client is repeatedly connected to the same SSL server, including during SSL ID renegotiation.
HTTP method parsing	Allows HTTP method parsing.

Table 1-1 New CSM Feature Set Description (continued)

New Features New in this Release	Description
Regular expression scalability improvements	Allows more scalable HTTP matching using regular expressions
Real server names	Allows you to name individual real servers. Names can then be used within serverfarms to reference a specific real server.
Non-TCP connection redundancy	Allows non-TCP flows replication to the standby CSM if connection redundancy is configured.
FT show command enhancements	The command displays additional information.
IOS SLB FWLB interoperation (IP reverse-sticky)	Allows you to create reverse sticky entries, allowing firewall load balancing sandwich topologies with IOS SLB.
Slowpath performance improvements	Improves the performance of health probing, configuration changes, and the ability of the CSM to handle ARP traffic. The new XML configuration and TCL scripting features in this release also benefit from this improvement.

Table 1-2 lists the CSM features available in this release and previous releases.

Table 1-2 CSM Feature Set Description

Features
Supported Hardware
Supervisor 1A with MSFC and PFC
Supervisor 2 with MSFC and PFC
Supported Protocols
TCP load balancing
UDP and all common IP protocol load balancing
Special application-layer support for FTP and the Real Time Streaming Protocol (RTSP)
Layer 7 Functionality
Full regular expression matching
URL and cookie switching
Generic HTTP header parsing
Miscellaneous Functionality
VIP connection watermarks
Sorry server
Optional port for health probes
IP reassembly
TCL (Toolkit Command Language) scripting

Table 1-2 CSM Feature Set Description (continued)

Features
XML configuration interface
SNMP
GSLB (Global Server Load Balancing)
Resource usage display
Idle timeout for unidirectional flows
STE integration for SSL load balancing
HTTP method parsing
Regular expression scalability improvements
Real server names
Non-TCP connection redundancy
FT show command enhancements
IOS SLB FWLB interoperation (IP reverse-sticky)
Slowpath performance improvements
Multiple CSMs in a chassis
CSM and IOS-SLB functioning simultaneously in a chassis
HTTP 1.1 persistence (all GETs to the same server)
Full HTTP 1.1 persistence (GETs balanced to multiple servers)
Fully configurable NAT
Server initiated connections
Route health injection
Load-balancing Algorithms
Round-robin
Weighted round-robin (WRR)
Least connections
Weighted least connections
URL hashing
Source IP hashing (configurable mask)
Destination IP hashing (configurable mask)
Source and Destination IP hashing (configurable mask)
Configurable pending connection timeout
Load Balancing Supported
Server load balancing (TCP, UDP, or generic IP protocols)
Firewall load balancing

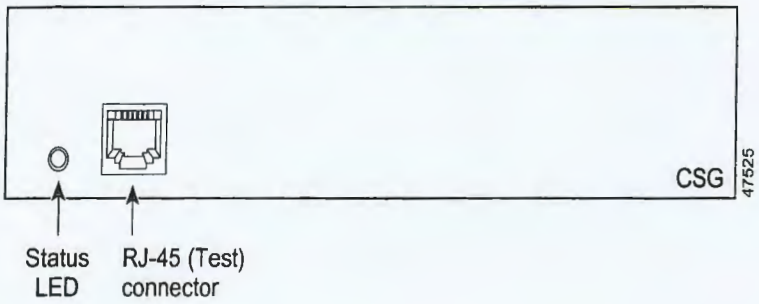
Table 1-2 CSM Feature Set Description (continued)

Features
DNS load balancing
Stealth firewall load balancing
Transparent cache redirection
Reverse proxy cache
SSL off-loading
VPN-Ipsec load balancing
Stickiness
Cookie
SSL ID
Source IP (configurable mask)
HTTP redirection
Redundancy
Sticky state
Full stateful failover (connection redundancy)
Health Checking
HTTP
ICMP
Telnet
TCP
FTP
SMTP
DNS
Return error code checking
Inband health checking
User-defined TCL scripts
Management
SNMP traps
Full SNMP and MIB support

Front Panel Description

Figure 1-1 shows the CSM front panel.

Figure 1-1 Content Switching Module Front Panel



Note The RJ-45 connector is covered by a removable plate.

Status LED

When the CSM powers up, it initializes various hardware components and communicates with the supervisor engine. The Status LED indicates the supervisor engine operations and the initialization results. During the normal initialization sequence, the status LED changes from off to red, orange, and green.

Note For more information on the supervisor engine LEDs, refer to the *Catalyst 6500 Series Module Installation Guide*.

Table 1-3 describes the Status LED operation.

Table 1-3 Content Switching Module Status LED

Color	Description
Off	• The module is waiting for the supervisor engine to provide power. • The module is not on line. • The module is not receiving power, which could be caused by the following: – Power is not available to the CSM. – Module temperature is over the limit[1].
Red	• The module is released from reset by the supervisor engine and is booting. • If the boot code fails to execute, the LED stays red after power up.

Table 1-3 Content Switching Module Status LED (continued)

Color	Description
Orange	• The module is initializing hardware or communicating with the supervisor engine. • A fault occurred during the initialization sequence. • The module has failed to download its Field Programmable Gate Arrays (FPGAs) on power up but continues with the remainder of the initialization sequence and provides the module online status from the supervisor engine. • The module has not received module online status from the supervisor engine. This problem could be caused by the supervisor engine detecting a failure in an external loopback test that it issued to the CSM.
Green	• The module is operational; the supervisor engine has provided module online status.
Green to orange	• The module is disabled through the supervisor engine CLI [2] using the **set module disable** *mod* command.

1. Enter the **show environment temperature** *mod* command to display the temperature of each of four sensors on the CSM.
2. CLI = command-line interface.

RJ-45 Connector

The RJ-45 connector, which is covered by a removable plate, is used to connect a management station device or a test device. This connector is used by field engineers to perform testing and to obtain dump information.

Operation Mode

Clients and servers communicate through the CSM using Layer 2 and Layer 3 technology in a specific VLAN configuration. (See Figure 1-2.) In a simple SLB deployment, clients connect to the client-side VLAN and servers connect to the server-side VLAN. Servers and clients can exist on different subnets. Servers can also be located one or more Layer 3 hops away and connect to the CSM through routers.

A client sends a request to one of the module's VIP addresses. The CSM forwards this request to a server that can respond to the request. The server then forwards the response to the CSM, and the CSM forwards the response to the client.

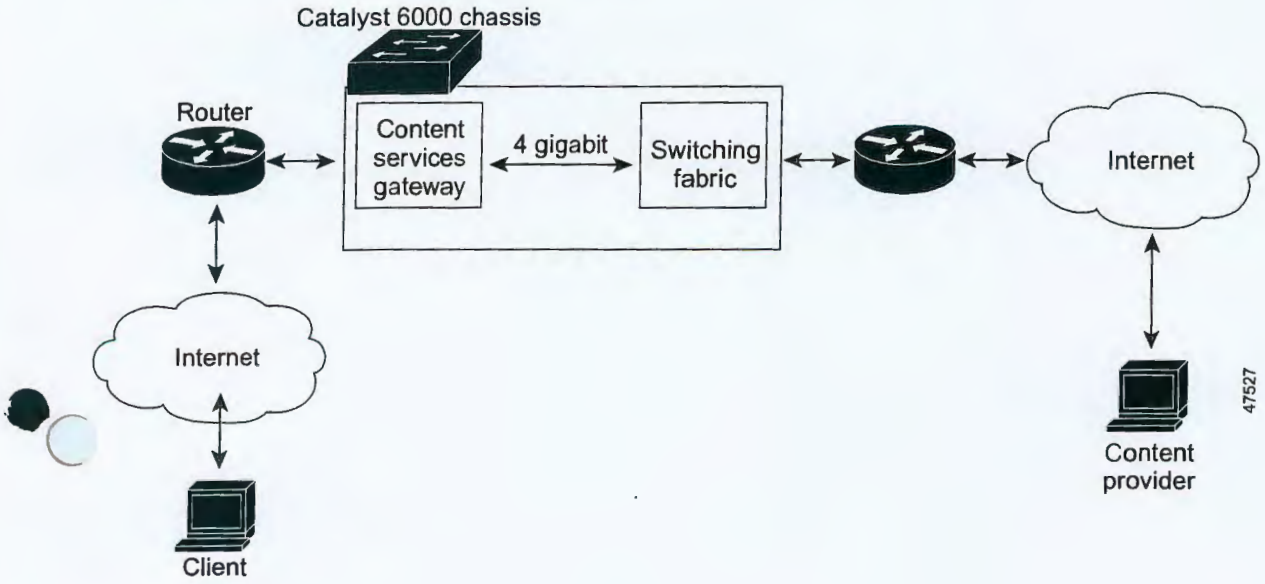
When the client-side and server-side VLANs are on the same subnets, you can configure the CSM in single subnet (bridge) mode. For more information, see the "Configuring the Single Subnet (Bridge) Mode" section on page 4-2.

When the client-side and server-side VLANs are on different subnets, you can configure the CSM to operate in a secure (router) mode. For more information, see the "Configuring the Secure (Router) Mode" section on page 4-4.

You can set up a fault-tolerant configuration in either the secure (router) or single subnet (bridged) mode using redundant CSMs. For more information, see the "Configuring Fault Tolerance" section on page 4-5.

Using multiple VLANs, single subnet (bridge) mode and secure (router) mode can coexist in the same CSM.

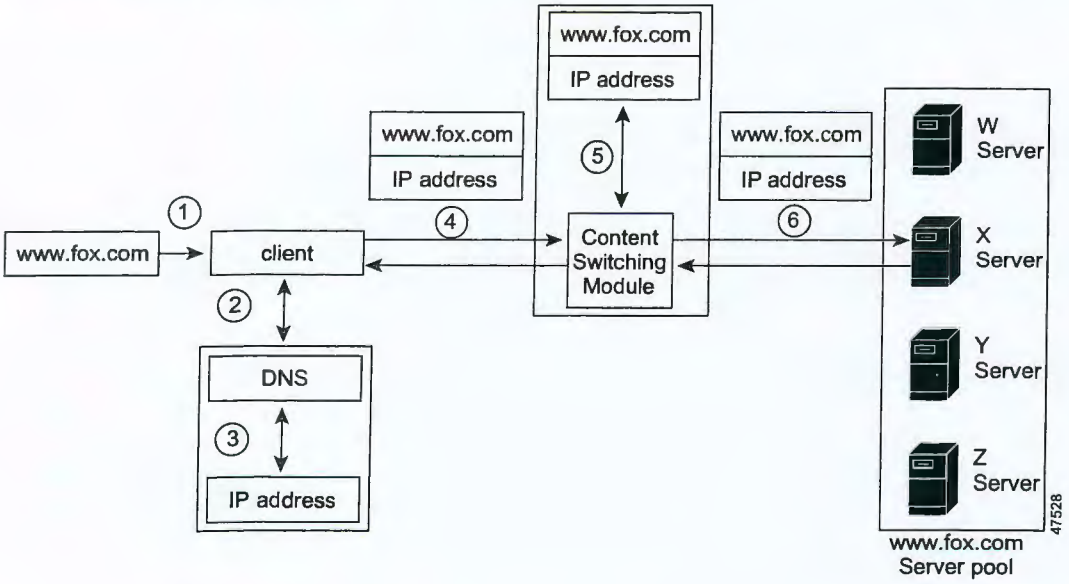
Figure 1-2 Content Switching Module and Servers



Traffic Flow

This section describes how the traffic flows between the client and server in a CSM environment. (See Figure 1-3.)

Figure 1-3 Traffic Flow between Client and Server



Note The numbers in Figure 1-3 correspond to the steps in the following procedure.

When you enter a request for information by entering a URL, the traffic flows as follows:

1. You enter a URL. (Figure 1-3 shows www.fox.com as an example.)
2. The client contacts a DNS server to locate the IP address associated with the URL.
3. The DNS server sends the IP address of the virtual IP (VIP) to the client.
4. The client uses the IP address (CSM VIP) to send the HTTP request to the CSM.
5. The CSM receives the request with the URL, makes a load-balancing decision, and selects a server.

   For example, in Figure 1-3, the CSM selects a server (X server) from the www.fox.com server pool, replacing its own VIP address with the address of the X server (directed mode), and forwards the traffic to the X server. If the NAT server option is disabled, the VIP address remains unchanged (dispatch mode).
6. The CSM performs Network Address Translation (NAT) and eventually TCP sequence numbers translation.

Product Overview

This chapter describes the Catalyst 6000 series switches, the Catalyst 6500 series switches, supervisor engines, and switching modules. This chapter contains these sections:

Catalyst 6000 Series Switches

The Catalyst 6000 series switches consist of the following two chassis:

- Catalyst 6006 (6 slots)
- Catalyst 6009 (9 slots)

These high-performance, modular, frame-based switches support high-density Fast Ethernet and Gigabit Ethernet in both campus-backbone and server-aggregation environments. The Catalyst 6006 and the Catalyst 6009 switches have a 32-Gbps switching capacity. Both platforms share the same supervisor engines, switching modules, and software, and they support redundant configurations of supervisor engines, power supplies, and port interfaces.

ATM LAN Emulation (LANE) and Multiprotocol over ATM (MPOA) support is provided by the ATM dual PHY OC-12 LANE/MPOA module.

Note Specific combinations of supervisor engines and modules may not be supported in your chassis. Refer to the release notes of the software version running on your system for specific information on modules and supervisor engine combinations that are not supported.

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.

Note The uplink ports are fully functional on the redundant supervisor engine in standby mode.

The Catalyst 6000 series switches support the following hardware:

- A supervisor engine with two gigabit interface uplinks and an optional redundant supervisor engine

  Note Supervisor Engine 720 is not supported in the Catalyst 6006 and Catalyst 6009 switches.

  Both supervisor engines in a single chassis must be completely identical. You can configure the redundant supervisor engines in a Catalyst 6000 series 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
- Additional switching modules (Ethernet, Fast Ethernet, Gigabit Ethernet, and ATM) in any combination
  - Five additional switching modules in the Catalyst 6006
  - Eight additional switching modules in the Catalyst 6009

  Note The Switch Fabric Modules are not supported in the Catalyst 6000 series switches.

- Hot-swappable fan assembly and modules
- Redundant AC-input or DC-input power supplies
- Backplane bandwidth of 32 Gbps

Catalyst 6500 Series Switches

The Catalyst 6500 series switches consist of the following five chassis:

- Catalyst 6503 (3 slots)
- Catalyst 6506 (6 slots)
- Catalyst 6509 (9 slots)
- Catalyst 6509-NEB (9 slots, vertical)
- Catalyst 6513 (13 slots)

The Catalyst 6506, Catalyst 6509, Catalyst 6509-NEB, and Catalyst 6513 switches can support a backplane architecture that scales from 32 Gbps to 256 Gbps. The Catalyst 6503 switch backplane architecture is limited to 32 Gbps.

The Catalyst 6500 series switches support the following hardware:

- A supervisor engine with two gigabit interface uplinks and an optional redundant supervisor engine.

  Note The Supervisor Engine 720 also has a 10/100/1000 Mbps uplink port.

  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 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 Catalyst 6513 switch requires either the Supervisor Engine 2 or Supervisor Engine 720.

- Additional switching modules in any combination:
  - Two additional switching modules in the Catalyst 6503 switch
  - Five additional switching modules in the Catalyst 6506 switch
  - Eight additional switching modules in the Catalyst 6509 and Catalyst 6509-NEB switches
  - Twelve additional switching modules in the Catalyst 6513 switch

Note Specific combinations of supervisor engines and modules may not be supported in your chassis. Refer to the release notes of the software version running on your system for specific information on modules and supervisor engine combinations that are not supported.

- Hot-swappable fan assembly and modules

Note For a Supervisor Engine 720, you need to install a high-speed fan tray and install a 2500 W or larger power supply.

- Redundant AC-input or DC-input power supplies
- Scalable backplane bandwidth of 32 Gbps, up to 256 Gbps
- A Switch Fabric Module (WS-C6500-SFM or WS-X6500-SFM2)
  - Only the Supervisor Engine 2 supports the Switch Fabric Module.
  - Supervisor Engine 720 does not support the Switch Fabric Modules.
  - Either the WS-C6500-SFM or WS-X6500-SFM2 Switch Fabric Module can be installed in slot 5 of the Catalyst 6506, Catalyst 6509, and Catalyst 6509-NEB switches. A redundant Switch Fabric Module can be installed in slot 6.
  - Only the WS-X6500-SFM2 Switch Fabric Module can be installed in slot 7 of the Catalyst 6513 switch. A redundant WS-X6500-SFM2 Switch Fabric Module can be installed in slot 8.

Note For redundancy, you can install a redundant Switch Fabric Module. The module that is installed first functions as the primary module. When you install two Switch Fabric Modules at the same time, the module in slot 5 or slot 7 acts as the primary module, and the module in slot 6 or slot 8 acts as the backup. If you reset the module in slot 5 or slot 7, the module in slot 6 or slot 8 becomes the primary module.

- A combination of an SFM (WS-C6500-SFM) with an SFM2 (WS-X6500-SFM2) in the same Catalyst 6506, Catalyst 6509, or Catalyst 6509-NEB chassis

Table 1-1 lists some key features of the Catalyst 6500 series switches.

Table 1-1 Catalyst 6500 Series Switches Key Features

Feature	Description
Performance and Configuration	Refer to the *Catalyst 6500 Series Switch Software Configuration Guide* or the *Catalyst 6500 Series Switch Cisco IOS Software Configuration Guide* for detailed information about the features supported on the switches.
Supervisor Engine 1 and Supervisor Engine 2	• Modular, upgradable feature modules for core switching logic. • Two modular Gigabit Ethernet ports supporting GBICs[1]. • MSFC[2] and PFC[3]supported. • PCMCIA slot. • Console port for terminal and modem access.
Fault Tolerance and Redundancy	• Support for two hot-swappable supervisor engines. • Fast switchover for redundant supervisor engine and switching modules. • Support for two fully redundant AC- or DC-input, load-sharing power supplies. • Power management for modules and power supplies. • Environmental monitoring of critical system components. • Hot-swappable fan assembly. High-speed fan tray also available[4]. • Redundant clock modules.

Table 1-1 Catalyst 6500 Series Switches Key Features (continued)

Feature	Description
Component Hot-Swapping	Modules (including the supervisor engine if you have redundant supervisor engines) and fans can be replaced without interrupting the system power or causing other software or interfaces to shut down.
Memory Components	• 512-KB NVRAM stores configuration information. • EEPROM[5] component on the supervisor engine stores module-specific information, such as the module serial number, part number, controller type, hardware revision, configuration information, and other details unique to each module. • 128-MB DRAM (Supervisor Engine 1A), 128-MB DRAM (Supervisor Engine 2), 256-MB DRAM (Supervisor Engine 2U), or 512-MB DRAM (Supervisor Engine 720) for the default system software. • 16-MB (Supervisor Engine 1), 32-MB (Supervisor Engine 2), or 64-MB (Supervisor Engine 720) Flash memory stores and runs software images. • PC Flash—One or two slots for an optional Flash PC card, Compact Flash card, or MicroDrive; use this additional memory to store and run software images and configuration files, or to serve as an I/O device. • Flash file system—Flash memory contains a file system. You can use a variety of commands to manage the file system (such as **cd**, **pwd**, **dir**, and **delete**). The file system includes the following devices: – Onboard bootflash – PC Flash slot
Management	• CLI through the console port or Telnet • Simple Network Management Protocol

1. GBICs = Gigabit Interface Converters
2. MSFC = Multilayer Switch Feature Card
3. PFC = Policy Feature Card
4. The high-speed fan tray is required if you install a Supervisor Engine 720. The high-speed fan tray requires that a 2500 W or larger power supply be installed in the chassis.
5. EEPROM = electrically erasable programmable read-only memory

Supervisor Engines

This section describes the features found on Supervisor Engine 1, Supervisor Engine 2, and Supervisor Engine 720. This section contains the following topics:

Note The Catalyst 6513 switch requires a Supervisor Engine 2 or Supervisor Engine 720.

The supervisor engine configurations are listed in Table 1-2.

Table 1-2 Supervisor Engines

Product Number	Description
Supervisor Engine 1[1]	
WS-X6K-SUP1-2GE	• Supervisor Engine 1, dual 1000BASE-X GBIC uplinks • QoS port architecture (Rx/Tx) is **1q4t/2q2t**
WS-X6K-SUP1A-2GE	• Supervisor Engine 1A, dual 1000BASE-X GBIC uplinks • QoS port architecture (Rx/Tx) is **1p1q4t/1p2q2t**
WS-X6K-S1A-MSFC2	• Supervisor Engine 1A, dual 1000BASE-X GBIC uplinks, PFC and MSFC2 daughter cards • QoS port architecture (Rx/Tx) is **1p1q4t/1p2q2t**

Table 1-2 Supervisor Engines (continued)

Product Number	Description
WS-X6K-SUP1A-MSFC	• Supervisor Engine 1A, dual 1000BASE-X GBIC uplinks, PFC and MSFC daughter cards • QoS port architecture (Rx/Tx) is **1p1q4t/1p2q2t**
WS-XSUP1A-PFC	• Supervisor Engine 1A, dual 1000BASE-X GBIC uplinks, PFC daughter card • QoS port architecture (Rx/Tx) is **1p1q4t/1p2q2t**
Supervisor Engine 2	
WS-X6K-S2-MSFC2	• Supervisor Engine 2, dual 1000BASE-X GBIC uplinks, fabric-enabled, supports a PFC2 and an MSFC2, 128 MB on supervisor engine, 128 MB on MSFC2 • QoS port architecture (Rx/Tx) is **1p1q4t/1p2q2t**
WS-X6K-S2U-MSFC2	• Supervisor Engine 2, dual 1000BASE-X GBIC uplinks, fabric-enabled, supports a PFC2 and an MSFC2, 256 MB on supervisor engine, 256 MB on MSFC2 • QoS port architecture (Rx/Tx) is **1p1q4t/1p2q2t**
WS-X6K-S2-PFC2	• Supervisor Engine 2, dual 1000BASE-X GBIC uplinks, fabric-enabled, and supports a PFC2 • QoS port architecture (Rx/Tx) is **1p1q4t/1p2q2t**

Table 1-2 Supervisor Engines (continued)

Product Number	Description
Supervisor Engine 720	
Supervisor Engine 720[2]	• Two Ethernet uplink ports: port 1 supports gigabit Small Form-Factor Pluggable (SFP) module; port 2 configurable with either a gigabit SFP or a 10/100/1000 Mbps RJ-45 • Integrated 720-Gbps Switch Fabric • 2 CompactFlash Type II slots (DISK 0 and DISK 1) • Must be installed in slots 5 or 6 in a 6-slot and a 9-slot chassis, and slots 7 or 8 in a 13-slot chassis • Requires installation of a high-speed fan tray • Policy Feature Card 3A (PFC3A) • Multilayer Switch Feature Card 3 (MSFC3) with 64-MB bootflash device and 512-MB DRAM • QoS port architecture (Rx/Tx) is **1p1q4t/1p2q2t**

1. Supervisor Engine 1 is not supported in the Catalyst 6513 switch.
2. Specific combinations of supervisor engines and modules may not be supported in your chassis. Refer to the release notes of the software version running on your system for specific information on modules and supervisor engine combinations that are not supported.

Figure 1-1 shows the front panel features of Supervisor Engine 1, Figure 1-2 shows the front panel features of Supervisor Engine 2, and Figure 1-3 shows the front panel features of the Supervisor Engine 720.

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:

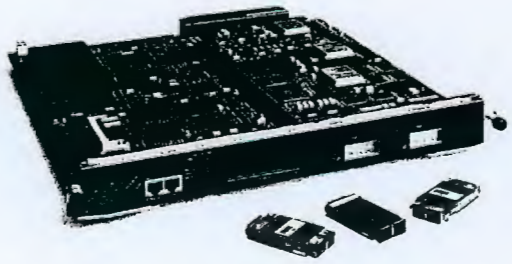
- *Feature-rich and wire-rate intelligent network services*—Support and complement comprehensive security and granular Quality of Service mechanisms, including identity-based networking capabilities based on IEEE 802.1x extensions and simplified configuration using two AutoQoS commands
- *End-to-end 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

- *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

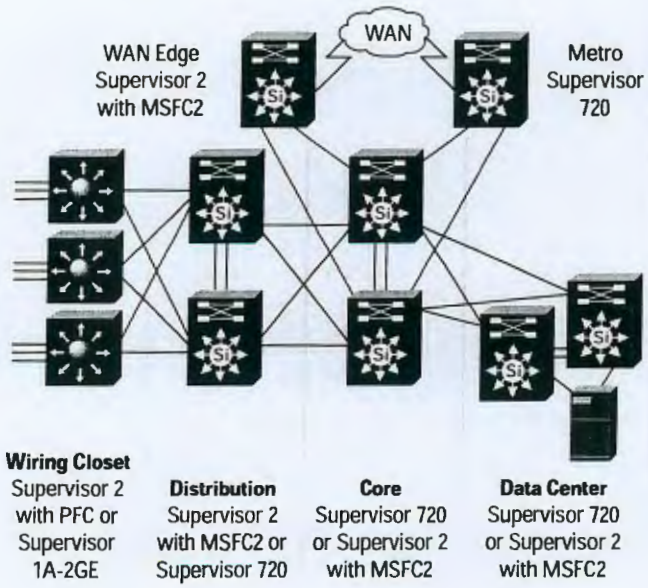


Supervisor Engine 2-MSFC2

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



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

9-roteamento

Product Overview - Scalable Performance

12849 E

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.

RQS nº 03/2005 - CN - CPMI - CORREIOS
0270
Fls. Nº
Doc: 3696

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.

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.

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

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

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.

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.

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

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:

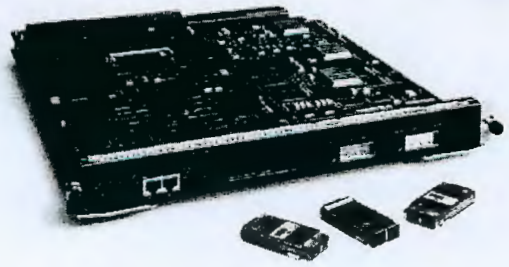
- *Layer 2 forwarding*—Performs Layer 2 forwarding with Layer2, 3, 4 features; requires MSFC2 upgrade to support Layer 3, 4 forwarding
- *MAC addresses*—128K
- *Forwarding rate*—Up to 30 Mpps per system
- *Bandwidth*—32 Gbps per system; 256 Gbps with SFM in chassis
- *Layer 2, 3 traffic classification 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

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

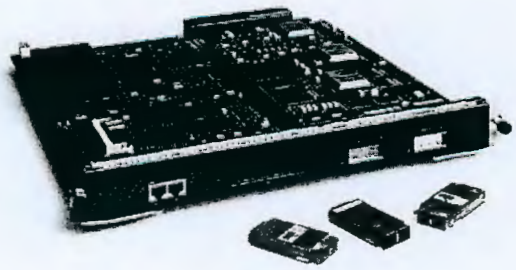


Supervisor Engine 1A-PFC

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



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

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.

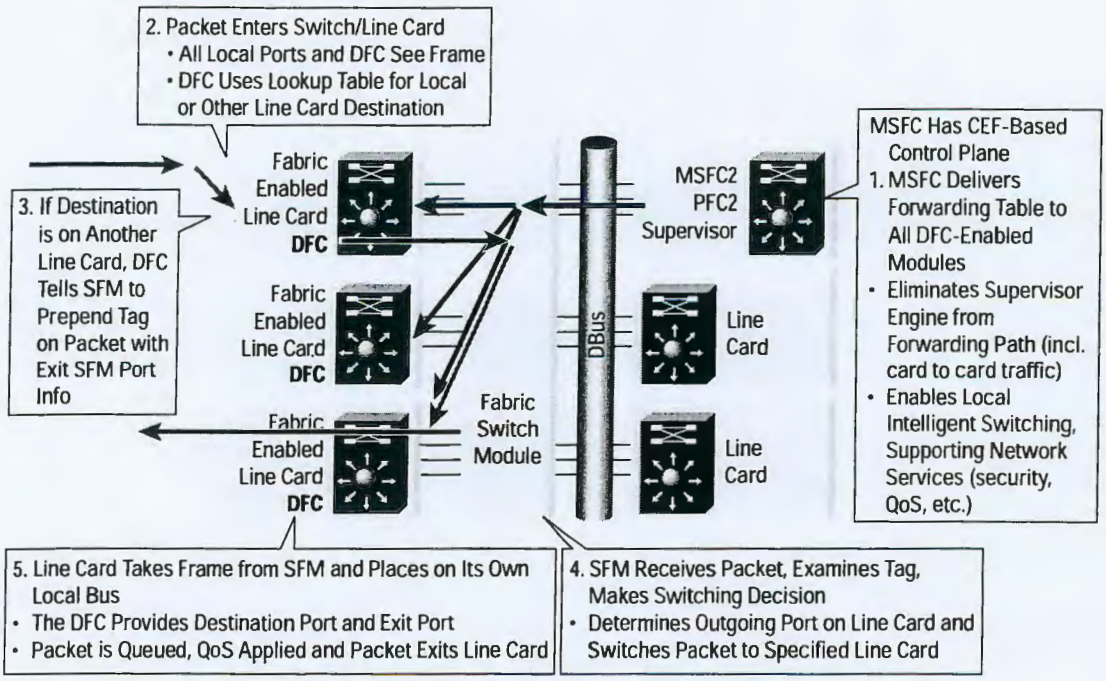
How Distributed Cisco Express Forwarding (dCEF) Works

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.

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.

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

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

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

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

203070/FTMG_07/03

Cisco Systems

White Paper

Buffers, Queues, and Thresholds on Cisco Catalyst **6500** Series Ethernet Modules

With the wide variety of Ethernet modules currently available on the Catalyst® 6500 Series switches, determining the size of the port buffers, the number and type of the receive and transmit queues, and the number of tail-drop or weighted random early detection (WRED) thresholds can be a daunting task. This document provides a brief discussion of how the port buffers, queues, and thresholds are used in the Catalyst 6500 Series Switch Ethernet modules, and then describes the buffer sizes, queue structures, and thresholds supported on each of the modules.

Note: This document does not discuss any of the Cisco 7600 optical services modules (OSMs) that are also supported in the Catalyst 6500 Series switches.

Overview of Buffers, Queues, and Thresholds

All the Catalyst 6500 Series Ethernet modules implement some form of receive and transmit buffering. These buffers are used to store frames as forwarding decisions are made within the switch, or as packets are enqueued for transmission on a port at a rate greater than the physical medium can support.

In the Catalyst 6500 architecture, access into the switch fabric is almost never the bottleneck. Rather, on the transmit side, one or several ports are the likely destination for a majority of the packets entering the switch. As such, the receive-side port buffers on the Ethernet modules are relatively small compared to the transmit-side port buffers.

Without quality-of-service (QoS) features enabled, all packets have equal access to the port buffers, regardless of the type of traffic. For example, voice-over-IP (VoIP) packets get placed in the same buffer as HTTP (Web) or FTP (file download) data packets. Furthermore, in the event of congestion (that is, a port buffer overflows), all traffic is equally subject to discard. To summarize, packets are serviced in the order in which they were received, and if the buffer is full, all subsequent packets are dropped. This is known as First In, First Out (FIFO) queuing with tail-drop.

When you enable QoS on the switch, the port buffers are divided into one or more individual queues. Each queue has one or more drop thresholds associated with it. The combination of multiple queues within a buffer, and the drop thresholds associated with each queue, allow the switch to make intelligent decisions when experiencing congestion. Traffic sensitive to jitter and delay variance, such as VoIP packets, can be moved to the head of the queue for transmission, while other less important or less sensitive traffic can be buffered or dropped.

Port Queue and Drop Threshold Types

When QoS is enabled, the multiple queues and drop thresholds on the Ethernet module switch ports are enabled. There are several different configurations of queue types and thresholds, depending on the model of the Ethernet module.

Ingress and egress scheduling are always based on the class-of-service (CoS) value associated with the frame. By default, higher CoS values are mapped to higher queue numbers. CoS 5 traffic, typically associated with VoIP traffic, is mapped to the strict priority queue, if present.

In addition to the different queues, each standard queue has one or more drop thresholds. There are two types of drop thresholds:

- *Tail-drop thresholds*—On ports with tail-drop thresholds, frames of a given CoS value are admitted to the queue until the drop threshold associated with that CoS value is exceeded; subsequent frames of that CoS value are discarded until the threshold is no longer exceeded.

  For example, if CoS 1 is assigned to queue 1, threshold 2, and the threshold 2 watermark is 60 percent, frames with CoS 1 will not be dropped until queue 1 is 60 percent full. All subsequent CoS 1 frames are dropped until the queue is less than 60 percent full.
- *WRED-drop thresholds*—On ports with WRED-drop thresholds, frames of a given CoS value are admitted to the queue based on a random probability designed to avoid buffer congestion. The probability of a frame with a given CoS being admitted to the queue or discarded depends on the weight and threshold assigned to that CoS value.

  For example, if CoS 2 is assigned to queue 1, threshold 2, and the threshold 2 watermarks are 40 percent (low) and 80 percent (high), frames with CoS 2 will not be dropped until queue 1 is at least 40 percent full. As the queue depth approaches 80 percent, frames with CoS 2 have an increasingly higher probability of being discarded rather than being admitted to the queue. When the queue is more than 80 percent full, all CoS 2 frames are dropped until the queue is less than 80 percent full. The frames that the switch discards when the queue level is between the low and high thresholds are picked at random, rather than on a per-flow or FIFO basis. This method works well with protocols such as TCP which are capable of adjusting to periodic packet drops by backing off and adjusting their transmission window size.

When referring to the individual queues and thresholds on a port, a terse nomenclature is used. This terminology describes the number of strict priority queues (if present), the number of standard queues, and the number of tail-drop or WRED thresholds within each of the standard queues. The different queue and threshold types on the Catalyst 6500 Series Ethernet modules are shown in Table 1.

Table 1 Receive and Transmit Port Queue and Drop Threshold Types on Catalyst 6500 Series Ethernet Modules

Port Queue and Drop Threshold Structure with QoS	Description
Receive Queues	
1q4t	One standard queue with four tail-drop thresholds
1p1q4t	One strict-priority queue, one standard queue with four tail-drop thresholds
1p1q0t	One strict-priority queue, one standard queue with one nonconfigurable (100%) tail-drop threshold
1p1q8t	One strict-priority queue, one standard queue with eight configurable WRED-drop thresholds and one nonconfigurable (100%) tail-drop threshold
Transmit Queues	
2q2t	Two standard queues with two tail-drop thresholds per queue
1p2q2t	One strict-priority queue, two standard queues with two WRED-drop thresholds per queue
1p3q1t	One strict-priority queue, three standard queues with one WRED-drop threshold and one nonconfigurable tail-drop threshold per queue
1p2q1t	One strict-priority queue, two standard queues with one WRED-drop threshold and one nonconfigurable (100%) tail-drop threshold per queue

Buffer Sizes, Queues, and Thresholds by Ethernet Module

Table 2 provides the following information for each of the Catalyst 6500 Series Ethernet modules:

- Total buffer size per port (Total buffer size)
- Overall receive buffer size per port (Rx buffer size)
- Overall transmit buffer size per port (Tx buffer size)
- Port receive queue and drop threshold structure (Rx port type)
- Port transmit queue and drop threshold structure (Tx port type)
- Default size of receive buffers per queue with QoS enabled (Rx queue sizes)
- Default size of transmit buffers per queue with QoS enabled (Tx queue sizes)

Table 2 Buffer Sizes, Queues, and Thresholds by Ethernet Module

Module Model Name	Module Description	Total Buffer Size	Rx Buffer Size	Tx Buffer Size	Rx Port Type	Tx Port Type	Rx Queue Sizes	Tx Queue Sizes
Supervisor Engine Modules (Gigabit Ethernet uplink ports)								
WS-X6K-S2U-MSFC2 WS-X6K-S2-MSFC2 WS-X6K-S2-PFC2	All Supervisor Engine 2 uplink ports	512 KB	73 KB	439 KB	1p1q4t	1p2q2t	SP—9 KB Q1—64 KB	SP—64 KB Q2—64 KB Q1—311 KB
WS-X6K-S1A-MSFC2 WS-X6K-SUP1A-MSFC WS-X6K-SUP1A-PFC WS-X6K-SUP1A-2GE	All Supervisor Engine 1A uplink ports	512 KB	73 KB	439 KB	1p1q4t	1p2q2t	SP—9 KB Q1—64 KB	SP—64 KB Q2—64 KB Q1—311 KB
WS-X6K-SUP1-2GE	Supervisor Engine 1 uplink ports	512 KB	80 KB	432 KB	1q4t	2q2t	Q1—80 KB	Q2—80 KB Q1—352 KB
Ethernet and Fast Ethernet Modules								
S-X6524-100FX-MM	24-port 100BASE-FX fabric-enabled with MT-RJ connectors	1116 KB	28 KB	1088 KB	1p1q0t	1p3q1t	SP—6 KB Q1—22 KB	SP—272 KB Q3—272 KB Q2—272 KB Q1—272 KB
WS-X6548-RJ-21	48-port 10/100BASE-TX fabric-enabled with RJ-21 connectors	1116 KB	28 KB	1088 KB	1p1q0t	1p3q1t	SP—6 KB Q1—22 KB	SP—272 KB Q3—272 KB Q2—272 KB Q1—272 KB
WS-X6548-RJ-45	48-port 10/100BASE-TX fabric-enabled with RJ-45 connectors	1116 KB	28 KB	1088 KB	1p1q0t	1p3q1t	SP—6 KB Q1—22 KB	SP—272 KB Q3—272 KB Q2—272 KB Q1—272 KB
WS-X6324-100FX-MM	24-port 100BASE-FX with MT-RJ connectors	128 KB	16 KB	112 KB	1q4t	2q2t	Q1—16 KB	Q2—22 KB Q1—90 KB
WS-X6324-100FX-SM	24-port 100BASE-FX with MT-RJ connectors	128 KB	16 KB	112 KB	1q4t	2q2t	Q1—16 KB	Q2—22 KB Q1—90 KB
-X6348-RJ-45	48-port 10/100BASE-TX with RJ-45 connectors	128 KB	16 KB	112 KB	1q4t	2q2t	Q1—16 KB	Q2—22 KB Q1—90 KB
WS-X6348-RJ21V	48-port 10/100BASE-TX with RJ-21 connectors and inline power	128 KB	16 KB	112 KB	1q4t	2q2t	Q1—16 KB	Q2—22 KB Q1—90 KB
WS-X6348-RJ-45V	48-port 10/100BASE-TX with RJ-45 connectors and inline power	128 KB	16 KB	112 KB	1q4t	2q2t	Q1—16 KB	Q2—22 KB Q1—90 KB
WS-X6224-100FX-MT	24-port 100BASE-FX with MT-RJ connectors	64 KB	8 KB	56 KB	1q4t	2q2t	Q1—8 KB	Q2—16 KB Q1—40 KB

Table 2 Buffer Sizes, Queues, and Thresholds by Ethernet Module

Module Model Name	Module Description	Total Buffer Size	Rx Buffer Size	Tx Buffer Size	Rx Port Type	Tx Port Type	Rx Queue Sizes	Tx Queue Sizes
WS-X6248-RJ-45	48-port 10/100BASE-TX with RJ-45 connectors	64 KB	8 KB	56 KB	1q4t	2q2t	Q1—8 KB	Q2—16 KB Q1—40 KB
WS-X6248-TEL	48-port 10/100BASE-TX with RJ-21 connectors	64 KB	8 KB	56 KB	1q4t	2q2t	Q1—8 KB	Q2—16 KB Q1—40 KB
WS-X6248A-TEL	48-port 10/100BASE-TX with RJ-21 connectors	128 KB	16 KB	112 KB	1q4t	2q2t	Q1—16 KB	Q2—22 KB Q1—90 KB
WS-X6148-RJ-45V	48-port 10/100BASE-TX with RJ-45 connectors and inline power	128 KB	16 KB	112 KB	1q4t	2q2t	Q1—16 KB	Q2—22 KB Q1—90 KB
WS-X6148-RJ21V	48-port 10/100BASE-TX with RJ-21 connectors and inline power	128 KB	16 KB	112 KB	1q4t	2q2t	Q1—16 KB	Q2—22 KB Q1—90 KB
WS-X6024-10FL-MT	24-port 10BASE-FL with MT-RJ connectors	64 KB	8 KB	56 KB	1q4t	2q2t	Q1—8 KB	Q2—16 KB Q1—40 KB
Gigabit Ethernet Modules								
WS-X6816-GBIC	16-port 1000BASE-X dual-fabric with GBIC connectors and onboard DFC	512 KB	73 KB	439 KB	1p1q4t	1p2q2t	SP—9 KB Q1—64 KB	SP—64 KB Q2—64 KB Q1—311 KB
WS-X6516-GBIC	16-port 1000BASE-X with GBIC connectors	512 KB	73 KB	439 KB	1p1q4t	1p2q2t	SP—9 KB Q1—64 KB	SP—64 KB Q2—64 KB Q1—311 KB
WS-X6516-GE-TX	16-port 10/100/1000BASE-T with RJ-45 connectors	512 KB	73 KB	439 KB	1p1q4t	1p2q2t	SP—9 KB Q1—64 KB	SP—64 KB Q2—64 KB Q1—311 KB
WS-X6408-GBIC	8-port 1000BASE-X with GBIC connectors	512 KB	80 KB	432 KB	1q4t	2q2t	Q1—80 KB	Q2—80 KB Q1—352 KB
WS-X6408A-GBIC	8-port 1000BASE-X with GBIC connectors	512 KB	73 KB	439 KB	1p1q4t	1p2q2t	SP—9 KB Q1—64 KB	SP—64 KB Q2—64 KB Q1—311 KB
WS-X6416-GBIC	16-port 1000BASE-X with GBIC connectors	512 KB	73 KB	439 KB	1p1q4t	1p2q2t	SP—9 KB Q1—64 KB	SP—64 KB Q2—64 KB Q1—311 KB
WS-X6416-GE-MT	16-port 1000BASE-SX with MT-RJ connectors	512 KB	73 KB	439 KB	1p1q4t	1p2q2t	SP—9 KB Q1—64 KB	SP—64 KB Q2—64 KB Q1—311 KB
WS-X6316-GE-TX	16-port 1000BASE-T with RJ-45 connectors	512 KB	73 KB	439 KB	1p1q4t	1p2q2t	SP—9 KB Q1—64 KB	SP—64 KB Q2—64 KB Q1—311 KB

Table 2 Buffer Sizes, Queues, and Thresholds by Ethernet Module

Module Model Name	Module Description	Total Buffer Size	Rx Buffer Size	Tx Buffer Size	Rx Port Type	Tx Port Type	Rx Queue Sizes	Tx Queue Sizes
10-Gigabit Ethernet Modules								
WS-X6502-10GE	1-port 10 GbE with OIM connectors	64.2 MB	256 KB	64 MB	1p1q8t	1p2q1t	51 KB 205 KB	SP—15.3 MB Q2—17.9 MB Q1—30.7 MB
WS-X6501-10GEX4	1-port 10 GbE with SC connectors	64.2 MB	256 KB	64 MB	1p1q8t	1p2q1t	51 KB 205 KB	SP—15.3 MB Q2—17.9 MB Q1—30.7 MB
Optical Services Modules								
OSM-*	All optical services modules (Layer 2 GE ports only)	512 KB	73 KB	439 KB	1p1q4t	1p2q2t	SP—9 KB Q1—64 KB	SP—64 KB Q2—64 KB Q1—311 KB

is document only discusses the four "standard" Gigabit Ethernet ports present on most of the OSMs. It does not discuss the 4-port GE-WAN OSM or any other OSM-related interfaces.

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

LW4072 01/03

Comprovação das Especificações Exigidas no Edital 050/2003

3.2. Switch tipo 2 (FE)

Switch Tipo 2	
cdccont_0900aecd8009d987.pdf	Cisco Catalyst 2950 Series Switches with Cisco Enhanced Image Software
camp_ds.pdf	CiscoWorks Campus Manager
rwan_op.pdf	CiscoWorks Routed WAN Management Solution 1.3
gbic_ds.pdf	Cisco Systems GigaStack Interface Converter

Cisco Systems

Data Sheet

Cisco Catalyst 2950 Series Switches with Cisco **Enhanced** Image Software

Product Overview

Cisco® Catalyst® 2950 Series switches are fixed-configuration, stackable models that provide wire-speed Fast Ethernet and Gigabit Ethernet connectivity for small and medium-sized 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 Series 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 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 Cisco CMS Software, Cisco Catalyst 2950 Series switches provide extensive management tools using Simple Network Management Protocol (SNMP) network management platforms such as CiscoWorks.

This product line offers two distinct sets of software features and several configurations to allow small, medium-sized, and enterprise branch offices to select the right combination for the network edge. Cisco Standard Image (SI) Software offers Cisco IOS® Software functioning for basic data, video, and voice services. For networks with requirements for additional security, advanced QoS, and high availability, the Cisco 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 Cisco EI Software for the Cisco Catalyst 2950 Series.

- Catalyst 2950G-48—48 10/100 ports and 2 Gigabit Interface Converter (GBIC)-based Gigabit Ethernet ports
- Catalyst 2950G-24—24 10/100 ports and 2 GBIC ports
- Catalyst 2950G-24-DC—24 10/100 ports, 2 GBIC ports, and DC power
- Catalyst 2950G-12—12 10/100 ports and 2 GBIC ports
- Catalyst 2950T-24—24 10/100 ports and 2 fixed 10/100/1000BASE-T uplink ports
- 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, as well as 1000BASE-SX, 1000BASE-LX/LH,

1000BASE-ZX, 1000BASE-T, and coarse-wave division multiplexing (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, Cisco UplinkFast and CrossStack UplinkFast technologies for high-speed uplink and stack interconnection failover, and Per-VLAN Spanning Tree Plus (PVST+) for uplink load balancing.

The Cisco Catalyst 2950T-24 Switch offers small and medium-sized enterprises server connectivity and an easy migration path to Gigabit by using the 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 Series Switch is combined with the Cisco Redundant Power System (RPS) 300 or RPS 675 for 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 Cisco SI Software

The Cisco Catalyst 2950SX-24, 2950-24, and 2950-12 switches are also members of the Cisco Catalyst 2950 Series. They are standalone, fixed-configuration, and managed 10/100 switches providing basic workgroup connectivity for small to medium-sized companies. These wire-speed desktop switches come with Cisco SI Software features and offer Cisco IOS Software functioning for basic data, video, and voice services at the edge of the network.

Cisco Catalyst 2950 Series Long-Reach Ethernet Switches

- *Cisco Catalyst 2950ST-24-LRE*—24 long-reach Ethernet (LRE) ports, 2 fixed 10/100/1000BASE-T ports, and two small form factor pluggable (SFP) ports (2 of the 4 uplinks active at one time)
- *Cisco Catalyst 2950ST-8-LRE*—Eight LRE ports, 2 fixed 10/100/1000BASE-T ports, and two SFP ports (two of the four uplinks active at one time)

The Cisco Catalyst 2950 Series LRE switch solution delivers cost-effective, high-performance broadband access over existing phone wiring in enterprise campus environments and multitenant buildings (hotels, apartment buildings, and office buildings, for example). Cisco Catalyst 2950 Series LRE switches come with Cisco EI Software features, enabling enterprise and service provider customers to extend intelligent services over legacy wiring (Category 1, 2, and 3) to distances up to 5000 feet. Cisco is the only company with technologies that allow customers to deliver intelligent network services across any combination of wired and wireless infrastructures. Refer to the Cisco Catalyst 2950 Series LRE Data Sheet for more information.

Intelligence in the Network

Networks 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 (WLAN) 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 the effective management of 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 high availability, security, scalability, and control. By adding Cisco intelligent functioning 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 fully realize the benefits of adding intelligent services into their networks. Making 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 is critical to further optimizing network operations.

Network Security Through Advanced Security Features

Cisco Catalyst 2950 Series switches offer enhanced data security through numerous 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. These security enhancements are available free of charge by downloading the latest software release for the Cisco Catalyst 3550 and 2950 series switches.

Secure Shell (SSH) and SNMPv3 protect information from tampering or eavesdropping by encrypting information being passed along the network, 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 that it 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 Transmission Control Protocol/User Datagram Protocol (TCP/UDP) ports. ACP lookups are performed in hardware; therefore, forwarding performance is not compromised when implementing this type of security in the network. In addition, time-based access control lists (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 Remote Authentication Dial-In User Service (RADIUS) server, 802.1x provides port-level security. In conjunction with a RADIUS server, 802.1x allows for dynamic port-based user authentication, which can be extended to dynamically

assign a virtual LAN (VLAN) based on a specific user, regardless of where they connect on the network. This intelligent adaptability allows IT departments to offer 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 multilayer Cisco Catalyst 2950 Series switches, network managers can implement high levels of console security. Multilevel access security on the switch console and the Web-based management interface prevent 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 the entire network.

Network Control Through Advanced QoS and Rate Limiting

Cisco Catalyst 2950 Series switches offer superior and highly granular QoS based on Layer 2–4 information to ensure that network traffic is classified and prioritized, and that 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 switches for the appropriate classification and egress queuing. This optimizes traffic prioritization and network availability without the challenge of a complex configuration.

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 DSCP field in the IP packet 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 TCP/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 assigned to the appropriate queue before exiting the switch. 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 a 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 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 or bandwidth-intensive traffic, such as enterprise resource planning (ERP) (Oracle, SAP, and so on), voice (IP telephony traffic), and CAD/CAM over less time-sensitive applications such as File Transfer Protocol (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-effort basis.

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 that require service-level agreements, or when it is necessary for the network manager to control the bandwidth given to certain users. Cisco Catalyst 2950 Series switches support up to 6 policers per Fast Ethernet port and up to 60 policers on a Gigabit Ethernet port, giving the network administrator granular control of LAN bandwidth.

Network Availability

To provide efficient use of resources for bandwidth-hungry applications like multicasts, Cisco Catalyst 2950 Series switches support Internet Group Management Protocol (IGMP) snooping in hardware. Through the support and configuration of IGMP snooping via 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. 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 distributing traffic loads across multiple links. This is not possible with standard Spanning-Tree Protocol implementations. Cisco UplinkFast technology helps ensure immediate transfer to the secondary uplink, an improvement over the traditional 30-to-60 second convergence time. An additional feature that enhances performance is Voice VLAN, which 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 that use 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

Cisco CMS Software is Web-based and embedded in Cisco Catalyst 3550, 2950, 3500 XL, 2900 XL, and 2900 LRE XL series switches. Through Cisco switch clustering technology, users can access Cisco CMS Software 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 Series switches, Cisco CMS Software can now extend beyond routed boundaries for even more flexibility in managing a Cisco cluster.

Cisco CMS Software provides an integrated management interface for delivering intelligent services, such as multilayer switching, QoS, multicast, and security ACLs. Cisco CMS Software allows administrators to take advantage of benefits formerly reserved for only the most advanced networks without the command-line interface (CLI) or even the details of the technology.

The new Guide Mode in Cisco CMS Software 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 streaming or videoconferencing, voice over IP (VoIP), and mission-critical applications. These wizards can save hours of time for network administrators, eliminate human errors, and help ensure that the configuration of the switch is optimized for these applications.

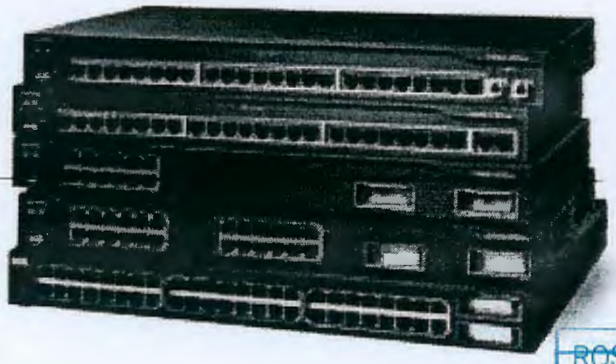
Cisco CMS Software supports standards-based connectivity options such as Ethernet, Fast Ethernet, Fast EtherChannel, Gigabit Ethernet, and Gigabit EtherChannel connectivity. Because Cisco switch clustering technology is not limited to a single stack of switches, Cisco CMS Software expands the traditional cluster domain beyond a single wiring closet and saves time and effort for network administrators.

Cisco Catalyst 2950 Series switches can be configured either as command or member switches in a Cisco switch cluster. Cisco CMS Software 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 features include the ability to configure multiple ports and switches simultaneously, to perform software updates across the entire cluster at once, and to clone configurations to other clustered switches for rapid network deployment. 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 Cisco CMS Software, Cisco Catalyst 2950 Series switches provide extensive management tools using SNMP network management platforms such as CiscoWorks for switched internetworks.

Cisco Catalyst 2950 Series switches deliver a comprehensive set of management tools to provide the required visibility and control in the network (Figure 1). Managed with CiscoWorks, Cisco Catalyst 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.

Figure 1
Cisco Catalyst 2950 Series Switches



Product Features and Benefits

Table 1 lists the features and benefits of the Cisco Catalyst 2950 Series switches.

Table 1 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 failover 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 failover recovery, enhancing network stability and availability. • Support for the optional 300-watt or 675-watt redundant Cisco AC power system provides a backup power source for up to 4 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 Cisco 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) and aggressive UDLD features detect and disable unidirectional links on fiber-optic interfaces caused by incorrect fiber-optic wiring or port faults.
Integrated Cisco IOS Software features for bandwidth optimization	• Bandwidth aggregation of up to 4 Gbps (2 ports full duplex) through Cisco 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. • Per-port broadcast, multicast, and unicast storm control prevents faulty end stations from degrading overall systems performance. • PVST+ allows for Layer 2 load sharing on redundant links to efficiently use 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, 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 (sequence number protection [SNAP] encapsulated tagged and untagged frames)

Feature	Benefit
Security	
Network-wide security features	• Filtering of incoming traffic flows based on Layer 2–4 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, helping to ensure that voice traffic travels directly from its entry point to the aggregation device through a virtual path and that it 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 gives an IP phone access to the Voice VLAN regardless of the authorized or unauthorized state of the port. • 802.1x with port security enables authenticating the port and managing network access for all MAC 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 U.S. export restrictions. • Port Security secures the access to a port based on the MAC address of a user's 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 enables centralized control of the switch and restricts 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 to disable the trust setting in the event that the IP phone is removed, preventing a rogue user from overriding prioritization policies in the network. • IGMP Filtering provides multicast authentication by filtering out nonsubscribers and limiting the number of concurrent multicast streams available per port. • Support for dynamic VLAN assignment through implementation of the VLAN Membership Policy Server (VMPS) client function provides flexibility in assigning ports to VLANs. Dynamic VLAN enables fast assignment of IP addresses. • Cisco CMS Software security wizards ease the deployment of security features for restricting user access to a server, a portion of the network, or the entire network.

Feature	Benefit
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 the 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. • 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 2–4 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, and 16-bit Ethertype. • The switches support identification of traffic based on Layer 3 type of service (ToS) field and 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, and 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 from 802.1p to DSCP. • The switches support 14 widely used DSCP values. • The switches support classifying or reclassifying packets based on default DSCP per port. They also support classification based on DSCP values in the ACL. • The switches support classifying or reclassifying frames based on the 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.
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

Feature	Benefit
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 a switch to generate a crash file for improved troubleshooting. • Show-interface-capabilities provides information on configuration capabilities of any interface. • The RTTMON Management Information Base (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.

Feature	Benefit
Management	
Cisco CMS Software	• Cisco CMS Software allows the user to manage up to 16 interconnected Cisco Catalyst 3550, 2950, 3500 XL, 2900 XL, and 2900 LRE XL series 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 helps ensure that any combination of the above switches can be managed with a Cisco Catalyst 2950 Series 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, or high-priority data. • A security wizard is provided to restrict unauthorized access to servers and networks, and to 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 Software Guide Mode assists users in the configuration of powerful advanced features by providing step-by-step instructions. • Cisco CMS Software provides enhanced online help for context-sensitive assistance. • An easy-to-use graphical interface provides both a topology map and a front-panel view of the cluster. • Multidevice and multiport 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. • A user-personalized interface allows users to modify polling intervals, table views, and other settings within Cisco CMS Software and to retain these settings the next time they use the software. • 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 provides 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 Versions 1 and 2 enable a CiscoWorks network management station to automatically discover the switch in a network topology. • Supported by the CiscoWorks LAN Management Solution.

Feature	Benefit
Management	
Ease of use and ease of deployment	• The Cisco GigaStack® GBIC delivers a hardware-based, independent stacking bus with up to a 2-Gbps forwarding rate in a point-to-point configuration, or 1 Gbps of forwarding bandwidth when daisy-chained with up to 9 switches. • Autoconfiguration eases the 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. • 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 1000BASE-T environments. • Autonegotiating 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 a 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 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 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

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 1530 bytes (Cisco Catalyst 2950G switches only)
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

Feature	Description
Management	• 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
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

Feature	Description
Standards	• RMON I and II standards • SNMPv1, v2c, and v3 (planned future support for v3)
Y2K	• Y2K compliant
Connectors and cabling	• 10BASE-T ports: RJ-45 connectors; two-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
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 autoranging unit. • The internal power supply supports input voltages between 100 and 240 VAC. • The supplied AC power cord should be used 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 675-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. • Attach only the Cisco RPS 675 (model PWR675-AC-RPS-NI=) to the RPS receptacle with this connector. **Cisco RPS 300 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. • Attach only the Cisco RPS 300 (model PWR300-AC-RPS-N1) to the RPS receptacle with this connector.

Feature	Description
Indicators	• Per-port status LEDs: link integrity, disabled, activity, speed, and full-duplex indications. • System status LEDs: system, RPS, and bandwidth utilization indications.
Dimensions (H x W x D) and weight	• 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 (RU) 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 percent (noncondensing) • 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
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 (autoranging); 50 to 60 Hz • DC input voltages for Cisco RPS 300: +12V @ 4.5A
Acoustic noise	• ISO 7770, bystander position—operating to an ambient temperature of 30°C: – 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
Predicted mean time between failure (MTBF)	• 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 nm • Optical receiver sensibility: –14 dBm2 • Optical transmitter power: –19 to –14 dBm • Transmit: –19 to –14 dBm

Feature	Description
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
Network Equipment Building Standards (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 Table 2 are available as part of the Cisco Desktop Switching Service and Support solution, and are available directly from Cisco and through resellers.

Table 2 Service and Support Programs

Service and Support	Features	Benefits
Advanced Services		
Total Implementation Solutions (TIS)—available direct from Cisco ***Packaged TIS***—available through resellers	• Project management • Site survey and configuration deployment • Installation, text, and cutover • Training • Major moves, adds, and changes • Design review and product staging	• Supplements existing staff • Ensures that functions meet customer needs • Mitigates risk
Technical Support Services		
Cisco SMARTnet® and Cisco SMARTnet Onsite services—available direct from Cisco ***Packaged Cisco SMARTnet service***—available through resellers	• 24x7 access to software updates • Web access to technical repositories • Telephone support through the Cisco Technical Assistance Center (TAC) • Advance replacement of hardware parts	• Enables proactive or expedited issue resolution • Lowers cost of ownership by using Cisco expertise and knowledge • Minimizes network downtime

Ordering Information

Model Numbers	Configuration
WS-C2950G-48-EI	• 48 10/100 ports and 2 1000BASE-X ports • Cisco EI Software image installed
WS-C2950G-24-EI	• 24 10/100 ports and 2 1000BASE-X ports • Cisco EI Software image installed
WS-C2950G-24-EI-DC	• 24 10/100 ports and 2 1000BASE-X ports; DC power • Cisco EI Software image installed
WS-C2950G-12-EI	• 12 10/100 ports and 2 1000BASE-X ports • Cisco EI Software image installed
WS-C2950T-24	• 24 10/100 ports and 2 1000BASE-T ports • Cisco EI Software image installed
WS-C2950C-24	• 24 10/100 ports and 2 100BASE-FX ports • Cisco EI Software image installed
WS-C2950ST-24-LRE	• 24 LRE ports, 2 fixed 10/100/1000BASE-T ports, and 2 SFP ports • Cisco EI Software image installed
WS-C2950ST-8-LRE	• 8 LRE ports, 2 fixed 10/100/1000BASE-T ports, and 2 SFP ports • Cisco EI Software image installed

For More Information

- 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 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

BU/LW4574 05/03

0312

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

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

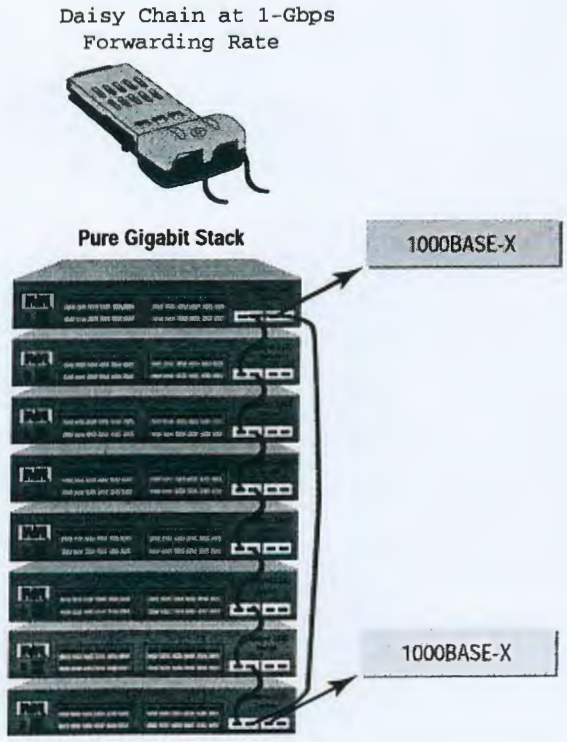
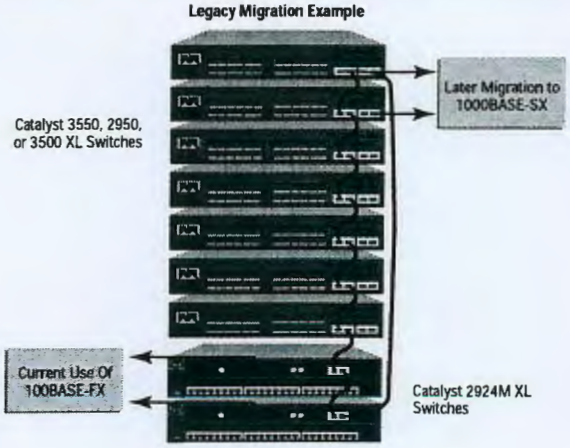


Figure 3 illustrates how the Catalyst 2912MF XL or Catalyst 2924M XL switch can be used in combination with Catalyst 3550, 2950G, or 3500 XL switches using the GigaStack GBIC half-duplex cascade feature. This configuration will provide the flexibility to implement a migration plan from legacy uplink 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

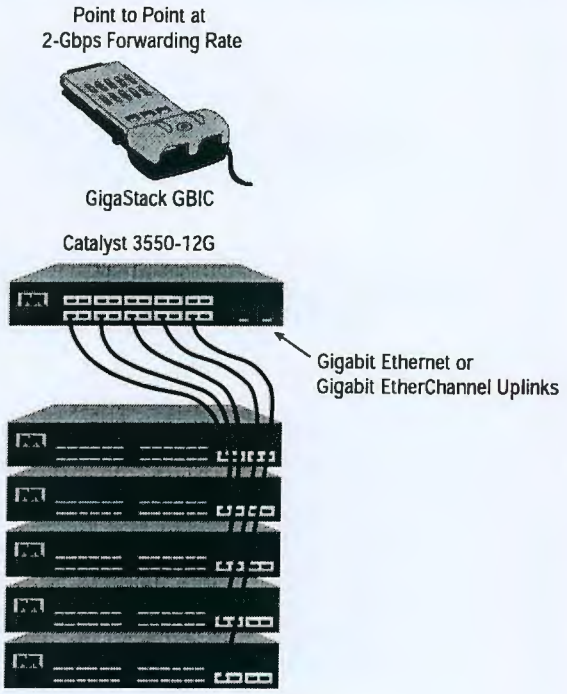
Customers can also use the GigaStack GBIC to create a low-cost dedicated Gigabit Ethernet connection between two stack members, providing a scalability option to increase overall stack bandwidth. When connecting two GigaStack GBICs with a single cable, the GBIC will autonegotiate to full-duplex and provide 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.

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.

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

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

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

0702/BW8402

Cisco Systems

Data Sheet

CiscoWorks **Campus Manager**

Campus Manager is a key component in the CiscoWorks family of management solutions designed to make Cisco networks the most manageable and available in the industry. Today's networks are critical business assets, and require sophisticated tools for administering, monitoring and configuring Layer 2 services. Designed for enterprise network operations staff, Campus Manager provides powerful tools with built-in network intelligence to reduce the complexity and automate manual tasks associated with maintaining complex physical and logical network infrastructures.

Campus Manager Overview

Campus networks are at the heart of business and mission-critical systems. The requirement to understand, monitor, and react to changing networking conditions drives the need for sophisticated, yet easy-to-use management tools. Campus Manager is part of the LAN Management Solution, part of the broad range of CiscoWorks network management solutions.

New in Version 3.3:

In addition to the rich set of management features already included, the new version of Campus Manager has been enhanced to provide even greater manageability for Cisco networks. New benefits include:

- Improved application performance
- Doubled capacity for tracking end users

Key Campus Manager features include:

- Intelligent discovery and display of Layer 2 networks on browser-accessible topology maps, independent of VTP server
- Configuration of virtual LAN (VLAN)/ LAN Emulation (LANE) and asynchronous transfer mode (ATM) services and assignment of switch ports to those services
- Link and device status display based upon Simple Network Management Protocol (SNMP) polling
- Identification of Layer 2 configuration discrepancies
- Diagnostic tools for connectivity related problems between end stations, and Layer 2 and Layer 3 devices
- Automatic location and correlation of information on users by media access control (MAC), IP address, NT or NetWare Directory Services (NDS) login or UNIX host name, with their physical connections to the switched network
- Visibility and launch point of Cisco CallManager from topology services as well as tracking of phone handset to IP, Mac address, and switch port
- Layer 2 and Layer 3 path trace between source and destination handsets
- Export of topology maps to Visio
- Java plugins to improve graphical user interface (GUI) performance

- Ability to form Custom Groups in Topology View based on criteria like SysLocation, SysName and IP address/ Subnet mask.
- Secure communication between the client browser and Campus applications using Secure Socket Layer (SSL) protocol.

Campus Manager enables administrators to more easily change, monitor, and control network relationships, making them more effective in delivering business-critical and advanced networking services to their users and customers.

Campus Manager is a suite of applications launched from a common "management desktop" used by all Web-based CiscoWorks applications. Campus Manager contains three applications that can be launched from the client's browser:

- Topology Services—This is the principal interface to a variety of large scale topology maps, tabular summaries, reports, and configuration services of the Layer 2 network. A directory-like tree interface lists physical Layer 2 and logical, Virtual Trunking Protocol (VTP), and ATM domain views along with table summaries of the devices and interface associated with these views. This tree structure acts as the launching point for topology maps, discrepancy reporting functions, and configuration services. The integrated VLAN and LANE configuration capabilities, ATM soft permanent virtual circuit (PVC) configuration and diagnostic tools, along with physical and logical configuration discrepancy checking reports and highlighting tools are found within the Topology Services menus. It also supports discovery and display of Cisco Customer Response Applications, and reports on services of these devices.

  Ability to form custom groups based on dynamic and static rules for the group membership. System defined groups and user defined grouping can be created by network administrators and users respectively and allows grouping by developing rules based on criteria such as IP address, subnets, SysLocation, SysName, SysContact, Image Version and hostname. A rules editor allows for creating, editing Topology groups and defines rules for membership.

Figure 1
Topology Services Tabular View

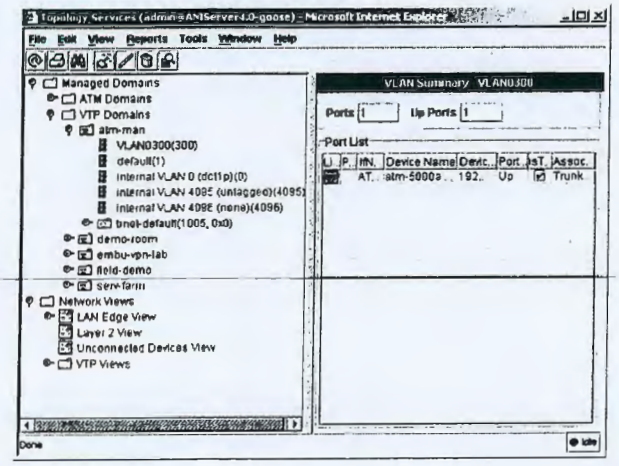


Figure 2
VTP Domain Topology Map

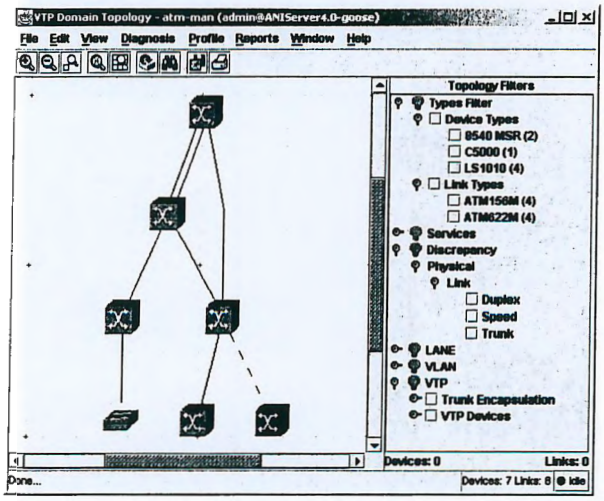


Figure 3
Forming Topology Groups

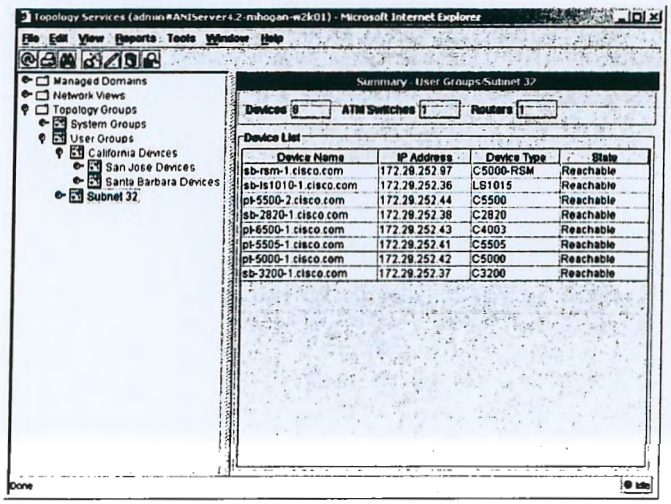
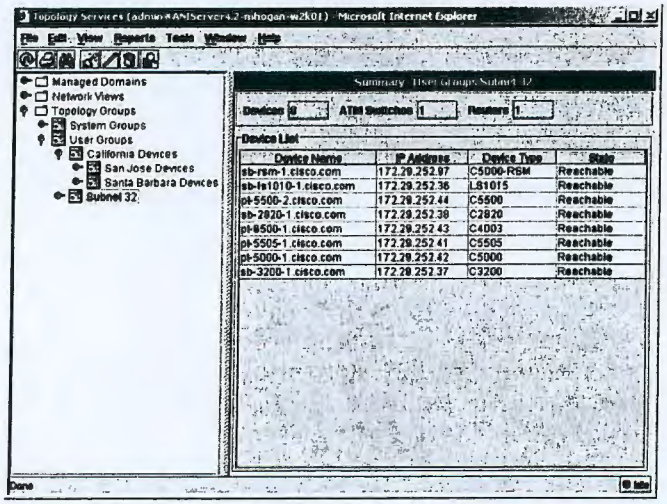


Figure 4
Topology Group in Topology Maps



- User Tracking—Designed to assist in locating end-station connections at the access switch, this application is a useful tool in troubleshooting or connectivity analysis. Through automated acquisition, a table of end-user stations and Layer 2 connection information is constructed. This table can be sorted and queried allowing administrators to easily find users. Users can be identified by name, IP handset, MAC and IP address, as well as the switch port and switch that they are connected, along with VLAN and VTP assignment of the port. Predefined reports, such as duplicate MAC per switch port, or duplicate IP addresses, enable managers to locate mobile users or violations in port policies.

Figure 5
User Tracking

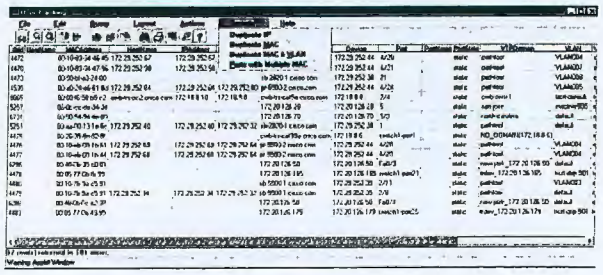
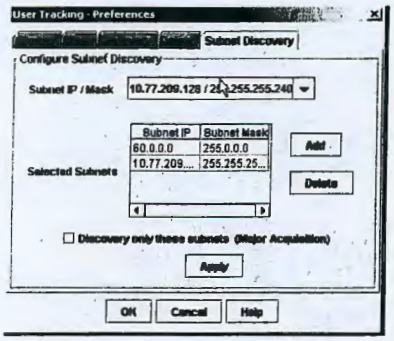
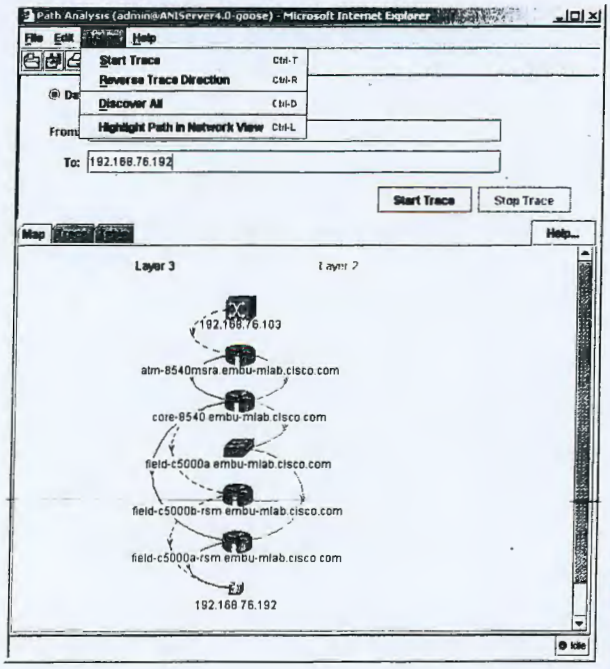


Figure 6
Subnet based acquisition



- Path Analysis—An application for switched network management, this is an extremely powerful tool for connectivity troubleshooting. Path Analysis utilizes User Tracking, topology services, and real-time spanning tree information to determine Layer 2 and Layer 3 connectivity between two end-points, or IP Handsets, in the network. The resulting trace is presented in graphical topology views that illustrate the Layer 2 and Layer 3 devices, path direction and link types, and in tabular formats that provide specific interface, IP address, VLAN, and link type information.

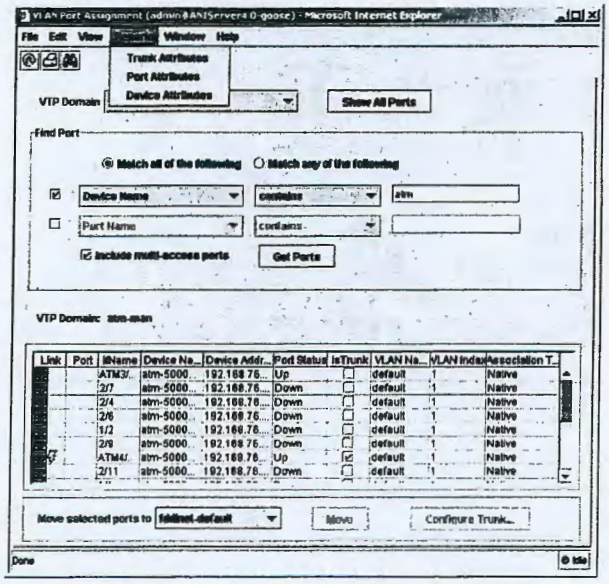
Figure 7
Path Analysis



VLAN/LANE Configuration and Port Assignment

Campus Manager provides an easy and graphical means for creating, modifying, or deleting VLANs, LANE elements, or assigning switch ports to VLANs. As VLANs are created or modified, port and user changes are instantly updated and transmitted to the switches, eliminating the need to update and configure each participating switch individually. As VLANs are selected, the table view shows the participating ports, port status, and switch information and the topology map can be launched to graphically highlight participating devices and links of the VLAN connections. Additional map tools allow managers to show spanning-tree states, VTP trunks, switch port links, and existing LANE service elements.

Figure 8
VLAN Port Assignment



Campus Manager 3.3 is a must for switched network management, and is an integral piece of the LAN Management Solution, by providing a broad, comprehensive set of tools for managing and administering the entire LAN environment.

Campus Manager 3.3 Features

Campus Manager provides a variety of functions within Topology Services, User Tracking, Path Analysis and VLAN/LANE port assignment that network managers can use to better understand, monitor, configure, diagnose, and be proactive to network infrastructure changes.

Topology Services

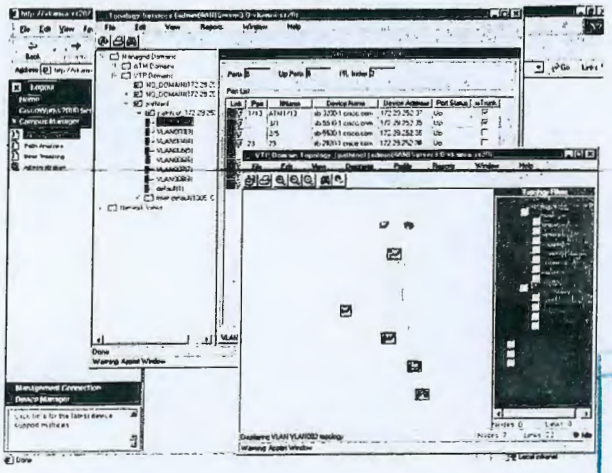
Topology Services provides access to a wide variety of physical and logical topology maps, summary lists of devices, ports, and their network relationships. Topology Services also acts as the launching point for topology-related configuration and diagnostic tools.

In Campus Manager 3.3, network topology maps can be displayed in a variety of ways from both a flat Layer 2 to abstracted views that better represent and scale to large campus networks. These abstractions are categorized into three different groups: managed domains, network views and topology groups. Managed domains are topological views of logical groups of devices organized around ATM switch fabrics and VTP domains. Network views are physical displays of the network and are organized to provide full and abstracted views, such as LAN edge views, Layer 2 views, unconnected device views, and VTP views. Topology Groups are custom views that are a subset of the entire network based on the group rule defined while creating the view. They are can be two types of groups—system defined groups that are custom views created by admin user and user defined views which are created by CiscoWorks users. Membership to these groups are made via rules that can be evaluated either automatically or upon user request and these groups help in generating custom views that are a subset of the Layer 2 views.

Key features in the Campus Manager topology services include:

- Autodiscovery and display of Cisco switches, routers, and probes using the Cisco Discovery Protocol (CDP) and SNMP
- Display of physical and logical Layer 2 connections within the discovered LAN environment
- Highlighting tools to identify specific classes of devices or links such as switches, route switch modules (RSMs), Fast Ethernet, EtherChannel®, ATM links, Cisco Customer Response Applications, and other relevant Cisco device elements
- Expanded scalability to support more than 2000 Cisco devices
- Display of multilayer switches and components (switching entities and route-processing entities) with the ability to highlight logical relationships between devices, such as flow masks and shortcuts
- Device status indicators on the topology maps based on CDP, ILMI, ELMI, and SNMP availability
- Automated discrepancy reporting during discovery highlights connection problems, link mismatches, and logical misconfigurations
- Graphical interface for creating VLAN and LANE services for Ethernet, Token Ring, and transparent VLANs
- Graphical interface for locating—through search parameters—and assigning switch ports individually or in bulk to a VLAN
- ATM soft PVC configuration and diagnostics

Figure 9
Topology Views and Tools



VLAN/LANE Configuration and Port Assignment

Campus Manager provides an easy and graphical means for creating, modifying, or deleting VLANs, LANE elements, or assigning switch ports to VLANs. As VLANs are created or modified, port and user changes are instantly updated and transmitted to the switches, eliminating the need to update and configure each participating switch individually. As VLANs are selected, the table view shows the participating ports, port status, and switch information and the topology map can be launched to graphically highlight participating devices and links of the VLAN connections. Additional map tools allow managers to show spanning-tree states, VTP trunks, switch port links, and existing LANE service elements.

VLAN management services provide:

- Tabular summary views of VLANs shows participating ports, devices, links, and port status information
- Graphical setup of VLANs (including transparent VLANs) and VLAN membership to simplify administration
- Integration of LANE configuration services in VLAN configuration tools for more efficient operational and engineering practices
- A separate interface for administrators to quickly search, using a variety of criteria, and assign selected switch ports, individually or in bulk, to VLANs
- Logical display of VLAN configurations makes it easy to visualize switch connections
- Automated discrepancy reports highlight connection problems and link mismatches
- Automated VLAN membership registration reduces administration and configuration requirements

ATM Management

Campus Manager offers a graphical tool for managing complex ATM networks, simplifying configuration and performance monitoring. ATM networks are displayed on the topology map and the logical VLAN and ATM domain views provide graphical representations of ATM switches and LANE elements. "Drill down" capability allows access to configuration and performance monitoring tools. ATM management functions include:

- Autodiscovery of ATM switches, including switched virtual circuit (SVC) and PVC connections
- Connectivity checking of SVC and PVC connections
- End-to-end virtual circuit path tracing and analysis, which assists in connectivity diagnostics
- LANE troubleshooting and performance analysis
- Quality of service (QoS) templates for simplifying the configuration of typical traffic such as video or constant-bit-rate (CBR)
- Simple configuration of soft PVCs
- ATM remote monitoring (RMON) data collection and analysis

User Tracking

User Tracking automatically locates servers and end-user workstations, and Cisco voice over IP (VoIP) telephone handsets and their connections to Layer 2 Cisco switches. During this discovery process it also tabulates specific connection information about that end station, including:

- VLAN name, type, and VTP domain
- Switch port number, name, and state

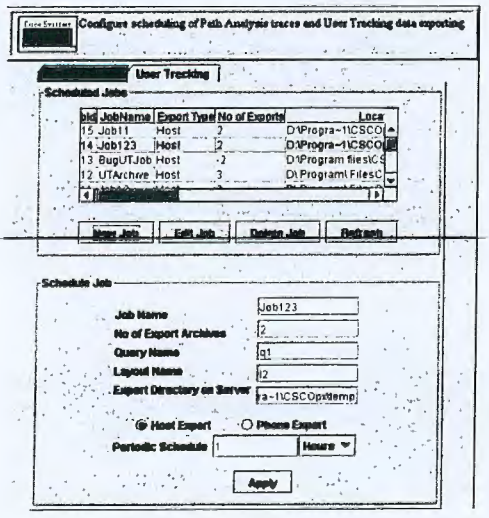
- MAC and IP address of the end station and its subnet
- Tabular and sortable listing of all switch port attached end-user workstations, servers and IP handsets
- Last-seen time stamp reflecting last acquisition in which the end station was detected
- User login name passed automatically from the Windows NT Primary Domain Controller or Novell Directory Structure, or from the UNIX host

Campus Manager simplifies the dynamic nature of many business environments by providing a large number of sortable parameters that can be used to locate end-user stations. User Tracking discovers end stations connected to switch ports automatically and provides a means to identify end users, their assigned VLANs, and host station connections. User Tracking also supports voice/data convergence with interfaces to Cisco CallManager for correlating the IP and MAC addresses of discovered VoIP handsets with their assigned phone number and users.

User Tracking provides the following features:

- Enhanced scalability to support 60,000 end stations
- Predefined reports that identify duplicate MAC and IP addresses, ports with multiple MAC addresses and duplicate sysnames.
- IP and MAC addresses of discovered VoIP handsets with their assigned phone number and users
- Tabular and sortable listing of all switch port-attached end-user workstations and IP handsets
- Customized tables for user-defined, detailed reporting
- GUI for user tracking information table configuration to support dynamic/mobile users
- Scheduling managers for automating address change updates
- Easy-to-use search utility box locating users by MAC addresses, IP addresses, DNS host names, switch port labels, and optional voice handsets
- Provides ability to schedule User Tracking. Also exports User Tracking reports.
- Ability to define acquisition based on a subnet range

Figure 10
Scheduled export of User Tracking Reports



Path Analysis

Path Analysis is a powerful diagnostic tool for determining the Layer 2 and Layer 3 path between two selected endpoints using Campus Manager-discovered end-station data, VLAN/LANE configuration information, real-time Layer 3 path trace information, and spanning-tree calculations. Displays of path information are available in both topological map and tabular displays. Key Path Analysis features include:

- View the Layer 2 and Layer 3 path information in a map format with traces showing end stations, Layer 2 and 3 devices, route directions, and cut-through paths
- View specific details of the Layer 2 and Layer 3 path, including IP addresses and interfaces traveled, VLAN and VTP domain names, and port speeds and duplex settings
- Perform traces immediately or schedule them
- Perform traces using IP address, DNS name, or by telephone number for voice calls as start/stop points
- Provide Layer 2 and Layer 3 trace information between Cisco voice elements using interfaces to call detail records for specific voice calls
- Provides ability to schedule path traces. Also exports path traces data.

Built on the CiscoWorks Management Server

The CiscoWorks management server provides common resources, such as Web services, discovery, shared databases and database services, and the management desktop. Cisco Management Connection, a service on the CiscoWorks2000 server, delivers a set of tools for integrating applications into the management desktop using Internet-based standards and technologies. These tools allow users to link Web-based management applications to the CiscoWorks family of products and application developers to easily link Web-based applications through a certified registration mechanism. Cisco Management Connection has been used by Cisco and more than 30 network management vendors, including Hewlett-Packard, Computer Associates, Sun Microsystems, and Tivoli Systems to create certified Cisco Management Connections for their applications. This rapid adoption has created an environment in which users can easily build management intranets that link together their favorite Web-based management applications.

Specifications

Server, Client, and Web Browser System Requirements

The server, client and web browser system requirements can be found in the Product Overview documents for the Routed WAN and LAN Management solutions and on Cisco's main on-line documentation site, under each CiscoWorks solution. Please refer to these and other Product Installation documentation for more detailed information on setting up and configuring these solutions.

Supported Cisco Devices

Most Cisco routers, Catalyst® and LightStream switches, as well as Cisco AVVID devices. Contact your Cisco representative for a complete list.

Supported Cisco IOS Versions

- Cisco IOS® version 10.3 and above
- Catalyst Supervisor code 2.1 and above

Availability

Campus Manager 3.3 is an integral part of multiple CiscoWorks solutions and is not sold as an individual product. For additional information on Campus Manager, see:
http://cisco.com/warp/public/cc/pd/wr2k/

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

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

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

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

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

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

203046/ETMG_03/03

Cisco Systems

Overview

CiscoWorks Routed WAN Management Solution 1.3

The CiscoWorks Routed WAN (RWAN) Management Solution extends the CiscoWorks product family by providing a collection of powerful management applications to configure, administer, and maintain a Cisco routed wide-area network (WAN).

The RWAN solution addresses the needs of managing WANs by improving the accuracy, efficiency, and effectiveness of your network administrators and operations staff while increasing the overall availability of your network through proactive planning, deployment, and troubleshooting tools.

CiscoWorks solutions comply with Internet standards and have no network management system (NMS) prerequisites. These solutions take advantage of Web browser technologies for accessibility and integration with other third-party Web-based management tools and platforms.

Complementary CiscoWorks solutions such as the LAN Management Solution (LMS) provide a solid foundation of campus management tools. The IP Telephony Environment Monitor (ITEM) ensures the readiness and manageability of converged networks that are supporting voice over IP (VoIP) and IP telephony traffic and applications. The Cisco VPN/Security Management Solution (VMS) provides an integrated set of Web-based applications with features that assist in the deployment and monitoring of virtual private network (VPN) and security devices. Additional solutions for managing quality of service (QoS), network and user authentication, identity and access control, content networking, and Remote Monitoring (RMON) are also available.

CiscoWorks management solutions play an integral part in deploying and maintaining a Cisco AVVID (Architecture for Voice, Video and Integrated Data) network infrastructure comprising converged data, voice, and content networking.

WAN Management Challenge

Today's enterprise WANs continue to grow as more mission-critical applications and services depend on reliable, high-performance intranet and Internet connections to remote offices, suppliers, customers, and partners worldwide. WAN links are typically the most expensive part of the network, and monitoring their performance and uptime is critical to maintaining a reliable and cost-effective network.

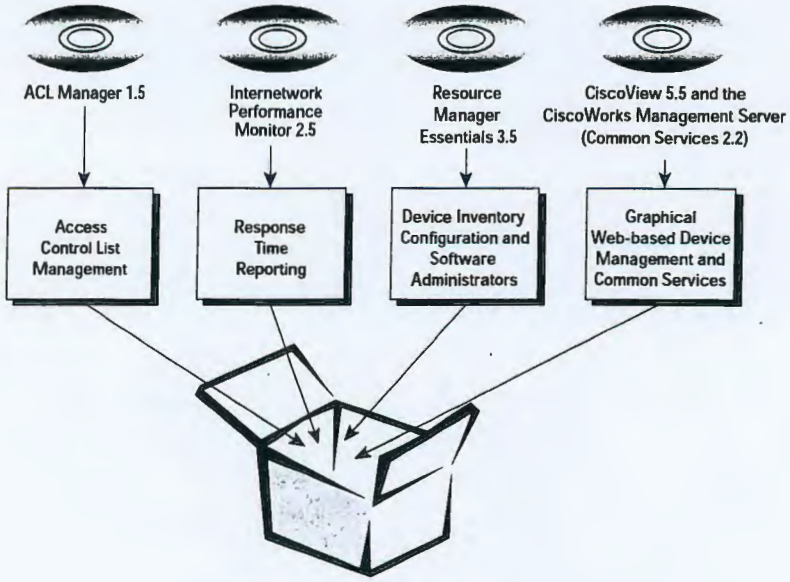
The ability to effectively measure response time between devices, users, and services is key to maintaining the highest levels of service quality. Proper management of WAN edge devices, links, and services becomes critical, and for this reason, Cisco has assembled a comprehensive set of WAN management tools designed to make the WAN manager's life much easier.

A Comprehensive Solution

The CiscoWorks Routed WAN Management Solution provides increased visibility into network behavior, assists in quickly

troubleshooting performance bottlenecks, and provides comprehensive tools to easily administer new software and configuration changes for optimizing bandwidth and utilization across expensive and critical links in the network (Figure 1).

Figure 1
RWAN Management Solution 1.3 Components



Solution Components

The following applications are included in the CiscoWorks RWAN Management Solution (refer also to Table 1):

- *CiscoWorks Access Control List (ACL) Manager*—CiscoWorks ACL Manager significantly reduces the time typically required to manage and administer access control lists using the command-line interface (CLI) of Cisco IOS® Software. It provides a wizard and policy template-based approach to simplifying the setup, management, and optimization of Cisco IOS Software-based IP and Internetwork Packet Exchange (IPX) traffic filtering and device access control. This tool includes an access list editor, policy template manager, network and service class managers for scalability, access list navigation tools for troubleshooting, and automated distribution of access list updates.
- *CiscoWorks Internetwork Performance Monitor (IPM)*—CiscoWorks IPM is a network response time and availability troubleshooting application that enables WAN managers to proactively troubleshoot network response times using Cisco IOS Software embedded technology. The path and hop performance analysis provided by CiscoWorks IPM simplifies the identification of devices that are contributing to latency and network delays. CiscoWorks IPM is used to diagnose latency, identify network bottlenecks, and analyze response times. The application is also valuable for managing the effectiveness of QoS features based on IP Precedence and for troubleshooting network jitter-related problems, both of which will be needed to deploy VoIP.
- *CiscoWorks Resource Manager Essentials (RME)*— CiscoWorks RME provides the tools needed to manage Cisco devices. It includes inventory and device change management, network configuration and software image management, network availability, and syslog analysis.

- *CiscoView*—CiscoView provides real-time status of Cisco devices graphically. CiscoView can drill down to display monitoring information on interfaces and access configuration functions.
- *CiscoWorks Management Server*—CiscoWorks Management Server provides the common management desktop services and security across the CiscoWorks Family of solutions. It also provides the foundation for integrating with other Cisco and third-party applications.

Table 1 RWAN Management Solution Key Application/Function

Key Application/Function	Product	Management Benefit
ACL optimization	CiscoWorks ACL Manager	Improves router performance by organizing access filters to sort by most frequent usage patterns
ACL profiles	CiscoWorks ACL Manager	Allows administrators to quickly and uniformly apply and update template-based ACLs; can reduce WAN costs and enhance security management
ACL distribution	CiscoWorks ACL Manager	Allows administrator to automate the process of updating access list information in multiple devices
Monitoring of WAN response time characteristics	CiscoWorks IPM	Measures the responsiveness of WAN connections to determine latency and jitter, and to determine where traffic bottlenecks exist
Path and hop analysis	CiscoWorks IPM	Identifies which devices in the network are causing the greatest latency in network traffic
Detailed software and hardware inventory reporting	CiscoWorks RME	Provides accurate Cisco inventory baseline information, including memory, slots, software versions, and boot ROMs needed to make decisions about the network
Automated update engines for device software and configuration changes	CiscoWorks RME	Allows software and configuration updates to be sent to selected devices on a scheduled basis; reduces time and errors involved in network updates
Consolidated troubleshooting tools device center	CiscoWorks RME	Offers a wide collection of switch and router analysis tools accessible from a single location; device center can be linked to by third-party applications
Centralized change audit logging and application access security	CiscoWorks RME	Comprehensive change monitoring log records user and application active on the network; CiscoWorks desktop controls user access to applications, ensuring that only appropriate classes of users can access tools that change network parameters versus read-only tools
Graphic device management	CiscoView	Displays a browser representation of Cisco router and switch devices, color-coded to indicate operations states, with access to configuration and monitoring tools
Third-party integration tools (Integration utility)	CiscoWorks Management Server	Simplifies the Web integration of third-party and other Cisco management tools

Key Functions and Applications

Deployment Options

Consider the following when installing the CiscoWorks RWAN Management Solution:

- All applications do not have to be installed initially; applications not installed initially may be installed later.
- Most applications require the CiscoWorks Management Server from the Common Services CD (formerly CD One), which must be installed first.
- The CiscoWorks ACL Manager application depends on CiscoWorks RME, which is included as part of the CiscoWorks RWAN Management Solution.

All solutions can coexist on the same server if they support and operate with the services of Common Services 2.2. However, network managers may want to consider such factors as the number of applications hosted, system resources, and number of devices to be managed in determining if all or a subset of the solutions are installed on the same server.

CiscoWorks solutions offer deployment flexibility. System administrators should use the guidelines given previously when planning the deployment of the various solution bundles. Some components within a solution require the CiscoWorks Management Server and must be installed on that machine. CiscoWorks IPM and CiscoView Software can be set up on an independent server. The placement of components is a function of performance requirements and the size of the network.

Server System Requirements

Hardware/Operating System

UNIX

- System: Sun UltraSPARCIII (Sun Blade 1000 Workstation or Sun Fire 280R Workgroup Server) running Solaris 2.8 (dual processor system required for hosting multiple management solutions)
- Memory: 1-GB RAM for workstations, 2-GB RAM for servers, 8-MB e-cache
- Available disk: 40-GB internal FC-AL disk drive for workstation and dual drives of this type for server configurations

Windows

- System: IBM PC compatible with 550-MHz or higher Pentium III processor running Microsoft Windows 2000 Advanced Server (with Terminal Services turned off), Server or Professional Edition with Service Pack 3 (dual processor system required for hosting multiple management solutions)
- Memory: 1-GB RAM
- Available disk: 40 GB with 2-GB swap recommended

Note: These system requirements are based on managing 500 devices with CiscoWorks RWAN and LAN Management solutions loaded on a single server. Refer to the installation documentation for more information on required operating system patches.

Client Browser System Requirements

Hardware/Operating System

UNIX

- System: Sun Ultra 10 running Solaris Versions 2.7 or 2.8
- System: HP9000 Series running HP-UX 11.0
- System: IBM RS/6000 workstation running AIX 4.3.3
- Memory: 256 MB

Windows

- System: IBM PC-compatible computer with 300-MHz or higher Pentium processor running Windows XP Professional with Service Pack 1, Windows 2000 Professional with Service Pack 2 or 3, or Windows Server with Server Pack 2 or 3.
- Memory: 256 MB

Note: Refer to the installation documentation for more information on required operating system patches.

Web Browser

UNIX

- Solaris: Netscape v4.76

Windows

- Windows 2000/XP: Netscape v4.78, 4.79
- Windows 2000/XP: Internet Explorer v6.0 or v6.0 with Service Pack1

Note: Refer to the installation documentation for more information on required operating systems patches, browser plug-ins, or Java Virtual Machine (JVM) versions.

Service and Support

CiscoWorks products are covered by the Cisco Software Application Service (SAS) program. This service program offers customers contract-based 7 x 24 access to the Cisco Technical Assistance Center (TAC), full Cisco.com privileges, and software maintenance updates. A Cisco SAS contract ensures that customers have easy access to the information and services needed to stay up-to-date with newly supported device packages, patches, and minor updates. For further information on service and support offerings, contact your local sales office.

Ordering Information

The CiscoWorks RWAN Management Solution includes all the necessary components needed for an independent installation on a Microsoft Windows or Sun Solaris workstation or server. The products within this solution can be combined with other CiscoWorks products if they support the same CiscoWorks Management Server version, operating environment, and system

requirements. Contact your local Cisco representative for available white papers and documentation outlining best practices for implementing a CiscoWorks management solution architecture.

To place an order, contact your Cisco sales representative.

Refer to the CiscoWorks RWAN individual product data sheets for more information on operating environment and system requirements.

For More Information

The following URL offers more information:

http://www.cisco.com/en/US/partner/products/sw/cscowork/ps2426/index.html

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

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

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

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

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

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

203046/ETMG_03/03

Comprovação das Especificações Exigidas no Edital 050/2003

3.3. Switch tipo 3 (FC)

Switch Tipo 3	
12000QuickStart.pdf	Brocade - SilkWorm 12000 QuickStart Guide
B1200_Sun.pdf	Silkworm 12000
FabMan_DS_02.pdf	Brocade Fabric Manager
fm_userguide.pdf	Brocade Fabric Manager - User's Guide Version 4.0

BROCADE

SilkWorm® 12000

QuickStart Guide

Publication Number 53-0000152-02

Corporate Headquarters
Brocade Communications Systems, Incorporated
1745 Technology Drive
San Jose, CA 95110
U.S.A.
T: (408) 487-8000
F: (408) 487-8101
info@brocade.com

European Headquarters
Brocade Communications Switzerland Sàrl
29, route de l'Aéroport
Case Postale 105
1215 Genève 15,
Switzerland
T: +41 22 799 56 40
F: +41 22 799 56 41
europe-info@brocade.com

Asia-Pacific Headquarters
Brocade Communications Systems K.K.
The Imperial Tower 15th Floor
1-1-1 Uchisaiwaicho
Chiyoda-ku, Tokyo 100-0011
Japan
T: +81 33507 5802
F: +81 33507 5900
apac-info@brocade.com

Publication Number 53-0000152-02

SilkWorm 12000 QuickStart Guide

The SilkWorm 12000 can be installed in the following ways:

- Set up as a stand-alone unit on a flat surface
- Installed in a 19-inch EIA (Electronic Industries Association) cabinet, using the 14U Rack Mount Kit provided with the SilkWorm 12000 (detailed instructions included with kit). Up to three SilkWorm 12000s can be installed in a 42U EIA cabinet.
- Installed in a mid-mount (Telco) rack, using the Mid-mount Rack Kit, available from your switch supplier (detailed instructions included with kit).

For simplicity, these instructions are written with the following assumptions:

- The "service aisle" refers to the aisle into which exhaust air is released
- The chassis is installed with the port side facing the service aisle

This guide provides the following information:

Installation Considerations and Safety Guidelines

Warning A fully populated SilkWorm 12000 weighs approximately 250 lbs and requires a minimum of two people and a hydraulic or assisted lift to install it.

Before installing, verify that the additional weight of the chassis does not exceed the cabinet's weight limits or unbalance the cabinet, including when some of the cards or power supplies are partially extended out of the chassis.

Caution To ensure adequate cooling, install the chassis with the port side facing the aisle into which exhaust air is released (usually called the "service aisle"). This prevents the fans from pulling in heated exhaust air.

The following steps are required to ensure correct installation and operation:

- Ensure the space in the EIA cabinet is 14U high, 29 inches deep, and 19 inches wide, with a minimum distance of 28.25 inches between the front and back rails.
- Verify that the additional weight of the chassis does not exceed the cabinet's weight limits.
- Plan for cable management before installing the chassis. Cables can be managed in a variety of ways, such as by routing cables below the chassis, to either side of the chassis, through cable channels on the sides of the cabinet, or by using patch panels.

- Ensure that two dedicated electrical branch circuits with the following characteristics are available:
  - 200 to 240 VAC, 50 - 60 Hertz (refer to the *SilkWorm 12000 Hardware Reference* for additional electrical specifications)
  - Protected by a circuit breaker in accordance with local electrical codes
  - Supply circuit, line fusing, and wire size that are adequate according to the electrical rating on the chassis nameplate
  - Grounded outlets installed by a licensed electrician and compatible with the power cords
- Ensure that all equipment installed in the cabinet is grounded through a reliable branch circuit connection. Do not rely on a secondary connection to a branch circuit, such as a power strip.
- Ensure the SilkWorm 12000 has access to a minimum airflow of 350 cubic feet per minute.
- Ensure the air temperature at the blower inlet does not exceed 40 degrees Celsius during operation.

Items Included With the SilkWorm 12000

The following items are included with the standard shipment of the SilkWorm 12000:

- The SilkWorm 12000, populated with:
  - Two, four or eight 16-port cards (customer-specified configuration)
  - Two CP cards (control processor cards)
  - Four power supplies
  - Three blower assemblies
- One Accessory Kit containing the following items:
  - The *SilkWorm 12000 QuickStart Guide*
  - The Brocade Documentation CD-ROM
  - ESD Grounding Strap
  - Power Cord Retainer
  - One 10-foot (3.05 meters) RS-232 serial cable, with an RJ-45 style connector / adapter on the end of the cable
- The 14U Rack Mount Kit with installation instructions.

Unpacking the SilkWorm 12000

This procedure requires a 1/2-inch socket wrench to remove the pallet bolts.

To unpack the SilkWorm 12000:

1. Open the shipping crate and remove the packing foam, anti-static plastic, and the 14U Rack Mount Kit and Accessory Kit.

   Note: To open one of the hinges on the crate, pull the handle out and turn counter-clockwise (to left), then slide open.

2. Unscrew the four bolts holding the SilkWorm 12000 to the pallet (see Figure 1), and remove the brackets.

Caution Remove the chassis door before moving the chassis.

3. Remove the chassis door from the chassis.
   a. Open the door to a 90 degree angle.
   b. Push the spring-loaded lever on the upper hinge up and into the notch in the hinge.
   c. Push the spring-loaded lever on the lower hinge down and into the notch in the hinge, supporting the door to prevent it from falling.

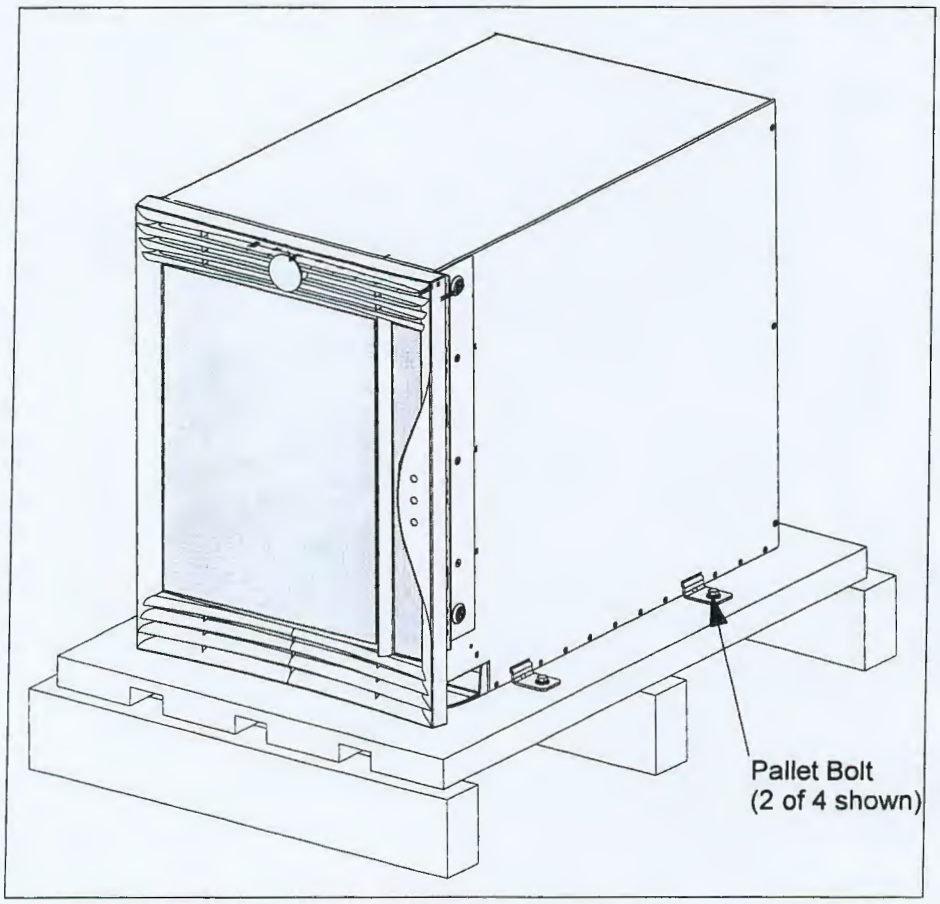


Figure 1 SilkWorm 12000 on its Shipping Pallet

Setting Up the SilkWorm 12000 as a Stand-alone Unit

If the SilkWorm 12000 is to be set up as a stand-alone unit, it must be placed on a stable, flat surface, with the blower side of the chassis having access to cool air. Brocade recommends orienting it so that the port side faces the service aisle.

4. To reinstall the door once the chassis is in place:
   a. Ensure that the spring-loaded pins on both door hinges are retracted (push levers into notches).
   b. Align the door hinges with the chassis portion of the hinges.
   c. Release the pins by pushing the levers out of the notches.

Providing Power to the SilkWorm 12000

5. Connect the power cords to a power source with voltage of 200 to 240 VAC, 50-60 Hz.
6. Connect the AC power cord retainer to the chassis:

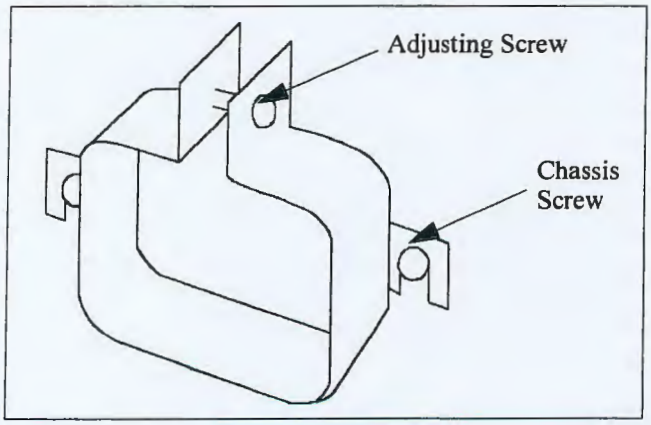


Figure 2 Power Cord Retainer

   a. Position a retainer over an AC power connector, oriented as shown in Figure 2, hooking the retainer tabs over the two screws on either side of the power connector. Tighten both screws.
   b. Loosen the adjusting screw to allow the power cord to fit into the retainer.
   c. Repeat Steps 6a - 6b for the other retainer.
7. Connect the power cords to the power connectors on the SilkWorm 12000, inserting them through the retainers. The power cords are designed with right and left bends to facilitate cord management. Ensure each cord has a minimum service loop of 6 inches at the connection to the switch, and is not exposed to stress.
8. Tighten the adjusting screws on both retainers until the power cords cannot be disconnected.
9. Flip both AC switches to "1". The AC switches light up green.

Note: The SIlkWorm 12000 automatically performs POST (power-on self-test) by default each time it is powered on. POST takes a minimum of three minutes, and is complete when indicator light activity returns to standard state (for information about indicator light patterns, refer to the *SilkWorm 12000 Hardware Reference*).

Caution Do not connect the switch to the network until the IP address is correctly set. For instructions on how to configure the IP address, refer to the *SilkWorm 12000 Hardware Reference*, provided on the Brocade Documentation CD-ROM.

SILKWORM SWITCH FAMILY

The Brocade SilkWorm 12000 Core Fabric Switch provides a highly reliable and intelligent solution for deploying enterprise-class Storage Area Networks (SANs) in mission-critical environments.

SILKWORM 12000

Highlights

- Meets enterprise-class "five-nines" availability requirements with redundant, hot-pluggable components, no single points of failure, and non-disruptive software upgrades
- Simplifies enterprise SAN deployment by combining high port density with exceptional scalability, performance, reliability, and availability
- Leverages Brocade Secure Fabric OS to provide a comprehensive security platform for the entire SAN fabric
- Supports emerging storage networking technologies with a unique multiprotocol architecture
- Provides 1 and 2 Gbit/sec operation and the capability for seamless extension to 10 Gbit/sec in the future
- Employs Brocade Inter-Switch Link (ISL) Trunking to provide a high-speed data path of up to 8 Gbit/sec between switches
- Delivers up to 128 ports in a single 14U enclosure and up to 384 ports in a single rack, facilitating easily managed SAN fabrics composed of thousands of ports
- Provides FICON support for mainframe environments, including open systems and FICON intermix modes, cascaded FICON fabrics, and both 1 and 2 Gbit/sec FICON speeds

Offered by

Sun microsystems

BROCADE

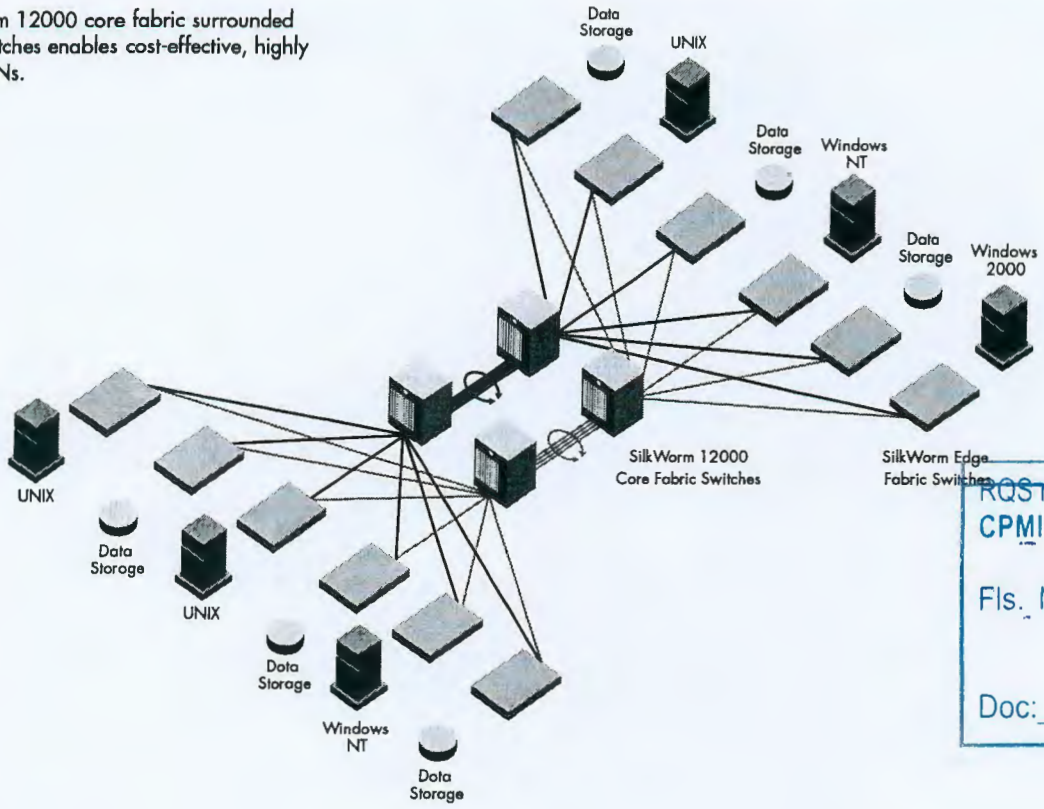
A High-port-density, Multiprotocol Switch for "Five-nines" Availability

As the industry's first 2 Gbit/sec director-class switch, the Brocade® SilkWorm® 12000 Core Fabric Switch provides unprecedented levels of availability, scalability, manageability, and security for open enterprise storage applications. Possible configurations range from a 32-port switch to dual 64-port switches in a single enclosure that provides "pay-as-you-grow" scalability.

Based on the Brocade Intelligent Fabric Services Architecture, the SilkWorm 12000 provides a reliable foundation for high-performance core-to-edge SANs that leverage proven core backbone networking methodologies. In addition, multiple SilkWorm 12000 switches can be interconnected at the core to form enterprise SAN fabrics capable of supporting thousands of hosts and storage devices in mission-critical environments (see Figure 1).

The SilkWorm 12000 provides higher levels of performance and availability than other director-class switches while supporting a more intelligent and scalable networked storage model. Moreover, the SilkWorm 12000 is designed to integrate with heterogeneous environments that include multiple operating systems such as Windows NT, UNIX, Linux, Solaris, AIX, and others. As a result, organizations have the flexibility to build cost-effective and easy-to-manage enterprise SAN fabrics. These capabilities make the SilkWorm 12000 ideal for mission-critical business continuance applications such as LAN-free back-up, remote mirroring, data replication, and high-availability clustering.

Figure 1. A SilkWorm 12000 core fabric surrounded by SilkWorm edge switches enables cost-effective, highly scalable enterprise SANs.



ULTRA-HIGH AVAILABILITY THROUGHOUT THE FABRIC

The core-to-edge SAN model features redundancy within the core fabric switch as well as a high-availability network approach for the entire fabric. Combining the proven reliability of the SilkWorm family with enterprise-class availability features, the SilkWorm 12000 provides a SAN fabric with built-in redundancy and no single point of failure. This infrastructure is capable of delivering overall system availability greater than 99.999 percent—the "five nines" of availability. Other key availability features include:

- Non-disruptive software upgrades
- Fabric Shortest Path First (FSPF) traffic rerouting
- Dual-redundant control processors with stateful failover
- Redundant, hot-swappable components
- Redundant power and cooling subsystems

INDUSTRY-LEADING PERFORMANCE

The SilkWorm 12000 is designed to provide high-performance switching at the core of large SANs. All external Fibre Channel ports can operate at 1 and 2 Gbit/sec per port (inbound and outbound) at distances up to 40 km. In addition, auto-sensing and speed-matching of data traffic ensures interoperability between 1 and 2 Gbit/sec devices. With Brocade Extended Fabrics software and Dense Wave Division Multiplexing (DWDM) technology, ISLs can span up to 120 km over Metropolitan Area Networks (MANs)—extending SAN connectivity without significantly inhibiting performance. This long-distance capability makes the SilkWorm 12000 ideal for disaster recovery solutions.

To provide even higher performance in the core, Brocade ISL Trunking combines up to four ISLs between a pair of switches into a single, logical high-speed trunk running at up to 8 Gbit/sec. Organizations can provision multiple trunk groups to meet even higher bandwidth requirements.

FICON SUPPORT

The SilkWorm 12000 supports the FICON protocol for mainframe environments, enabling organizations to utilize a single platform for both open systems and mainframe storage networks. The SilkWorm 12000 supports intermix mode, the ability to run both open systems Fibre Channel and FICON traffic on a port-by-port basis within a single switch. The Brocade FICON implementation also supports cascaded FICON fabrics as well as both 1 and 2 Gbit/sec FICON speeds. In addition, industry-leading security features provide the highest levels of protection for mission-critical enterprise data and applications.

INTELLIGENCE WITHIN THE SWITCH

To improve security and manageability, Brocade Frame Filtering intelligence is built directly into the SilkWorm 12000 ASIC technology. This design enables the unique capability of hardware-enforced zoning based on World Wide Name (WWN) for greater security and easier management. Organizations can also use Brocade Advanced Performance Monitoring to improve end-to-end performance analysis on a fabric-wide basis. This optional feature helps reduce storage costs by improving SAN performance tuning, resource optimization, and administrator productivity.

SUPERIOR RELIABILITY, AVAILABILITY, AND SERVICEABILITY

Enterprise-class SilkWorm 12000 reliability features include the following:

- Redundant control processors provide continuous performance during failovers and enable non-disruptive firmware upgrades.
- Continuous monitoring of environmental components improves

reliability and availability.

- Redundant, hot-swappable components help ensure continuous operation, even if critical components require servicing.
- Power-On Self-Test (POST), online/offline diagnostics, and per-port statistics enable organizations to monitor ports and diagnose problems without disrupting switch operations.
- Error detection and fault isolation facilities automatically disable failing ports and restart them when the problem has been resolved.
- Call-home capabilities through Brocade Fabric Manager enable remote notification of system events.

SE[illegible] UPGRADES, COST-EFFECTIVE MIGRA[illegible]N, AND INVESTMENT PROTECTION

To help protect existing technology investments, the SilkWorm 12000 provides a seamless upgrade path and backward and forward compatibility with SilkWorm entry, midrange, and port aggregation offerings. As SAN technologies evolve, the SilkWorm 12000 architecture is designed to integrate with emerging storage networking protocols such as iSCSI and FC-IP. The current design is fully extendable to future 10 Gbit/sec technologies with a switch module upgrade rather than a forklift upgrade of the entire system.

A NEW LEVEL OF SAN SECURITY

The SilkWorm 12000 supports Brocade Secure Fabric OS®, the most comprehensive fabric-based security architecture available. Based on state-of-the-art networking security technology, this architecture addresses a wide variety of vulnerabilities within the SAN fabric. Advanced security features such as Public Key Infrastructure (PKI) authentication and Access Control Lists (ACLs) provide powerful tools for securing SAN access and supporting mission-critical applications. In addition, software- and hardware-enforced Brocade Advanced Zoning helps secure data by preventing unauthorized access.

OPEN SAN MANAGEMENT

The SilkWorm 12000 simplifies management by networking both core and edge switches under Brocade Fabric OS, the embedded operating system. In addition to centralizing management, this approach enables heterogeneous device connectivity, automatic data routing and rerouting, self-healing ISL Trunking capabilities, and scalable connectivity. Moreover, the Brocade Fabric Access API enables software vendors to develop feature-rich management applications that leverage the underlying distributed intelligence of Brocade SANs.

INTELLIGENT SAN MONITORING

To simplify SAN monitoring and maintenance, the SilkWorm 12000 provides the following functions:

- Fabric OS enables value-added Brocade SAN fabric monitoring and an ecosystem of management applications through the industry-leading, open Brocade Fabric Access API.
- Industry-standard Management Information Base (MIB) support enables SNMP-based management platforms to access switch information.
- Network administrators can manage switch configurations through a command line interface for automated scripting or through the GUI-based Brocade WEB TOOLS.

CONSULTING AND SUPPORT SERVICES

Sun's Storage Services are an essential part of delivering complete storage solutions. Sun Professional Services can help you plan, architect, and implement your SAN and Sun Educational Services can help train and certify your staff to operate your SAN at its peak capability. Meet your 24x7 mission critical requirements for maximum uptime using Sun Support Services.

SILKWORM 12000 CORE FABRIC SWITCH SPECIFICATIONS

System [illegible]hitecture

[illegible]ibre Channel ports	128 ports, universal (E, F, and FL); up to eight 16-port Fibre Channel modules
[illegible]ontrol processor	Redundant (active/standby) control processor modules with automatic failover
[illegible]calability	Full fabric architecture: 239 switches maximum
[illegible]erformance	1.063 Gbit/sec line speed, full duplex; 2.125 Gbit/sec line speed, full duplex; auto-sensing of 1 Gbit/sec and 2 Gbit/sec port speeds; optionally programmable to fixed port speed; speed matching between 1 Gbit/sec and 2 Gbit/sec ports
[illegible]SL Trunking	Up to four 2.125 Gbit/sec ports per ISL trunk; up to 8.5 Gbit/sec per ISL trunk
[illegible]ggregate bandwidth	512 Gbit/sec end-to-end
[illegible]witch latency	<2.1 µsec any port to any port at 2 Gbit/sec, cut-through routing
[illegible]laximum frame size	2112-byte payload
Frame buffers	108 per 4-port group, dynamically allocated
Classes of service	Class 2, Class 3, Class F (inter-switch frames)
Port types	FL_Port, F_Port, and E_Port; self-discovery based on switch type (U_Port); optional port type control
Data traffic types	Fabric switches supporting unicast, multicast (255 groups), and broadcast
Media types	Hot-pluggable, industry-standard Small Form-Factor Pluggable (SFP), LC connector; Short-Wavelength Laser (SWL), up to 500 m (1,640 ft); Long-Wavelength Laser (LWL), up to 10 km (6.2 mi); Extended Long-Wavelength Laser (ELWL), up to 40 km (24.8 mi); distance depends on fiber optic cable and port speed
Fabric services	Simple Name Server; Registered State Change Notification (RSCN); Brocade Advanced Zoning; WEB TOOLS; Fabric Watch; Extended Fabrics; Remote Switch; ISL Trunking; Advanced Performance Monitoring

SILKWORM 12000

High Availability

Control processor	Redundant (active/standby) control processor modules; automatic and non-disruptive failover; non-disruptive software upgrades; dual-flash memory on each control processor to store two software images
Modules	Hot-swappable
Backplane	Fully passive
Input power	Dual AC inputs
Chassis power	Four AC-DC power supply modules, 2N redundant
Cooling	Three blower assembly modules (two operational required)

Management

Management	Telnet; SNMP (FE MIB, FC Management MIB); WEB TOOLS; Fabric Watch; Fabric Access layer
Management access	10/100 Ethernet (RJ-45), in-band over Fibre Channel (requires fabric); two serial ports (DB-9) per control processor module
Diag[illegible]s	POST and embedded online/offline diagnostics

Mechanical Specifications

Mounting	Rack mountable in a standard 19 in. EIA rack; Telco-style mid-mounting available
Ports per rack	Up to 384 ports per 42U rack
Enclosure	Rear panel-to-door airflow
Size	43.74 cm (17.22 in.) width 61.24 cm (24.11 in., 14U) height 70.90 cm (27.90 in.) depth without door 74.20 cm (29.20 in.) depth with door
Weight	98 to 113 kg (215 to 250 lb)

Environment

Temperature	Operating: 0°C to 40°C
[illegible]midity	Operating: 20% to 85% non-condensing at 40°C
Altitud[illegible]	0 to 3 km
Shock	20 g, 6 ms, half sine
Vibration	Operating: 0.5 g p-p, 5 to 500 Hz; Non-operating: 2.0 g, 5 to 500 Hz
Heat dissipation	1960 Watts (6700 BTU/hour) fully loaded

Power

Supported power range	Nominal: 200 to 240 VAC, single phase Operational: 180 to 264 VAC auto-sensing Maximum 2300 Volt-Amps Maximum 12 Amps
In-rush current	40A maximum, < 1/4 AC cycle, per AC input
Frequency	47 to 63 Hz

Fibre Channel Standards

Standard	Revision
FC-AL-2	NCITS 332: 1999
FC-FLA	NCITS TR-20:1998
FC-GS-4	rev 7.6
FC-FS	Rev 1.7
FC-PI	Rev 13
FC-PLDA	NCITS TR-19: 1998
FC-SW-3	Rev 6.3
FC-VI	Rev 1.61
IPFC	RFC 2625
FCP-2	Rev 7
SCSI Enclosure Services	Rev 8b
FC-SB-2	Rev 2.1
FC-FS	Rev 1.7
FC-MI	Rev 1.92
FC-DA	Rev 1.5
FC-SB-3	Rev 1.2

Regulatory Compliance

	Safety	EMC
Canada	CSA 60950	ICES-003 Class A
United States	UL 60950	FCC Part 15 Class A
Japan	IEC60950	VCCI Class A
European Community	EN60950 TUV, NEMKO	EN55022 Level A EN55024
Australia/New Zealand		AS/NZS 3548
International	IEC 60950	CISPR 22

For additional information on this product, go to *www.sun.com/storage/san*

Sun Microsystems, Inc. 901 San Antonio Road, Palo Alto, CA 94303-4900 USA **Phone** 1-650-960-1300 or 1-800-555-9SUN **Web** sun.com/storage

Sun microsystems
We make the net work.

BROCADE
The intelligent platform for networking storage

Brocade Fabric Manager is a powerful management platform for configuring and administrating multiple Brocade Storage Area Network (SAN) fabrics.

BROCADE FABRIC MANAGER

Highlights

- Provision, monitor, and administer large numbers of switches and multiple Brocade SAN fabrics with greater efficiency
- Perform management tasks across multiple devices and fabrics as a single management operation
- Intelligently group multiple Brocade switches or ports to facilitate aggregated management
- Visualize and track changes to SAN configuration and state information through multiple views at multiple levels of detail
- Launch Fabric Manager from other enterprise management applications as the "element manager" for the fabric or multiple fabrics
- Track SAN assets by using detailed table views that can be exported to a spreadsheet
- Discover details about devices logged into the fabric, including HBA asset information
- View the SAN layout through a topology map that specifies ISL, switch, and device details
- Identify, isolate, and manage SAN events across large numbers of switches and fabrics

A Complete SAN Management Tool for Brocade-Based SANs

Brocade® Fabric Manager is a powerful application that manages multiple Brocade SilkWorm® switches and fabrics in real time. In particular, Fabric Manager provides the essential functions for efficiently configuring, monitoring, dynamically provisioning, and managing Brocade SAN fabrics on a daily basis.

Through its single-point SAN management platform, Fabric Manager facilitates the global integration and execution of management tasks across multiple fabrics—thereby lowering the overall cost of SAN ownership. As a result, it provides a flexible and powerful tool optimized to provide organizations with rapid access to critical SAN information.

In addition, Fabric Manager is tightly integrated with other Brocade SAN management products, such as WEB TOOLS and Fabric Watch. Organizations can also use Fabric Manager in conjunction with other leading SAN and storage resource management applications as the drill-down element manager for a single or multiple Brocade fabrics.

BASIC FEATURES FOR HIGHLY EFFICIENT MANAGEMENT OF MULTIPLE SANS

By increasing the efficiency of the administrators who manage multiple Brocade SANs, Fabric Manager helps reduce provisioning, monitoring, and management time and costs. With the unique ability to provide real-time information and streamline SAN management tasks, Fabric Manager provides the following key capabilities:

- Manages multiple Brocade switch elements across multiple fabrics. It discovers and collects SAN data, and provides multiple views of that

BROCADE

BROCADE FABRIC MANAGER

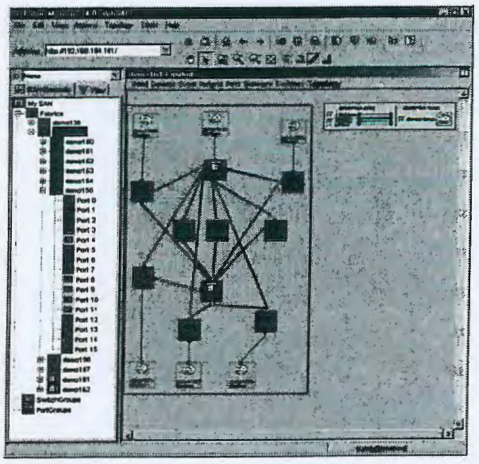


Figure 1.
To simplify management, the fabric explorer tree and the topology map show the true SAN fabric structure, including core-to-edge layouts.

- data—including topology maps (Figure 1) and detailed views.
- Shows the status of critical fabric elements and key discovery data at varying levels of detail, such as high-level "At-a-Glance" views (see Figure 2), and detailed tables that display information about switches, ports, devices, and events.

ADVANCED FEATURES FOR EVEN GREATER MANAGEMENT CAPABILITIES

Fabric Manager provides several unique methods for managing SANs, including:

- **Change management:** Provides a fabric snapshot/compare feature that tracks changes to fabric objects and fabric membership, enabling administrators to generate detailed change reports over time.
- **Fabric views at varying levels of details:** Supports cascading table views that reveal details about devices, ports, switches, and fabrics.
- **Brocade Secure Fabric OS® management:** Allows full control of Secure Fabric OS policy display and configuration, enabling administrators to securely control switch and device connectivity, management access, and other key functions.
- **Call Home support:** Facilitates remote support, fault isolation, and diagnosis to lower the cost of supporting Brocade SANs.
- **HBA management:** Discovers and tracks HBA asset data, and upgrades firmware from a central location without host-based agents.

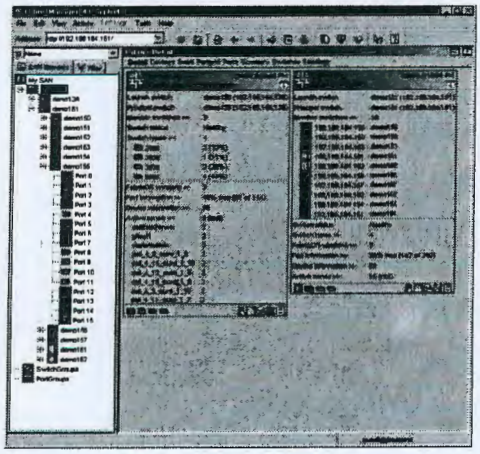


Figure 2.
The Fabric Manager "At-a-Glance" feature shows both SAN and group information at multiple levels of detail.

- **Fabric, switch, and port naming:** Enables the assignment of specific names to SAN objects.
- **Advanced license key management:** Securely manages Brocade license keys across all SAN fabrics under Fabric Manager control, while offering the capabilities to receive licenses from Brocade support and to support pre- and post-installation cross-checking of license keys.
- **Profiling, backup, and cloning:** Enables administrators to capture a switch configuration profile, back up the snapshot, and compare the backup to current switch configurations. In addition, cloning facilitates the distribution of profiles to switches within the fabric.
- **Scalable firmware download:** Provides a fully configurable environment for controlling the Brocade Fabric OS firmware upgrade process when utilized with sequenced reboot. To increase flexibility, this feature is dynamically configurable and scalable across logical groups, password controls, multiple fabrics, and SAN infrastructures with multiple security levels.

MAXIMIZING SAN INVESTMENTS

Brocade and its partners offer complete SAN solutions to meet a wide range of technology and business requirements. These solutions include education and training, support, service, and professional services to help optimize SAN investments. For more information, contact an authorized Brocade sales partner or visit **www.brocade.com**.

SYSTEM REQUIREMENTS

Operating system	Windows 2000 (Client/Server) Solaris 8 (Client only)
Memory/CPU	512 MB RAM/ 800 MHz CPU for managing up to 500 ports
	1024 MB RAM/ 1.5 GHz CPU for managing more than 500 ports
Hard drive storage	50 MB free disk space

BROCADE
The intelligent platform for networking storage

Corporate Headquarters
San Jose, CA USA
T: (408) 487-8000
info@brocade.com

European Headquarters
Geneva, Switzerland
T: +41 22 799 56 40
europe-info@brocade.com

Asia Pacific Headquarters
Tokyo, Japan
T: +81-3-5402-5300
apac-info@brocade.com

Latin America Headquarters
Miami, FL USA
T: (305) 716-4165
latinam-sales@brocade.com

BROCADE

Brocade Fabric Manager

User's Guide Version 4.0

Publication Number: 53-0000823-02
Publication Date: 04/25/03

Chapter 4

Common Fabric Manager Tasks

This chapter includes the following sections:

Introduction

This chapter explains how to perform common Fabric Manager tasks. More complicated or mission-critical tasks appear in separate chapters later in this user's guide.

Discover a Fabric

You must *discover* a fabric to add it to the **SAN Elements** tab and administer it with Fabric Manager. To discover a fabric, perform the following steps:

1. Place your cursor in the **Address** field and delete the contents of the field.
2. In the **Address** field, enter the IP address or switch name of a switch in the fabric that you want to administer and press **Enter**.

Note: You do not need to include **http://** before the IP address to discover a fabric.

Run a Subnet Scan

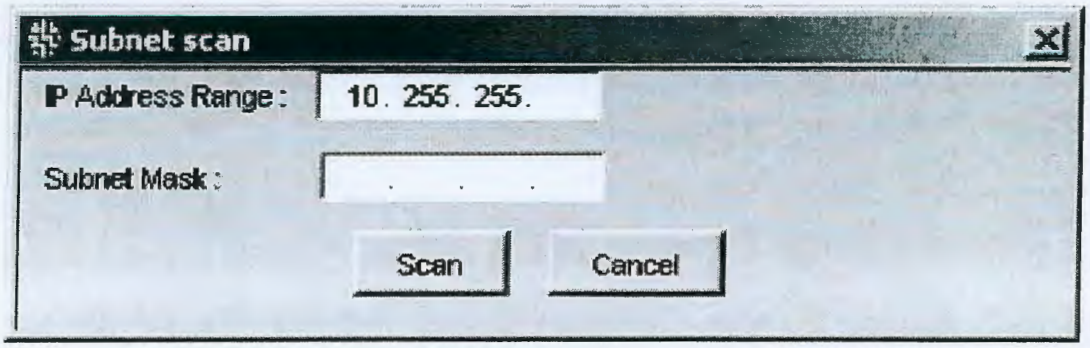
Fabric Manager can scan a subnet to discover fabrics. With this discovery mechanism, you do not need to know the exact address of a switch to discover a fabric. When you specify a subnet, Fabric Manager lists the switches and fabrics that it finds so you can add them to the **SAN Elements** tab.

Note: Switches may appear in your subnet scan even after you unplug the ethernet cables of those switches.

To run a subnet scan, perform the following steps:

1. From the **Tools** menu, select **Subnet scan...** The **Subnet scan** dialog opens.
2. Enter the first three sets of digits of an IP address in the first three sections of the **IP Address Range** field.

Example



3. Enter a wildcard in the last section of the **IP Address Range** field to represent the range of scan. Choose from one of the following three options:

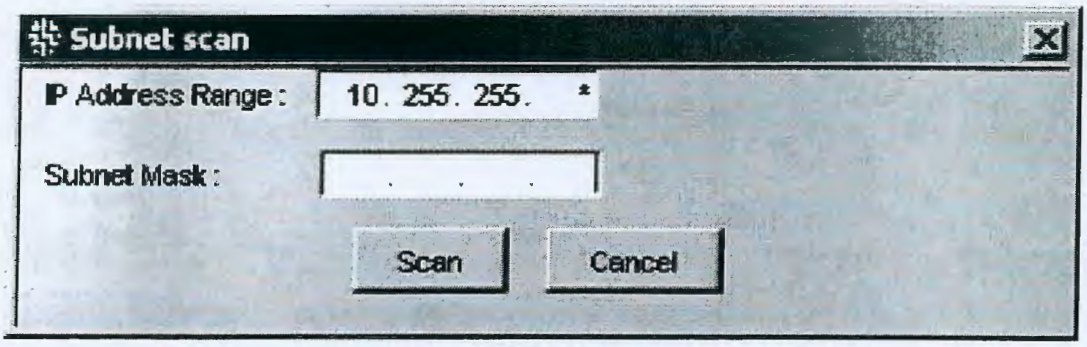
   a. **192.168.168.*** discovers any fabric in the address range of 192.168.168.0 - 192.168.168.255.

   b. **192.168.168.1**** discovers any fabric in the address range of 192.168.168.100 - 192.168.168.199. (The first digit in the wildcard cannot exceed a value of two; see note.)

   c. **192.168.168.11*** discovers any fabric in the address range of 192.168.168.110 - 192.168.168.119. (See note.)

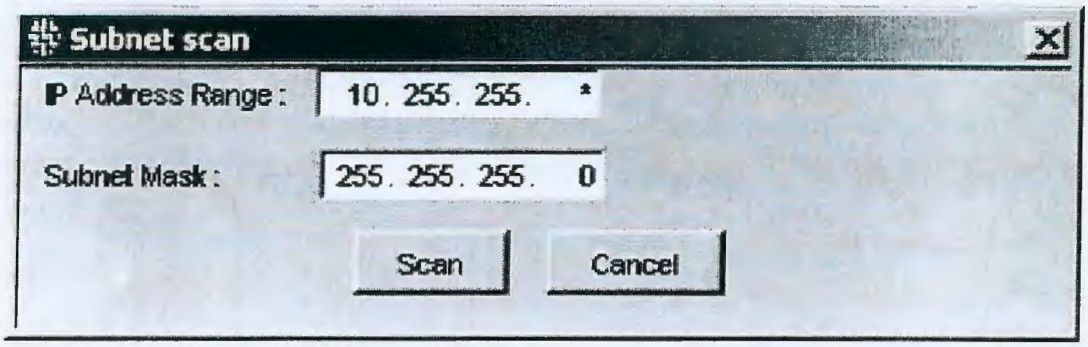
Note: The number before the "*"can be any number so long as the resulting range is between 0 and 255. For example, you cannot enter 192.168.168.3**, or 192.168.168.26*. Also, if you enter 192.168.168.25*, the range will be 192.168.168.250 - 192.168.168.255.

Example



4. Enter a subnet mask to avoid scanning the IP address for the network or broadcasting.

Example



5. Click **Scan**. The scan result appears. IP addresses that appear as underlined links with two angle brackets (>>) represent fabrics. Click the link to view the switches in the fabric.

Note: To add a switch or fabric to your **SAN Elements** tab, click the checkbox next to the element, then click the **Add** button.

Delete a Fabric

To no longer monitor a fabric with Fabric Manager, perform the following steps:

1. In the **SAN Elements** tab, click the fabric that you want to remove from Fabric Manager.
2. Press the **Delete** key to remove the fabric. Fabric Manager will prompt you to make sure that you want to delete the fabric.

Tip: You can also select **Delete** from the Actions menu to remove the selected fabric from Fabric Manager.

Note: Switches and ports from this fabric that you added to logical switchgroups and portgroups still appear in the groups.

Manually Refresh a Fabric

All At-A-Glance Views are updated at 20 second intervals; everything else in the GUI is updated whenever there is a change in current data. If you notice a discrepancy between the data displayed in Fabric Manager and the fabric itself, perform a manual refresh (or "re-discover") the fabric to update the GUI.

To refresh a fabric, perform the following steps:

1. In the **SAN Elements** tab, click the fabric that you want to refresh.
2. From the **Actions** menu, select **Refresh**.

Note: This action disables ISL Checking and Fabric Checking on your fabric. You must re-enable the features once the refresh is complete.

Rename a Fabric

When you discover a fabric, Fabric Manager assigns a name to that fabric that matches the name of the switch that you used to discover the fabric. For instance, to monitor a fabric that includes Switch_01, enter the IP address of Switch_01 in the Address field to discover the fabric. Fabric Manager then names that fabric Switch_01 and displays that name in the **SAN Elements** tab.

After you discover the fabric, you can assign a name to the fabric that serves a more useful purpose for you (for instance, "mktng_SAN" or "HQ"). To rename a fabric, perform the following steps:

1. In the **SAN Elements** tab, click the fabric that you want to rename.
2. From the **Edit** menu, select **Rename**. A cursor appears to the right of the current name.

Tip: You can also use the F2 key or triple-click a fabric, switch, or port icon to rename it.

3. Rename the fabric and press **Enter**.

Rename a Switch

To rename a switch, perform the following steps:

1. In the **SAN Elements** tab, click the switch that you want to rename.
2. From the **Edit** menu, select **Rename**. A cursor appears next to the name of the switch in the **SAN Elements** tab.
3. Edit the name of the switch and press **Enter**.

Tip: You can also use the F2 key or triple-click a fabric, switch, or port icon to rename it.

Rename a Port

When you rename a port on a switch that runs firmware versions other than 3.1.0 and 4.1.0, the port name only applies to your local Fabric Manager view. If you rename a port on a switch that runs firmware versions 3.1.0 or 4.1.0, Fabric Manager propagates that name to the port and changes the port name on the switch, provided the Fabric Login information has been set up successfully. To rename a port, perform the following steps:

1. In the **SAN Elements** tab, click the port that you want to rename.
2. From the **Edit** menu, select **Rename**. A cursor appears next to the name of the switch in the **SAN Elements** tab.
3. Edit the name of the port and press **Enter**.

Tip: You can also use the F2 key or triple-click a fabric, switch, or port icon to rename it.

View SAN Information

To view information about a particular element of your SAN, *click the element immediately above it in the hierarchy.* When you click the "parent" element, information about the "child" element that you want to view appears in the right-hand view window.

When you click an element in the **SAN Elements** tab, Fabric Manager displays information about all immediately-subordinate elements in the hierarchy. For instance, if you click My SAN in Summary view, Fabric Manager displays summaries for Fabrics, SwitchGroups, and PortGroups. If you click a particular fabric in the hierarchy, Fabric Manager displays information on each switch in the fabric. If you click a particular group, Fabric Manager displays information on each member of the group.

Each view in the View menu displays different informational content, and you can customize which content appears. (For more information on how to customize views, refer to *Customize a View* on page 4-6.)

Table 4-1 provides a high-level description of what each view displays. For more detailed information on each view, refer to *View Menu Reference* on page C-1.

Table 4-1 Fabric Manager Views

View	Description
Detail	Provides information about the components and status of an element.
Devices	Provides information about all devices that connect to an element.
Event	Provides an event log for the element and the status reason.
Portgrid	Displays the node that connects to each port. **Note:** The Portgrid View displays devices only; it does not show ISL information.
Ports	Provides information about the status and traits of each port.
Summary	Provides a summarized version of Detail view. **Note:** Summary view provides the same view options as Detail view. Customize Summary view to display content that you frequently reference. Customize Detail view to provide a more thorough report. For more information, refer to *Customize a View* on page 4-6.
Switches	Provides information about the status and traits of each switch.
Topology	Provides a graphical display of topology.

Customize a View

Customize a view so that each time you select that view, it displays only the information that you want to see. To customize a view, perform the following steps:

1. Click an element in the **SAN Elements** tab.
2. From the **View** menu, select the view that you want to customize.
3. From the **Edit** menu, select **View Options...** The **Edit View Options** window appears.
4. Click an item, then click the appropriate directional arrow to add items to the display or remove items from the display. You can use the **Ctrl** and **Shift** keys to select multiple items at once. In the view display columns, designate the order of the columns as follows:
   a. Click an item in the Display Items field.
   b. Click an up or down directional arrow to change the order of the column in the display.
5. Click **OK**.

Change Pane Descriptions

When you change a pane description, you change the text that appears immediately below the name of the pane. To change a description, perform the following steps:

1. In the **SAN Elements** tab, click the element that you want to change.
2. From the **Edit** menu, select **Change Description**. The **Please enter the new description** dialog appears.
3. In the **New Description** field, enter a description for the pane and click **OK**. To view the description, click the parent element in the **SAN Elements** tab. The new description appears on the appropriate pane.

Log In to Multiple Switches Simultaneously

You can use Fabric Manager to log in to multiple switches at the same time. With multiple login, you do not need to log in to each switch individually to administer your fabric. After you log in to a switch, Fabric Manager stores your login information and automatically logs you in to the switches. You must log in to a switch to perform the following Fabric Manager tasks:

- firmware download to HBAs and switches
- license key installation
- fabric compare and merge
- date/time synchronization
- baseline configuration upload/download
- sequenced reboot
- security policy configuration
- fabric backup
- diff with backup

To log in to multiple switches, perform the following steps:

1. From the **File** menu, select **Fabric Login...**
2. Select switches or fabrics from the **SAN Elements** tab and click the right-hand arrow to move them to the **Selected Switches** window.

Note: Click-and-drag fabrics or switches to quickly move switches into the **Selected Switches** window.

---

3. In the **User Id** field, enter your user ID.
4. In the **Password** field, enter your password.
5. Click **Apply**. The success or failure of the login appears in the **Status** column of the **Selected Switches** window. A key icon (🔑) appears next to each switch and fabric that completes a successful login.

Note: If you did not log in to all of the switches successfully, remove the successful switches from the Selected Switches window and retry with a new user ID and password.

Select Identity

Fabric Manager lets you view SAN elements by the identifier that you find most useful. Because you can identify most SAN elements in multiple ways (for instance, you can identify a switch by IP address, domain ID, WWN, and name), Fabric Manager lets you choose the identifier that you want. When you select identity, you choose the type of identifier that Fabric Manager displays for each element.

To select identity, perform the following step:

1. From the **ID** pulldown menu, select the type of identifier that you want to use to label the elements in your display.

Navigate Fabric Manager

Click elements, menus, views, and navigation buttons to navigate Fabric Manager. As you move from view to view and element to element, Fabric Manager tracks your views so you can use the navigation buttons to move back and forth between the selections that you made from the View menu and view selector. The sections that follow describe the navigation tools that Fabric Manager provides.

Navigate with Elements and Views

To navigate Fabric Manager, you must select different elements and different views. Fabric Manager provides the following two ways to access different views:

1. From the **View** menu, select the view that you want to access.
2. Use the view selector.

   To use the view selector, perform the following steps:

   1. Click the **Display view selector** icon ( ) in the top right-hand corner of the interface. The view selector appears.

Figure 4-1 View Selector

   2. In the view selector, click the view that you want to access.

Note: The icon that displays the view selector ( ) serves other functions when it appears in other locations. Only the icon in the top right-hand corner of the interface will display the view selector.

Table 4-2 provides a list of views and explains the information that each view displays. For more detailed information about each view, refer to *View Menu Reference* on page C-1.

Table 4-2 Fabric Manager Views

View	Description
Detail	Provides information about the components and status of an element.
Devices	Provides information about all devices that connect to an element.
Event	Provides an event log for the element and the status reason.
Portgrid	Displays the node that connects to each port. **Note:** The Portgrid View displays devices only; it does not show ISL information.
Ports	Provides information about the status and traits of each port.
Summary	Provides a summarized version of Detail view. **Note:** Summary view provides the same view options as Detail view. Customize Summary view to display content that you regularly reference. Customize Detail view to provide a more thorough report. For more information, refer to *Customize a View* on page 4-6.
Switches	Provides information about the status and traits of each switch.
Topology	Provides a graphical display of topology.

Navigate with Navigation Buttons and History

Fabric Manager maintains a history of the views that you visit. Use the navigation buttons to move forward and backward through views that you have already accessed. Use navigation buttons as follows:

- Click the **Back** button ( ) to return to the previous view.
- Click-and-hold the **Back** button to display a list of the views that you have visited, then drag the mouse to the view you want to see and release the mouse button.
- Click the **Forward** button ( ) to move forward to the next view in your view history.
- Click-and-hold the **Forward** button to display a list of the views that you have visited, then drag the mouse to the view you want to see and release the mouse button.
- Click the **Home** button ( ) to display the view that appeared when you launched Fabric Manager.

Customize Tables

With Fabric Manager you can change the order and size of columns that appear in views such as Portgrid and Switches. With customizable tables, you can do the following:

- Click-and-drag table headers to change the order in which columns appear in the table.
- Click-and-drag the border between column headers to resize columns.

- Click column headers to organize information in ascending or descending order by that column.

Note: The **Status** column in Portgrid view and Switches view sorts contents by severity when you click the column header.

Copy Tables to Spreadsheet Applications

Fabric Manager tables migrate quickly and easily to spreadsheet applications. To copy a table to a spreadsheet application, perform the following steps:

1. Navigate to a view that displays a table.
2. From the **Edit** menu, select **Copy Table**.
3. Open a spreadsheet application.
4. From the **Edit** menu, select **Paste**.

Enable/Disable Elements

You can use Fabric Manager to quickly disable or enable large numbers of switches or ports across multiple switches or fabrics. To enable or disable elements, perform the following steps:

1. Verify that you have logged-in to all necessary switches. You cannot enable or disable a port or switch until you log in to that switch. For more information on how to log in, refer to *Log In to Multiple Switches Simultaneously* on page 4-7.
2. From the **SAN Elements** tab, select the switches, ports, or groups that you want to disable.
3. From the **Actions** menu, select **Disable/Enable...** and click the appropriate option.

Note: The switch enable/disable menu item enabling/disabling is based on switch status, i.e. when the switch is disabled then only switch enable menu item is enabled, the switch disable menu item is greyed out, and vice versa. For telnet, switch enable/disable commands can be executed regardless of switch status.

Configure Log Parameters

Configure log parameters to set the file log path and priority levels for Fabric Manager log information. When you configure the level of each log, you designate what errors Fabric Managers saves to the file log and what errors appear when you open the Fabric Manager log. Changes made to logging paths and log levels are dynamic and do not require an application restart to take effect.

Caution: Do not change log parameters unless support personnel instruct you to do so.

To configure log parameters, perform the following steps:

1. From the **File** menu, select **Options...** The **Options** window opens.
2. From the **Configurations** navigation tree, click **Log Parameters**.
3. In the **Log Directory Path** field, enter a directory or click **Browse** to select a directory to store the log directory.
4. From the **FabricManager Log Level** pulldown menu, select a severity level. Fabric Manager will log all events of that severity level and lower.
5. From the **File Log Level** pulldown menu, select a severity level. Fabric Manager will log all events of that severity level and lower.
6. Click **OK**.

Print

Fabric Manager can print the following views:

- Devices
- Event
- Portgrid
- Ports
- Switches
- Topology

To print a view, perform the following steps:

1. From the **View** menu, select a view that Fabric Manager can print.
2. From the **File** menu, select **Print...** The Print dialog opens.
3. Select a printer and click **OK**.

Print in One Page

To print a view in one page, perform the following steps:

Note: The option to print in one page applies exclusively to Topology view.

1. From the **View** menu, select a view that Fabric Manager can print.
2. From the **File** menu, select **Print In One Page...** The Print dialog opens.
3. Select a printer and click **OK**.

Download a Configuration

With Fabric Manager, you have the opportunity to download a configuration from a saved baseline file or from a switch. During the download process, you can selectively choose the settings that you want to download and the settings that you want to omit. For instructions on saving a baseline configuration to a file, refer to *Save a Baseline Configuration to a File* on page 16-2.

Download to Switches from a Baseline File

To download a baseline file to one or more switches, perform the following steps:

1. From the **Tools** menu, select **Config > Compare/Download from File**. The **Compare/Download from File -- Select Baseline Configuration** dialog opens.
2. Navigate to the baseline file and click **Open**. The **Compare/Download from File -- Target Switch Selection** window opens.
3. From the **SAN Elements** tab, select switches you want to compare and move them to the right-hand window and click **OK**. You can
   - Navigate to a switch, click the switch, then click the right-pointing arrow.
   - Click-and-drag a switch from the **SAN Elements** tab to the right-hand window.
   - Press-and-hold **Ctrl**, click multiple switches in the **SAN Elements** tab, and click the right-pointing arrow.
   - Press-and-hold **Ctrl**, click multiple switches, and click-and-drag the switches from the **SAN Elements** tab to the right-hand window.
   - Click-and-drag a fabric to the right-hand window to move add all of the switches in that fabric to the window.

   The **Compare/Download from File -- Switch Configuration comparison and Download** window opens.
4. Click **Apply Baseline...**

Note: The delay timer at the bottom of the **Apply Baseline...** dialog cannot be configured from this dialog. It is propagated from current settings in the sequenced reboot group and represented by the combination of "Fabric Stabilization timeout" and "Delay after Fabric Stabilization" parameters.

Note: Prompts will appear to ensure that you do now download a configuration accidentally.

The **Apply Baseline** window opens. The **root** navigation tree divides the switches into the following two groups:

- Non-Reboot Config Group: these switches are Linux-based and do not need to reboot after a config download.
- Reboot Config Group: these switches are VXWorks-based and must reboot after a config download.

5. Click **Apply**. Fabric Manager will prompt you to be sure that you want to proceed. The download proceeds one group at a time. The status of the switches appears in the right-hand window.

Download to Switches from a Baseline Switch

To download a configuration from a baseline switch to one or more switches, perform the following steps:

1. From the **Tools** menu, select **Config > Compare/Download from Switch**. The **Compare/ Download from Switch -- Source Configuration Selection** window opens.
2. Navigate to the switch that you want to use as a baseline and click the right-pointing arrow to move that switch to the right-hand window.
3. Click **OK**. The **Compare/Download from Switch -- Target Switch Selection** window opens.
4. From the **SAN Elements** tab, select switches you want to compare and move them to the right-hand window. You can
   - Navigate to a switch, click the switch, then click the right-pointing arrow.
   - Click-and-drag a switch from the **SAN Elements** tab to the right-hand window.
   - Press-and-hold **Ctrl**, click multiple switches in the **SAN Elements** tab, and click the right-pointing arrow.
   - Press-and-hold **Ctrl**, click multiple switches, and click-and-drag the switches from the **SAN Elements** tab to the right-hand window.
   - Click-and-drag a fabric to the right-hand window to move add all of the switches in that fabric to the window.
5. Click **Apply Baseline...**

Configure File Transfer Options

To configure file transfer options, perform the following steps:

1. From the **File** menu, select **Options...** The **Options** window opens. The **Options** window is displayed in Figure 4-2.

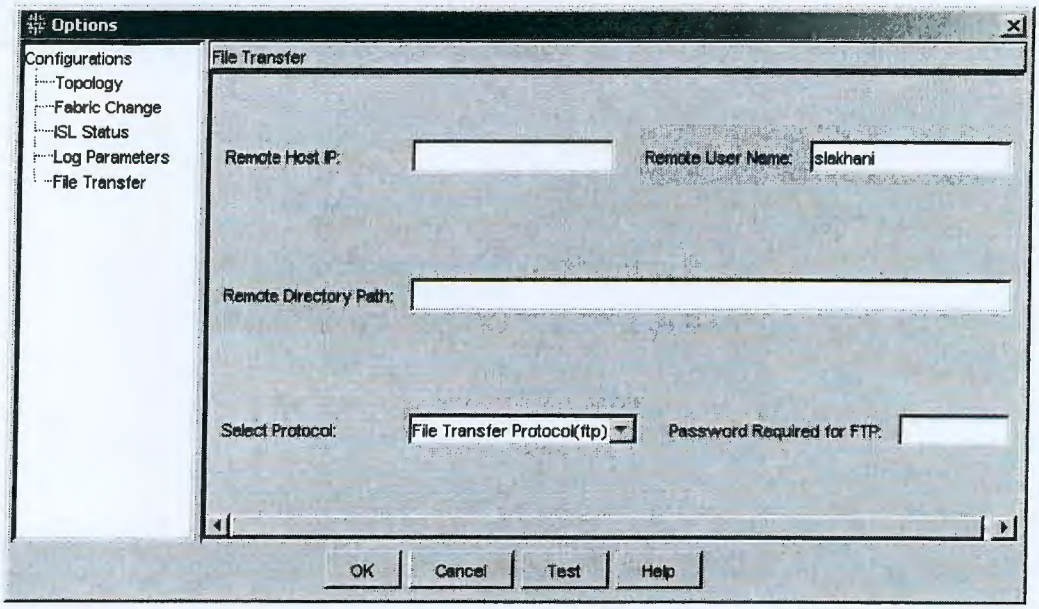


Figure 4-2 Options Window

2. The default view in the Options window is the File Transfer view. If the File Transfer view is not displayed, select File Transfer from the Configurations navigation tree. The **Configurations** navigation tree is displayed in Figure 4-3.

Figure 4-3 Options Window Configurations Tree

3. In the **Remote Host IP field**, enter the IP address of your FTP server.
4. In the **Remote User Name** field, enter your login name.
5. In the **Remote Directory Path** field, enter a default FTP directory.

Note: Do not enter a file name, only a directory.

6. From the Select Protocol pulldown menu, select **File Transfer Protocol(ftp)**.
7. In the **Password Required for FTP** field, enter your password and click **OK**.
8. Click **Test** to ensure that you can access the FTP server specified. Fabric Manager will report success or failure.

9. Click **OK** to save settings.

Synchronize Time and Date Across a Fabric

You can synchronize time and date across an entire fabric. Because the firmware timestamps entries in the port log dump, you can more easily correlate events when you synchronize your fabric.

Note: To synchronize time and date, you must choose fabrics, not switch groups.

To synchronize time and date, perform the following steps:

1. Log in to the switches in the fabric that you want to synchronize. For more information, refer to *Log In to Multiple Switches Simultaneously* on page 4-7.
2. In the **SAN Elements** tab, click the fabric that you want to synchronize.
3. From the **Action** menu, select **Set Time...** The **Time** dialog opens. The **Time** dialog is displayed in Figure 4-4.

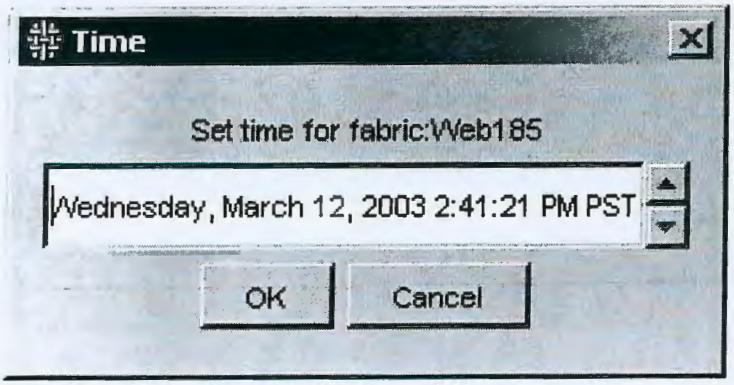


Figure 4-4 Time Dialog

4. To adjust the time or date, click the appropriate field in the **Time** dialog and use the up and down arrows to iterate the value, then click **OK**.

Filter Elements

The Filter tab consists of the following three components:

- a text field
- a pulldown menu
- a **SAN Elements** field

To use the Filter tab, perform the following steps:

1. From the pulldown menu, select an identifier. For more information, refer to *Filter Tab* on page 3-4.
2. In the text field, type text (letters, numbers, or symbols such as a period) that appears in the elements that you want to view. For instance, to view elements that all include **switch** in the name, select **Name** from the pulldown menu and enter **switch** in the text field. To view elements that include **10.32** in the IP address, select **IP** from the pulldown menu and enter **10.32** in the text field.
3. Press Enter. Every element that includes the text that you entered appears in the **SAN Elements** field.

Designate a Switch as a Core Switch

Note: This procedure applies only to Core Edge topologies.

All switches defined in the FCS policy of a secure fabric are considered core switches. Any switches with devices attached to them are automatically considered edge switches. For more information, refer to *Topology View* on page C-16. If you want to manually assign a core switch, perform the following steps:

1. From the **SAN Elements** tab, click the switch that you want to designate.
2. From the **Actions** menu, select **Core Switch**. When you view the fabric to which that switch belongs in Topology view and select the core-edge layout, your switch will appear as a core switch.

Chapter 6

Grouping

This chapter includes the following sections:

Introduction

Logical *groups* consist of SAN elements (either switches or ports) that you select to monitor as a unit. When you click a group in the **SAN Elements** tab and select Summary view, you immediately see the status of the switches or ports that you added to the group. You can use groups to

- Simplify monitoring.
- Simplify management.
- Organize switches by function, switch type, firmware version, or any other criteria that you choose.
- Create functional hierarchies of groups.

Create groups of similar switches and ports so you can monitor and configure them as a unit instead of individually. For instance, if you create a group of switches that run the same firmware, you can download new firmware to those switches as a group, rather than one by one. Whenever you need to perform the same task on multiple switches, you can save time if you create a group and perform that task on the group. Examples of such tasks include

- Multiple switch login.
- Simultaneous firmware downloads.
- Fabric-wide license key activations.

Note: A switch can appear in multiple groups at the same time.

Groups persist on your server in your FabricManager.xml file. You can import and export groups so that multiple users can share group definitions.

Note: Switches remain in a group even if you remove their source fabrics from Fabric Manager. That is, if switch X is in fabric Y and you add it to group Z, switch X remains in group Z even after you delete fabric Y from Fabric Manager.
Furthermore, when you look at a logical switch group in the Topology view, links will disappear if the switches that are in this group are no longer in the SAN Elements tab in Fabric Manager.

Best Practices

The following list describes valuable ways to use Fabric Manager groups:

- Create groups of switch model types or firmware versions to expedite firmware downloads.
- Group switches by function to monitor switches that belong to different departments or that serve as a backbone to the SAN.
- Group switches by physical location to monitor fabrics in disparate locations.
- Group switches by SAN island to monitor or update individual islands
- Group switches by redundancy so you can maintain half of a fabric while the other half continues to carry traffic.
- Nest fabrics to drill down to the source of a problem. For instance, if you create a switch group for a campus, then nest within that switch groups for departments, you can move down the hierarchy to determine the source of any status change.
- Create separate groups for monitoring and management to reduce unnecessary levels of nesting.
- Group ports by certain devices and hosts to more easily monitor those elements.
- Use groups to simplify the monitoring view of a large or complex fabric.

Note: When you remove a switch from a fabric, you must remove that switch from all group definitions because Fabric Manager does not do so dynamically. For the same reason, if you replace the switch with a new switch, you must add that switch to all applicable group definitions.

Create a Group

With Fabric Manager, you can create a group of switches or a group of ports. Group switches together that serve similar purposes (for instance, all core switches or all switches that run the same firmware) and group ports together that serve similar purposes (for instance, all E_Ports).

Create SwitchGroups

A switch group consists of a collection of switch identifiers. After you create a group, you can click-and-drag that group during tasks to work with all switches at once. For instance, if you want to log in to all of the switches in a group, you can drag the group into the appropriate window so you do not need to select each individual switch. To create a group of switches, perform the following steps:

1. From the **File** menu, select **Groups > Edit Switch Groups...** The **Edit Switch Groups** dialog box appears.
2. Click the **SwitchGroups** icon in the right-hand window.

   Note: The group that you create appears nested within the item that you click in this step. If you click an existing group instead of the **SwitchGroups** icon, your new group will appear as a subgroup of that group. After you create a group, you can click-and-drag it to a new location in the hierarchy.

3. Click **Create...** The **Create Group** dialog box appears.

4. Type a name for your group in the **Name** field and click **Okay**.
5. Click the icon of the group that you created.
6. In the left-hand window, click the switch that you want to add to your group, then click the right-pointing arrow to add the switch to the group.

Note: To add multiple switches at once, press and hold the **Ctrl** key as you click additional switches or simply click-and-drag any node in the tree to add the switches from that node.

Note: Click-and-drag switches directly from the left-hand window to the switch group to more quickly populate the group.

7. Click **OK** after you add switches to your group. The group appears in the **SAN Elements** tab under **SwitchGroups**. To view the contents of the group, click the group.

Create PortGroups

A port group essentially consists of a collection of port identifiers. After you create a group, you can click-and-drag that group during tasks to work with all ports at once. Perform the following steps to create a group of ports:

1. From the **File** menu, select **Groups > Edit Port Groups...** The **Edit Port Groups** dialog box appears.
2. Click the **PortGroups** icon in the right-hand window.

Note: The group that you create appears nested within the item that you click in this step. If you click an existing group instead of the **PortGroups** icon, your new group will appear as a subgroup of that group. After you create a group, you can click-and-drag it to a new location in the hierarchy.

3. Click **Create...** The **Create Group** dialog box appears.
4. Type a name for your group in the **Name** field and click **Okay**.
5. Click the icon of the group that you created.
6. In the left-hand window, click the port that you want to add to your group, then click the right-pointing arrow to add the port to the group.

Note: To add multiple ports at once, press and hold the **Ctrl** key as you click additional ports.

Note: Click-and-drag ports directly from the left-hand window to the port group to more quickly populate the group.

7. Click **OK** when you have finished adding ports to your group. The group appears in the **SAN Elements** tab under **PortGroups**. To view the contents of the group, click the group.

Delete a Group

1. From the **File** menu, select **Groups > Edit {Switch | Port}Groups...** The **Edit {Switch | Port} Groups** dialog box appears.
2. In the right-hand window, navigate to the group that you want to delete and click that group.
3. Click **Delete**, then click **OK**.

Tip: You can also select the group you want to delete from the SAN Elements tab and press **Delete** on your keyboard to delete a group.

Export Groups

When you create a group, that group exists in your FabricManager.xml file. To share your group definitions with other users, export the group so another user can import the group.

To export a group, perform the following steps:

1. From the **File** menu, select **Groups > Export...** The **Export** dialog box appears.
2. Click the **Browse...** button, navigate to the file to which you want to export the group, and click **Open**.
3. Under the **SAN Elements** tab in the left window, click the group or groups that you want to add to the file.

Note: You must select the parent group in order to import the parent group and all of its sub-groups at a later time.

4. Click the arrow to add the group(s) to the file, then click **Save**.

Import a Group

Import groups to add group definitions from other users to your personal profile so you do not need to recreate the groups yourself. To import a group, perform the following steps:

1. From the **File** menu, select **Groups > Import...** The **Import from file:** dialog box opens.
2. Navigate to the file that contains the group that you want to import. Click the file, then click **Open**. The groups in the file appear under the **SAN Elements** tab under the appropriate groups type.

Chapter 8

Zoning

This chapter includes the following sections:

Introduction

Fabric Manager uses Advanced Web Tools to configure and administer zoning. This chapter provides high-level zoning instructions, then goes into detail about zoning concepts and practices.

Note: Specific Advanced Web Tools interfaces vary by firmware. Your interface and functionality may not match the interface that appears in the figures and examples in this chapter.

Zoning enables you to partition your SAN into logical groupings of devices that can access each other. For example, you can partition your SAN into two zones, *winzone* and *unixzone*, so that your Windows servers and storage do not interact with your UNIX servers and storage. To configure zoning, you must use zones, aliases, and configurations.

Zone

A zone is a region within the fabric where switches and devices can communicate. A device can only communicate with other devices connected to the fabric within its specified zone. You can specify members of a zone based on the following identifiers:

- alias names
- switch domain and port area number pairs (for example, "2, 20")
- WWNs
- QuickLoop AL_PAs

Alias

An alias is a logical group of ports, WWNs, or AL_PAs. Specifying groups of ports or devices as an alias makes zone configuration easier, by enabling you to configure zones using an alias rather than a long string of individual members. You can specify members of an alias using the following methods:

- A switch domain and port area number pair

  Example

  2,20

- WWN (device)
- QuickLoop AL_PAs (device)

Configuration

A configuration (often called a config) is a group of zones. Zoning is enabled on a fabric by enabling a specific configuration. You can specify members of a configuration with the following identifiers:

- zone names
- QuickLoop names
- Fabric Assist (FA) zone names

Zoning Schemes

Various levels of zoning (or zoning *schemes*) isolate systems that have different operating environments. For example, you can create a zone of all ports connected to UNIX servers, or another zone of all ports connected to Windows servers. Zones limit access of devices to other devices connected to the fabric within the same zone.

Zones can be configured dynamically. They can vary in size depending on the number of fabric connected devices, and devices can belong to more than one zone. Because zone members can access only other members of the same zone, a device not included in a zone is not available to members of that zone.

Security

When you enable security, you can only access zoning with the primary FCS switch. The zoning icon does not appear on any other switch in the display. If you do not enable security, you can configure zoning from any switch.

Zoning Methods

Zoning methods determine what appears in the subsequent components of the **Zone Administration** window. You can use four methods to define members of a zone. Each method is considered either hard zoning or soft zoning. Hard zoning defines alias members exclusively with domain/port ID pairs or with WWNs. Soft zoning defines alias members with a mixture of port IDs and WWNs. Table 8-1 lists and describes the methods.

Table 8-1 Zoning Methods

Method	Description
Mixed Zoning	This method enables you to define members using the port area number, device WWNs, QuickLoop AL_PAs. This method is considered soft zoning.
Port Zoning	This method enables you to define members using port area number only. This method is considered hard zoning.
WWN Zoning	This method enables you to define members of zone using device WWNs. This method is considered hard zoning.
AL_PA Zoning	This method enables you to define members of zone using QuickLoop AL_PAs only. This method is considered hard zoning.

Zoning Method and Tabs Available

Depending on the zone method that you use, certain tabs may or may not be available on the **Zone Administration** window.

Table 8-2 Zone Methods and Tabs Table

Zone Level	Available Tabs
Mixed Zoning	Alias, Zone, QuickLoop, Fabric Assist, Config
Port Zoning	Alias, Zone, QuickLoop, Fabric Assist, Config
WWN Zoning	Alias, Zone, QuickLoop, Fabric Assist, Config
AL_PA Zoning	Alias, Zone, QuickLoop, Config

Access the Zone Administration Window

To access the Zone Administration window, perform the following steps:

1. From the **View** menu, select **Summary**.
2. In the **SAN Elements** tab, click the fabric that you want to view.
3. From the **Actions** menu, select **Zone Admin...** Web Tools launches and prompts you to log in.

4. Log in to Advanced Web Tools. The **Zone Administration** window opens.

View the Zone Configuration Summary

To view the **Zone Configuration summary**, perform the following steps:

1. Access the **Zone Administration** window. For more information, refer to *Access the Zone Administration Window* on page 8-3.
2. Select **File > Print Summary**. The **Zone Configuration summary** dialog box appears. An example of the **Zone Configuration summary** is shown in Figure 8-1.

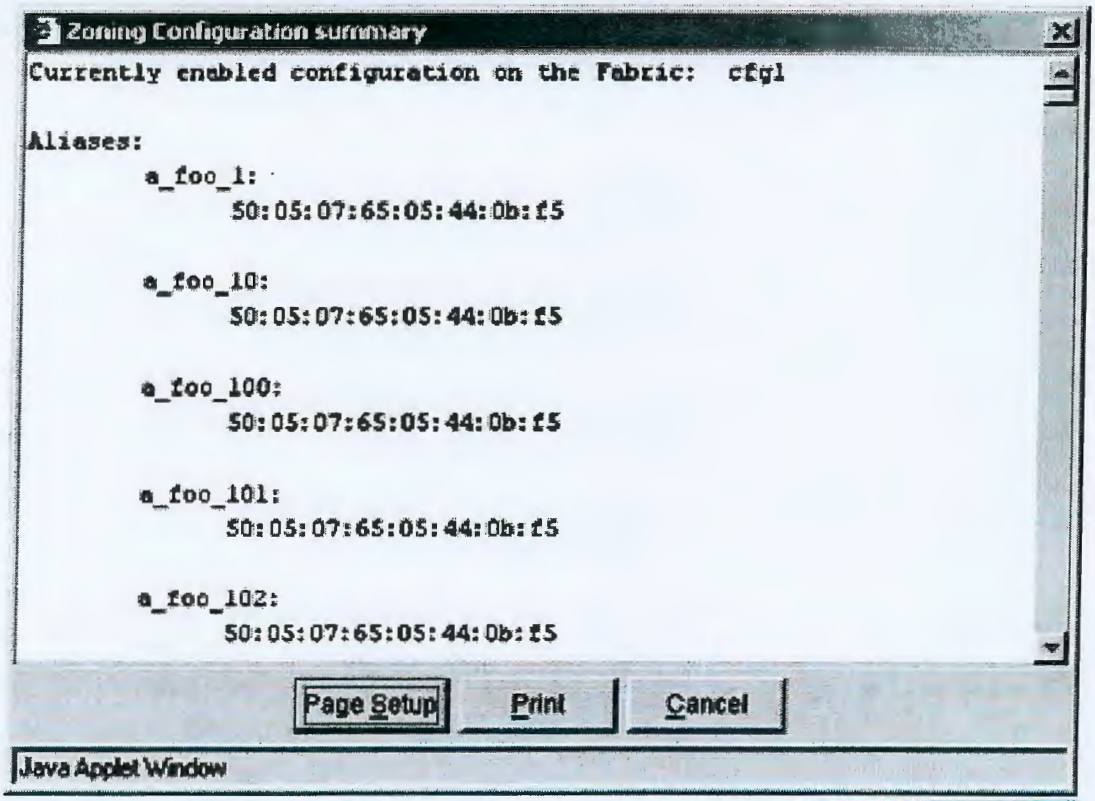


Figure 8-1 Zone Configuration Summary

Add a WWN in the Zoning Database

To add a WWN to the zoning database, perform the following steps:

1. Access the **Zone Administration** window. For more information, refer to *Access the Zone Administration Window* on page 8-3.
2. Select **Edit > Add a WWN**. The **Add WWN...** dialog box appears.
3. Enter a WWN value in the **WWN** field.

4. Click the **OK** button. The WWN is added to the zoning database and can be used as a member.

Note: This WWN added does not need to currently exist in the fabric. This procedures enables you to configure a WWN as a member in a zone configuration before you add that device to the fabric.

Delete a WWN in the Zoning Database

To delete a WWN from the zoning database, perform the following steps:

1. Access the **Zone Administration** window. For more information, refer to *Access the Zone Administration Window* on page 8-3.
2. Select **Edit > Delete a WWN**. The **Delete WWN...** dialog box is displayed.
3. Enter a WWN value in the **WWN** field.
4. Click the **OK** button. The WWN is deleted from the zoning database and as a member from any alias or zone.

Replace a WWN in the Zoning Database

This procedures enables you to replace a WWN throughout the zoning database. This is helpful when exchanging out devices in your fabric, and easily maintaining your current Configuration. To replace a WWN in the zoning database, perform the following steps:

1. Access the **Zone Administration** window. For more information, refer to *Access the Zone Administration Window* on page 8-3.
2. Select **Edit > Replace a WWN**. The **Replace WWN...** dialog box is displayed.
3. Enter the WWN to be replaced in the **Replace** field.
4. Enter the new WWN in the **By** field.
5. Click the **OK** button. The old WWN is replaced in the zoning database by the new WWN, including within any alias or zone where the old WWN was a member.

Search for a Zone Member

To search for a zone member, perform the following steps:

1. Access the **Zone Administration** window. For more information, refer to *Access the Zone Administration Window* on page 8-3.
2. Select **Edit > Search Member**.
3. Type the zone member name in the **Member Name** field.
4. (Optional) Check one or more checkboxes to narrow the search.
5. Click the **Next** button to begin the zone member search.

Select a Zoning Method

The zoning method you choose determines how members appear in the various member selection windows. It also determines whether you are using hard zoning or soft zoning.

1. Access the **Zone Administration** window. For more information, refer to *Access the Zone Administration Window* on page 8-3.
2. From the **View** pulldown menu, select one of the following:
   - **Mixed Zoning**
   - **Port Zoning**
   - **WWN Zoning**
   - **AL_PA Zoning**

   The zoning method that you choose determines how members appear in the various member selection windows. Refer to *Zoning Methods* on page 8-3 for more information.

Refresh Zoning

To refresh zoning, perform the following steps:

1. Access the **Zone Administration** window. For more information, refer to *Access the Zone Administration Window* on page 8-3.
2. From the **View** menu, select **Refresh Zoning** to refresh the zoning database and delete any unsaved changes. You can view the current zoning database from the **Zone Configuration Summary** window. For more information, refer to *View the Zone Configuration Summary* on page 8-4.

Refresh the Fabric

To refresh the fabric, perform the following steps:

1. Access the **Zone Administration** window. For more information, refer to *Access the Zone Administration Window* on page 8-3.
2. From the **View** menu, select **Refresh Fabric** to refresh the enabled zone configuration on the fabric and delete any unsaved changes. You can view the current zoning database from the **Zone Configuration Summary** window. For more information, refer to *View the Zone Configuration Summary* on page 8-4.

Enable a Configuration

The **Actions > Enable a Config** option enables a configuration that has previously been created (refer to *Create a Configuration* on page 8-15). A dialog box appears; select the desired configuration from the pulldown menu.

Several configurations can reside on a switch at once and you can quickly alternate between configurations. For instance, you may want to enable one configuration during the business hours, and enable another overnight. You can only enable one zone configuration at a time.

To create a new configuration, refer to *Create a Configuration* on page 8-15. To enable a configuration, perform the following steps:

1. Access the **Zone Administration** window. For more information, refer to *Access the Zone Administration Window* on page 8-3.
2. Click the **View** pulldown menu.
3. Select the desired level of zoning.
4. Select the **Config** tab.
5. Select **Actions > Enable Config** to activate a configuration. The **Enable Config** dialog box appears. Figure 8-2 shows the **Enable Config...** dialog.

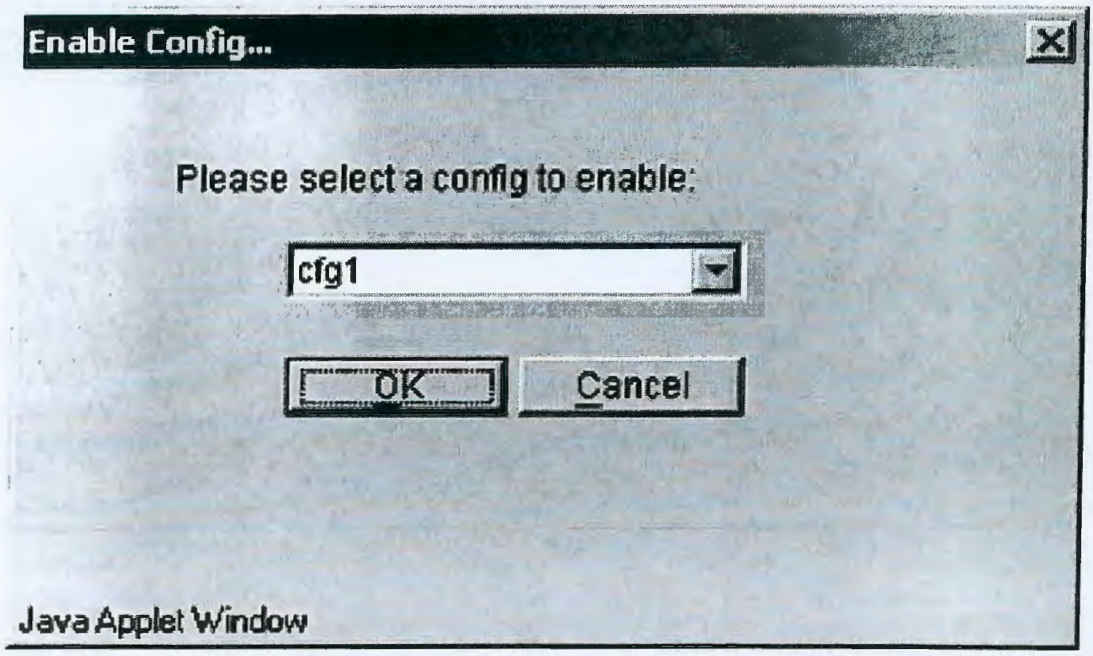


Figure 8-2 Enable Config Dialog Box

6. Select the configuration to be enabled from the pulldown menu. A warning dialog box appears.
7. Click the **Yes** button to enable the selected configuration.

Disable Zoning

The **Actions > Disable Zoning** option disables the enabled configuration. The **Disable Config** dialog box appears. When you disable the zoning feature, the fabric enters non-zoning mode and all devices can freely access other devices in the fabric.

When you disable the active configuration, the zoning feature is disabled on the fabric and all devices within the fabric can communicate with all other devices. This does not mean that the zoning database is deleted however, only that there is no configuration active on the fabric. To disable zoning, perform the following steps:

1. Access the **Zone Administration** window. For more information, refer to *Access the Zone Administration Window* on page 8-3.
2. Select **Actions > Disable Zoning** to disable the current enabled configuration. The **Disable Config** warning appears.
3. Click the **Yes** button to disable the current configuration.

Save Changes to an Existing Configuration

To save changes to an existing configuration, perform the following steps:

1. Access the **Zone Administration** window. For more information, refer to *Access the Zone Administration Window* on page 8-3.
2. Click the **Config** tab.
3. Make desired changes to configuration (refer to *Create a Zone* on page 8-10).

Note: You can make changes to a configuration that is currently enabled; changes will not appear until the configuration is disabled and re-enabled.

4. Select the **Actions > Save Config Only** option.

Note: The configuration changes will be saved. Changes will not take effect until the configuration is re-enabled.

To enable the configuration, refer to *Enable a Configuration* on page 8-6.

Clear the Zoning Database

The following procedure disables any active configuration and deletes the entire zoning database.

1. Access the **Zone Administration** window. For more information, refer to *Access the Zone Administration Window* on page 8-3.
2. Select the **Actions > Clear All** option. The **Disable Config** warning appears.

Caution: This action will not only disable zoning on the fabric, but will deleted the entire zoning database.

3. Click the **Yes** button to disable the current configuration.

Create an Alias

To create an alias, perform the following steps:

1. Access the **Zone Administration** window. For more information, refer to *Access the Zone Administration Window* on page 8-3.
2. Select the **View** menu to determine the method used to view members. The different methods are as follows:
   - Mixed Zoning
   - Port Zoning
   - WWN Zoning
   - AL_PA Zoning

   The member view method you choose determines how members are displayed in the **Member Selection List** window. Refer to *View Menu* on page H-3 for more information.
3. Click the **Alias** tab (selected by default).
4. Click the **Create Alias** button. The **Create New Alias** dialog box appears.
5. Enter a name for the new alias.
6. Click the **OK** button.
7. Click on any "+" signs in the **Member Selection List** to view the nested elements. The choices available in the **Member Selection List** depend on the selection that you made in the **View** menu.
8. Highlight an element in the **Member Selection List** that you want to include in your alias. The **Add Member** button becomes active.
9. Click the **Add Member** button to add alias members. Selected members move to the **Alias Members** window.
10. Repeat step 7 and step 8 to add more elements to your alias.
11. Use the **Add Other** button to include a WWN, port, or QuickLoop (AL_PA) that is not currently a part of the fabric (optional).

    The new alias appears in the **Name** pulldown list.

Modify the Members of an Alias

To modify the members of an alias, perform the following steps:

1. Access the **Zone Administration** window. For more information, refer to *Access the Zone Administration Window* on page 8-3.
2. Select the **Alias** tab (selected by default).
3. From the **Name** pulldown menu, select the alias you want to modify.
4. Highlight an element in the Member Selection List that you want to include in your alias; or, highlight an element in the **Alias Members** field that you want to delete.
5. Click the **Add Member** button to add an alias member or click the **Remove Member** button to remove an alias member.

Delete an Alias

To delete an alias, perform the following steps:

1. Access the **Zone Administration** window. For more information, refer to *Access the Zone Administration Window* on page 8-3.
2. Select the **Alias** tab (selected by default).
3. From the **Name** pulldown menu, select the alias you want to delete.
4. Click the **Delete** button. The **Confirm Deleting Alias** dialog opens.
5. Click the **OK** button to delete the alias from the zoning database.

Rename an Alias

To rename an alias, perform the following steps:

1. Access the **Zone Administration** window. For more information, refer to *Access the Zone Administration Window* on page 8-3.
2. Select the **Alias** tab (selected by default).
3. From the **Name** pulldown menu, select the alias you want to rename.
4. Click the **Rename** button. The **Rename an Alias** dialog box appears.
5. Enter a new alias name and click **OK**.

Create a Zone

To create an zone, perform the following steps:

1. Access the **Zone Administration** window. For more information, refer to *Access the Zone Administration Window* on page 8-3.
2. Select the **View** menu to determine the method used to view members. The different methods include the following:
   - Mixed Zoning
   - Port Zoning
   - WWN Zoning
   - AL_PA Zoning

   The member view method that you choose determines how members are displayed in the **Member Selection List** window. For more information, refer to *View Menu* on page 14-3.
3. Select the **Zone** tab.
4. Click the **Create** button. The **Create New Zone** dialog box appears.
5. Enter a name for the new zone and click the **OK** button.
6. Click on any "+" signs in the **Member Selection List** to view the nested elements. The choices available in the **Member Selection List** depend on the selection made in the **View** menu.

7. Highlight an element in the **Member Selection List** that you want to include in your Zone. The **Add Member** button becomes active.
8. Click the **Add Member** button or use drag and drop to add zone members. Selected members move to the **Zone Members** window.
9. Repeat step 7 and step 8 to add more elements to your zone.
10. Use the **Add Other** button to include a WWN, port, or QuickLoop (AL_PA) that is not currently a part of the fabric (optional). The new zone appears in the **Name** pulldown menu.

Modify the Members of a Zone

To modify the members of a zone, perform the following steps:

1. Access the **Zone Administration** window. For more information, refer to *Access the Zone Administration Window* on page 8-3.
2. Select the **Zone** tab.
3. From the **Name** pulldown menu, select the zone that you want to modify.
4. Highlight an element in the **Member Selection List** that you want to include in your zone; or, highlight an element in the **Zone Members** field that you want to delete.
5. Click the **Add Member** button to add a zone member or click the **Remove Member** button to remove an zone member.

Delete a Zone

To delete a zone, perform the following steps:

1. Access the **Zone Administration** window. For more information, refer to *Access the Zone Administration Window* on page 8-3.
2. Select the **Zone** tab.
3. From the **Name** pulldown menu, select the zone you want to delete.
4. Click the **Delete** button. The **Confirm Deleting Zone** dialog opens.
5. Click the **OK** button.

Rename a Zone

To rename a zone, perform the following steps:

1. Access the **Zone Administration** window. For more information, refer to *Access the Zone Administration Window* on page 8-3.
2. Select the **Zone** tab.
3. From the **Name** pulldown menu, select the zone you want to rename.
4. Click the **Rename** button. The **Rename a Zone** dialog box appears.

5. Enter a new zone name and click the **OK** button.

Create a QuickLoop

To create a QuickLoop, perform the following steps:

1. Access the **Zone Administration** window. For more information, refer to *Access the Zone Administration Window* on page 8-3.
2. From the **View** menu, select one of the following methods:
   - Mixed Zoning
   - Port Zoning
   - WWN Zoning
   - AL_PA Zoning

   The method that you choose determines how members appear in the **Member Selection List** window. For more information, refer to *View Menu* on page H-3.
3. Select the **QuickLoop** tab.
4. Click the **Create** button. The **Create New QuickLoop** dialog box appears.
5. Enter a name for the new QuickLoop and click the **OK** button.
6. Highlight an element in the **Member Selection List** that you want to include in your QuickLoop. (Click on any "+" signs in the **Member Selection List** to view the nested elements. The choices available in the **Member Selection List** depend on the selection made in the **View** menu.) The **Add Member** button becomes active.

Note: There is a limit of 2 members per QuickLoop.

---

7. Click the **Add Member** button to add QuickLoop members. Selected members move to the **QuickLoop Members** field.
8. Repeat step 6 and step 7 to add more elements to your QuickLoop.
9. Use the **Add Other** button to include a WWN, port, or QuickLoop (AL_PA) that is not currently a part of the fabric (optional).

   The new QuickLoop appears in the **Name** pulldown menu.

Modify the Members of a QuickLoop

To modify the members of a QuickLoop, perform the following steps:

1. Access the **Zone Administration** window. For more information, refer to *Access the Zone Administration Window* on page 8-3.
2. Select the **QuickLoop** tab.
3. From the **Name** pulldown menu, select the QuickLoop you want to modify.
4. Highlight an element in the **Member Selection List** that you want to include in your QuickLoop or highlight an element in the **QuickLoop Members** that you want to delete.

5. Click the **Add Member** button to add a QuickLoop member or click the **Remove Member** button to remove an QuickLoop member.

Delete a QuickLoop from the Database

To delete a QuickLoop, perform the following steps:

1. Access the **Zone Administration** window. For more information, refer to *Access the Zone Administration Window* on page 8-3.
2. Select the **QuickLoop** tab.
3. From the **Name** pulldown menu, select the QuickLoop you want to delete.
4. Click the **Delete** button. The **Confirm Deleting QuickLoop** dialog opens.
5. Click the **OK** button.

Rename a QuickLoop

To rename a QuickLoop, perform the following steps:

1. Access the **Zone Administration** window. For more information, refer to *Access the Zone Administration Window* on page 8-3.
2. Select the **QuickLoop** tab.
3. From the **Name** pulldown menu, select the QuickLoop you want to rename.
4. Click the **Rename** button. The **Rename a QuickLoop** dialog box appears.
5. Enter a new QuickLoop name.
6. Click the **OK** button.

Create a Fabric Assist Zone

To create a Fabric Assist zone, perform the following steps:

Note: This example uses the Mixed Zone level.

---

1. Access the **Zone Administration** window. For more information, refer to *Access the Zone Administration Window* on page 8-3.
2. Enter the admin level user name and password.
3. From the **View** menu, select **Mixed Zoning**. (You can select any view except for the Devices view.) The **Mixed View** tab appears.
4. Select the **Fabric Assist** tab.
5. Select the **Create** button. The **Create New FA** dialog box appears.
6. Enter a name for the new FA zone and click the **OK** button. (A fabric host is required.)

7. Highlight the desired Fabric Assist zone members from the **Member Selection List**.
8. Click the **Add Member** button. The new members appear in the **Fabric Assist Members** window. The newly created FA zone also appears in the **Config** tab.

Modify the Members of a Fabric Assist Zone

To modify the members of a Fabric Assist zone, perform the following steps:

1. Access the **Zone Administration** window. For more information, refer to *Access the Zone Administration Window* on page 8-3.
2. Select the **Fabric Assist** tab.
3. From the **Name** pulldown menu, select the Fabric Assist Zone that you want to modify.
4. Highlight an element in the **Member Selection List** that you want to include in your Fabric Assist zone; or, highlight an element in the **Fabric Assist Zone Members** field that you want to delete.
5. Click the **Add Member** button to add a Fabric Assist zone member or click the **Remove Member** button to remove an Fabric Assist zone member.

Delete a Fabric Assist Zone

To delete a Fabric Assist zone, perform the following steps:

1. Access the **Zone Administration** window. For more information, refer to *Access the Zone Administration Window* on page 8-3.
2. Select the **Fabric Assist Zone** tab.
3. From the **Name** pulldown menu, select the Fabric Assist zone you want to delete.
4. Click the **Delete** button. The **Confirm Deleting Fabric Assist Zone** dialog opens.
5. Click the **OK** button.

Rename a Fabric Assist Zone

To rename a Fabric Assist zone, perform the following steps:

1. Access the **Zone Administration** window. For more information, refer to *Access the Zone Administration Window* on page 8-3.
2. Select the **Fabric Assist** tab.
3. From the **Name** pulldown menu, select the Fabric Assist zone that you want to rename.
4. Click the **Rename** button. The **Rename a Fabric Assist Zone** dialog box appears.
5. Enter a new Fabric Assist zone name and click the **OK** button.

Create a Configuration

To create an configuration, perform the following steps:

1. Access the **Zone Administration** window. For more information, refer to *Access the Zone Administration Window* on page 8-3.
2. From the **View** menu, select one of the following methods:
   - Mixed Zoning,
   - Port Zoning,
   - WWN Zoning,
   - AL_PA Zoning.

   The member view method that you choose determines how members appear in the **Member Selection List** window. Refer to *View Menu* on page H-3 for more information.
3. Select the **Config** tab.
4. Click the **Create** button. The **Create New Config** dialog box appears.
5. Enter a name for the new configuration and click the **OK** button.
6. Click on any "+" signs in the **Member Selection List** to view the nested elements.
7. Highlight an element in the **Member Selection List** that you want to include in your configuration. The **Add Member** button becomes active.
8. Click the **Add Member** button to add configuration members. Selected members move to the **Config Members** field.
9. Repeat step 7 and step 8 to add more elements to your configuration.
10. Select the **Actions > Save Config Only** option. The new configuration appears in the Name pulldown list. To enable the configuration, refer to *Enable a Configuration* on page 8-6.

Note: Any changes made to the currently enabled configuration will not appear until the configuration is re-enabled.

Modify the Members of a Configuration

To modify the members of a configuration, perform the following steps:

1. Access the **Zone Administration** window. For more information, refer to *Access the Zone Administration Window* on page 8-3.
2. Click the **Config** tab.
3. From the **Name** pulldown menu, select the configuration that you want to modify.
4. Click an element in the **Member Selection List** that you want to include in your configuration or click an element in the **Config Members** that you want to delete.

5. Click the **Add Member** button to add a configuration member or click the **Remove Member** button to remove a member from a configuration.

Note: You can make changes to a configuration that is currently enabled; changes will not appear until the configuration is disabled and re-enabled.

6. Select the **Actions > Save Config Only** option.

Note: The configuration changes will be saved. Changes will not take effect until the configuration is re-enabled.

To enable the configuration, refer to *Enable a Configuration* on page 8-6.

Delete a Configuration

You cannot delete a currently enabled configuration.

To delete a configuration, perform the following steps:

1. Access the **Zone Administration** window. For more information, refer to *Access the Zone Administration Window* on page 8-3.
2. Select the **Config** tab.
3. From the **Name** pulldown menu, select the configuration you want to delete.
4. Click the **Delete** button. The **Confirm Deleting Config** dialog opens.
5. Click the **OK** button.

Rename a Configuration

To rename a configuration, perform the following steps:

1. Access the **Zone Administration** window. For more information, refer to *Access the Zone Administration Window* on page 8-3.
2. Select the **Config** tab.
3. From the **Name** pulldown menu, select the configuration you want to rename.
4. Click the **Rename** button. The **Rename a Config** dialog box appears.
5. Enter a new **Config** name and click the **OK** button.

Note: You can make changes to a configuration that is currently enabled; changes will not appear until the configuration is disabled and re-enabled.

6. Select the **Actions > Save Config Only** option.

Note: The configuration changes will be saved. Changes will not take effect until the configuration is re-enabled.

To enable the configuration, refer to *Enable a Configuration* on page 8-6.

Create a Configuration Analysis Report

1. Access the **Zone Administration** window. For more information, refer to *Access the Zone Administration Window* on page 8-3.
2. Select the **Config** tab.
3. From the **Name** pulldown menu, select a configuration to analyze.
4. Select the **Analyze Config** button. An analysis window appears. An example of an analysis report is shown in Figure 8-3.

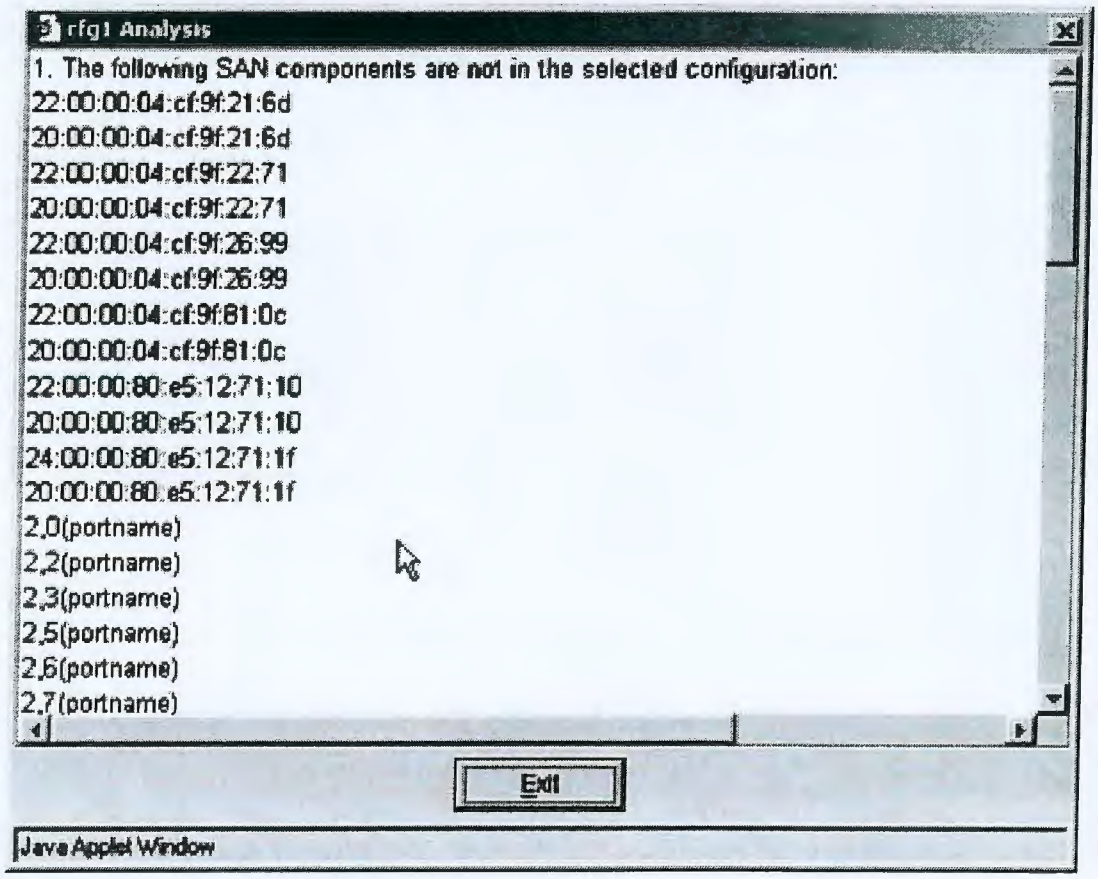


Figure 8-3 Analyze Config Report Example

5. View the Configuration Analysis. A report appears that lists the following:
   - SAN components (ports, WWNs, and AL_PAs) that are not included in the configuration.
   - SAN components (ports, WWNs, and AL_PAs) that are contained in the configuration but not in the fabric.

Chapter 14

Fabric Checking

This chapter includes the following sections:

Introduction

You can configure the Fabric Checking feature to monitor the fabric and registers events when you add switches to or remove switches from the fabric. When you add or remove a switch from a selected fabric, Fabric Checking adds an entry to the switch event log and changes the status color of the fabric. You can configure Fabric Checking to ignore additions to the fabric, but the software always registers an event when you remove a switch.

Fabric Manager polls the fabric every fifteen seconds to determine if the fabric has changed. Table 14-1 lists the changes that Fabric Checking monitors and describes how the software responds to the change.

Table 14-1 Fabric Checking Alerts

Change	Response
switch disconnects from fabric	Fabric Manager creates a "ghost" switch image that lasts until you restore the switch to the fabric or disable Fabric Checking. The following actions take place to represent the changes in Fabric Manager: • Fabric Manager adds an entry to the switch event log stating that the switch has been removed from the fabric. • Fabric Manager changes the status color of the fabric. • A "ghost" switch image appears in the Topology View, At-A-Glance View(s), and the Switch table. • Entries for the "ghost" switch are removed from the portgrid, ports, and devices tables.
switch connects to fabric	Fabric Manager adds an entry to the switch event log and changes the status color of the fabric.

Note: Fabric Checking monitors *switches* (not devices) removed from and added to a fabric.

Advantage

Fabric Checking allows users to know when changes occur in the fabric. If you administer a fabric that you want no one to add switches to or remove switches from, Fabric Checking helps you monitor that activity.

Enable Fabric Checking on a Fabric

To enable Fabric Checking, perform the following steps:

1. In the **SAN Elements** tab, click the fabric that you want to check.
2. From the **Actions** menu, select **Fabric Checking**. A dark blue ring appears around the icon in the SAN Elements tab, the Topology View, and the At-A-Glance views to indicate that you enabled Fabric Checking.

Reset Fabric Checking

Reset Fabric Checking after you make a permanent addition or deletion to your fabric. To reset Fabric Checking, perform the following steps:

1. In the **SAN Elements** tab, click the fabric that you want to reset.
2. From the **Actions** menu, select **Fabric Checking** to disable fabric checking on the fabric.
3. From the **Actions** menu, select **Fabric Checking** to enable Fabric Checking with the new topology.

Automatically Enable Fabric Checking on All Fabrics

To automatically enable fabric checking on all fabrics that Fabric Manager discovers, perform the following steps:

1. From the **File** menu, select **Options...** The **Options** dialog box appears. This dialog box is displayed in Figure 14-1.

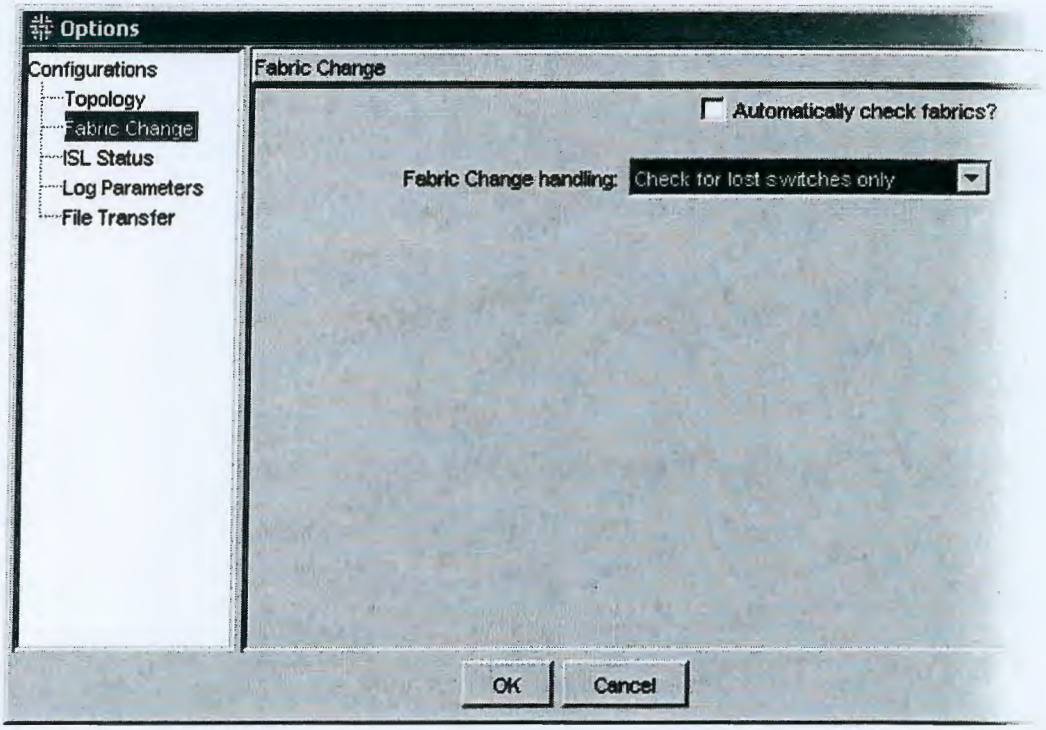


Figure 14-1 Options Window for Fabric Checking

2. In the **Configurations** tree, click **Fabric Change**. The **Fabric Change** dialogue appears in the right-hand window.
3. In the **Fabric Change** window, check the **Automatically check fabrics?** checkbox and click **OK**.

Disable Fabric Checking

To disable Fabric Checking, perform the following steps:

1. In the **SAN Elements** tab, click the fabric that you no longer want to check.
2. From the **Actions** menu, select **Fabric Checking**. The check mark beside **Fabric Checking** is removed.

Monitor Fabric Checking in Topology View

When you remove a switch from a checked fabric, the switch appears "ghosted" in Topology view and the links to the switch no longer appear. When you return the switch, the standard node replaces the "ghost" node.

Figure 14-2 displays a fabric that runs Fabric Checking.

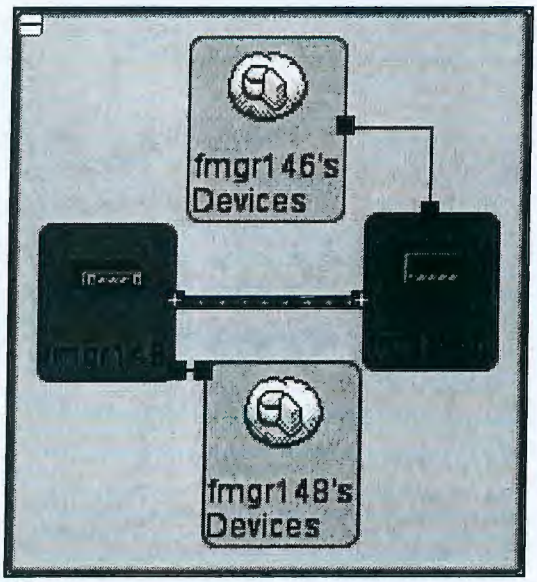


Figure 14-2 Fabric Before a Remove Event

Figure 14-3 displays the same fabric after the administrator removes a switch. Switch fmgr146 appears "ghosted."

Figure 14-3 Fabric After a Remove Event

Note: If ISL Checking and Fabric Checking are both enabled, and a switch is removed from the fabric, a red color link will be displayed in the Topology view connecting the "ghosted" switch node to the original switch it was connected to.

Appendi

D

Actions Menu Reference

This appendix includes the following sections:

Introduction

The Actions menu displays tasks that you can perform with Fabric Manager. You can only access items in this menu in the following cases:

- when you click a specific fabric in the **SAN Elements** tab
- when you click a specific switch in the **SAN Elements** tab
- when you click a switchgroup node in the **SAN Elements** tab
- when you click a switchgroup in the **SAN Elements** tab
- when you click a specific port in the **SAN Elements** tab
- when you click a portgroup node in the **SAN Elements** tab
- when you click a portgroup in the **SAN Elements** tab
- when you click a specific card in the **SAN Elements** tab (for switches that support cards)

Fabric Actions

When you click a fabric in the **SAN Elements** tab and open the Actions menu, the menu provides a series of fabric-wide tasks that you can perform. Table D-1 lists and describes the actions.

Table D-1 Fabric Actions

Action	Description
Events	Opens the Fabric Manager Event Log.
Telnet to FCS...	Telnets to the FCS of a secure fabric. If you click a non-secure fabric in the **SAN Elements** tab, you cannot access this action and it appears as **Telnet...** **Note:** This option only appears when you click a secure fabric in the **SAN Elements** tab.
Security...	Opens the **Security Admin** window to administer security. For more information, refer to *Security Admin Window* on page D-4. **Note:** This option only appears when you click a secure fabric in the **SAN Elements** tab.
Zone Admin...	Opens the **Zone Administration** window of Web Tools.
Name Server...	Opens the **Name Server Table** window in Web Tools.
ISL	Opens the ISL submenu to initiate or restamp ISL checking. For more information, refer to *ISL Submenu* on page D-5.
Set Time...	Opens the **Time** dialog box to update the time and date settings on the switches in the fabric. To configure the time, place your cursor in any part of the Time field and use the up arrow or down arrow to iterate the field, then click **OK**.
Refresh FDMI Info	Refreshes FDMI information. **Note:** This option only appears when FDMI capable HBAs are connected to switches running Fabric OS versions that support FDMI.

Table D-1 Fabric Actions (Continued)

Action	Description
Backup...	Opens the **Backup fabric configuration-Select a folder** window to create a backup file that contains the following information: • the configuration file of every switch in the fabric • the license keys for every switch in the fabric • a list of switches that belong to the fabric • an ISL stamp **Note:** The Backup action does not store the current ISL stamp. It creates a stamp of the ISLs as they appear *at the moment of the backup*. • all zone definitions (and notes the active zone) • which firmware version each switch runs • name server information
Diff with Backup...	Opens the **Diff fabric configuration with backup** window to compare a fabric to a backup file and lists discrepancies.
Fabric Checking	Activates or deactivates Fabric Checking. A dark blue ring appears around the fabric icon to indicate that you enabled Fabric Checking, and a check mark appears next to the action in the **Actions** menu.
Refresh	Refreshes the Fabric Manager display to reflect any status changes.
Delete	Deletes the selected fabric.
Rename	Allows you to rename the selected fabric.

Security Admin Window

The **Security Admin** window consists of tabs that let you view and configure the various security policies. The **Security Admin** window is displayed in Figure D-1.

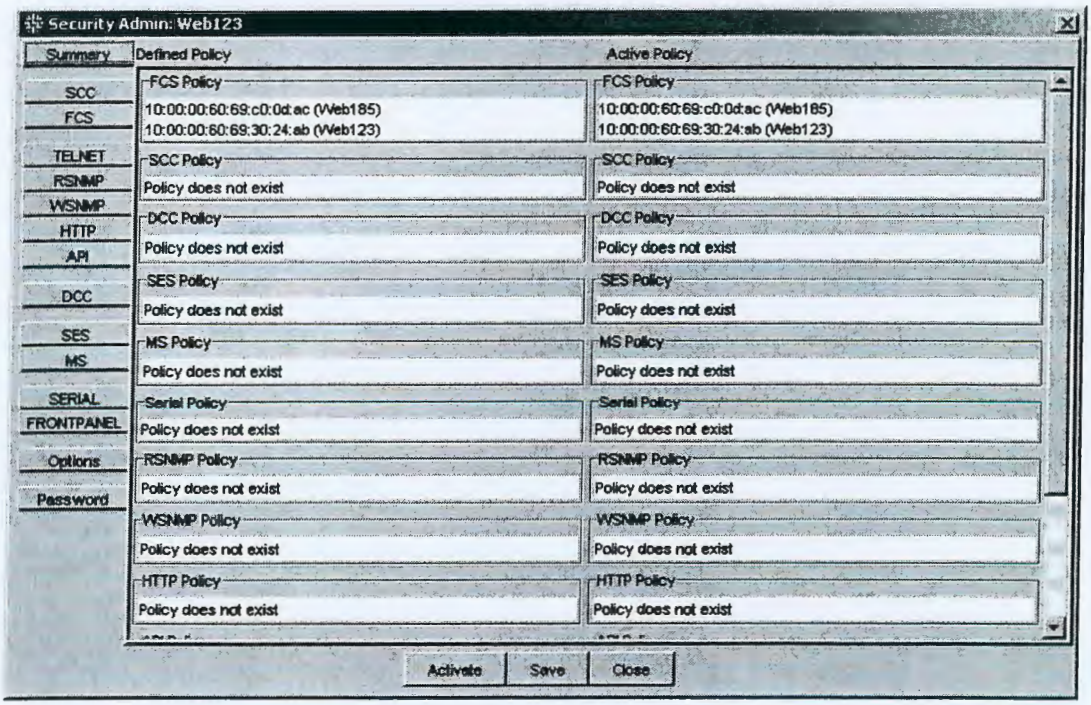


Figure D-1 Security Admin Window

Table D-2 lists and describes the tabs and buttons in the Security Admin window.

Table D-2 Security Admin Window Objects

Object	Description
Summary tab	Presents a column of defined security policies and a column of active security policies.
SCC tab	The components of this tab let you add a switch to a secure fabric. For more information, refer to *Add a Switch to a Secure Fabric* on page 11-3.
FCS tab	The components of this tab display each switch that serves as a Fabric Configuration Server (FCS) and lets you add or remove switches from the list.
TELNET tab	The components of this tab let you grant access to individual switches to run telnet in a secure fabric.
RSNMP tab	The components of this tab let you grant access to individual switches to run RSNMP in a secure fabric.
WSNMP tab	The components of this tab let you grant access to individual switches to run WSNMP in a secure fabric.
HTTP tab	The components of this tab let you grant access to individual switches to run HTTP in a secure fabric.

Table D-2 Security Admin Window Objects (Continued)

Object	Description
API tab	The components of this tab let you grant access to individual switches to run API in a secure fabric.
DCC tab	The components of this tab let you create a security policy. For more information, refer to *Configure DCC Policy Options* on page 11-7.
SES tab	The components of this tab let you grant access to individual switches to run SES in a secure fabric.
MS tab	The components of this tab let you grant access to individual switches to run Management Server in a secure fabric.
SERIAL tab	The components of this tab let you grant access to individual switches to accept a serial connection in a secure fabric.
FRONTPANEL tab	The components of this tab let you grant access to individual switches to accept configuration changes from the front panel in a secure fabric.
Options tab	The field in this tab lets you enable or disable No Node WWN zoning.
Password tab	The components of this tab let you change passwords for FCS switches and non-FCS switches.
Activate button	Activates the changes that you made to the components of the **Security Admin** window tabs.
Save button	Saves the changes that you made to the components of the **Security Admin** window tabs but does not apply them.
Close button	Closes the **Security Admin** window.

ISL Submenu

The **ISL** submenu lets you initiate or restamp ISL checking. Table D-3 lists and describes the options that appear in the **ISL** submenu.

Table D-3 ISL Submenu Options

Option	Description
ISL Checking	Enables ISL Checking. For more information on this topic, refer to *ISL Checking* on page 13-1.
Restamp	Resets the ISL stamp to which ISL Checking compares the fabric. For more information on this topic, refer to *Stamp/Restamp* on page 13-3.

Switch Actions

When you click a switch in the **SAN Elements** tab and open the Actions menu, the menu provides a series of switch-wide tasks that you can perform. Table D-4 lists and describes the actions.

Table D-4 Switch Actions

Action	Description
Events	Opens the Events View in Fabric Manager.
Switch View	Opens the **Switch View** window of Web Tools.
Admin...	Opens the **Switch Admin** window of Web Tools.
Fabric Watch...	Opens the **Fabric Watch** window of Web Tools.
Telnet	Opens a telnet session to the switch.
Close Telnet	Closes a telnet session to the switch. **Note:** This option is not applicable to switches that run 4.X firmware.
Disable/Enable	Disables or enables the switch.
Core Switch	Labels a switch as a core switch. **Note:** This action impacts the location of the switch in Topology view for Core Edge layouts.
Delete	Deletes the switch.
Rename	Allows you to rename the switch.

Port Actions

When you click a port in the **SAN Elements** tab and open the Actions menu, the menu provides port-wide tasks that you can perform. Table D-5 lists and describes the actions.

Table D-5 Port Actions

Action	Description
Disable/Enable	Disables or enables the port.

NEC
12720
E

Comprovação das Especificações Exigidas no Edital 050/2003

3.4. Switch tipo 4 (KVM)

23/07/03

NEC

12719

Switch Tipo 4	Black Box - Servswitch Affinity
22921.pdf	

0399

BLACK BOX® NETWORK SERVICES

Black Box Corporation • 1000 Park Drive • Lawrence, PA 15055-1018 • Tech Support: 724-746-5500 • **www.blackbox.com** • **e-mail: info@blackbox.com**

SERVSWITCH™ AFFINITY

Affordable many-to-many multiplatform KVM switching.

Key Features

- ***As many as 16 users have keyboard/mouse/video control over as many as 1024 PC, Sun, RS/6000, SGI, HP, and/or Alpha computers.***
- ***With additional converters, also supports Apple computers.***
- ***Easily expandable with plug-in Port Cards and flexible cabling.***
- ***Free lifetime firmware upgrades.***
- ***Supports video resolutions up to 1280 x 1024.***
- ***High levels of security, including passwords and access profiles.***
- ***Controlled through on-screen display, with additional keyboard commands and a terminal-based serial-port options menu.***
- ***Some models have redundant power supplies.***

Is your server room growing by leaps and bounds? Wouldn't it be nice to have a keyboard/video/mouse-switching system that could keep up with all the hardware, all the users, the constant changes, and the realities of your budget?

Our ServSwitch™ Affinity could be the one. It will support most major hardware platforms, including IBM® PS/2®, PC/AT®, and RS/6000®; Sun®; SGI™; HP® 700 and 9000 series; and Compaq® Alpha™. IBM type computers can use any keyboard mode and any of a variety of mouse types. Video can be any of several types at up to 1280 x 1024 resolution. With additional adapters, you can attach Apple® Macintosh® CPUs too—see **"What else you might need"** on page 4.

You can attach as many as 16 computers to a single unit or 1024 computers to a daisychained Affinity system. Either way, you can also attach up to 4, 8, or 16 independent users; more users can be connected, but they'll have to contend for access.

Here's how it works: Each ServSwitch Affinity has four slots for Port Cards. 0 x 4 Port Cards (product code KV1300C) have four CPU (computer) ports and a serial port only; 1 x 4 Cards (KV1301C) also have a KVM (user) port.

The Affinity chassis also has a fifth, top slot used for expansion purposes; the 16-User models have a matching sixth, bottom slot. 4-User models ship with a Terminator Card (KV1304C) installed in the expansion slot; you can swap in a 4-User Expansion Card (KV1305C) if you'll be daisychaining the Affinity. 8- and 16-User models, which are designed to be part of a daisychain, come without anything installed in the expansion slot(s). You need to purchase and install an 8-User Expansion Card (KV1306C) for each slot in order for the unit to work.

The only difference between the three 4-User Affinity models with single power supplies is which Cards they're preinstalled with; see the start of **"Ordering Information"** on page 5 for a list of which Cards come with each model.

You can add capacity to your Affinity system at any time by installing Port Cards in vacant slots or adding more chassis to a daisychain.

The Port Card's serial ports are used for terminal-based initial system configuration; they are also used to upgrade the Affinity's firmware (upgrades are free for the lifetime of the Affinity!).

The ServSwitch Affinity's main controls are its on-screen menus (with a full range of configuration and operating functions). These menus are augmented by a number of keyboard commands.

For added security, the Affinity supports password-protected access groups. Computers can belong to multiple groups, but users can only belong to one. Users will only be able to access the computers in their group.

When users do access computers, they'll have one of four assigned access levels: view only (no keyboard/mouse control), share (view access until current user becomes inactive, then add keyboard and mouse), control (sole control but others can view), or private (sole control, no one else can interrupt or view).

For mission-critical applications, we offer models of the Affinity with dual, redundant power supplies. If one power supply ever fails, the other can take on the entire load until a replacement supply can be installed.

Specifications

Hardware Required: Monitor that supports your computers' highest video standard; in multiplatform applications, should be multisync model that can video from either composite sync or separate horizontal/vertical sync signals

Compliance: CE, FCC Part 15 Subpart J Class A, IC Class/ classe A

Standards:
- With original Serv cabling: VGA (color or monochrome/page white) video;
- With original Serv cabling (minimal) or coaxial cabling (recommended): SVGA and (with KV99MA adapter) Mac video;
- With coaxial cabling: XGA (color or monochrome), Sun, RS/6000, or SGI video

Interfaces:
- On CPU ports and user ports of Port Cards and IN 1 and OUT 1 ports of primary Expansion Cards:
  - Proprietary composite of:
    - IBM PS/2, PC/AT, or Sun compatible keyboard;
    - PS/2, RS-232 serial (except on user ports), or Sun compatible mouse; and
    - Video (see **Standards** above);
  - With the KV99MCON converter, also supports ADB (Mac compatible) keyboard and mouse ports;
  - IN 1 and OUT 1 also carry system-control signals;
- On Expansion Cards' other IN and OUT ports: Proprietary video composite (see **Standards** above);
- On serial ports of Port Cards: EIA/TIA RS-232 proprietarily pinned on RJ-12 ("6-wire RJ-11") connectors, DTE

Resolution: Up to 1280 x 1024, but will depend on the length of CPU and User Cables in your system

Serial (RS-232) Characteristics:
- Protocol: Asynchronous;
- Data format: 8 data bits, 1 stop bit, no parity (fixed);
- Data rate: 9600 or 57,600 bps

Maximum Distance:
- 20 ft. (6.1 m) of CPU or User Cable—possibly as much as 100 ft. (30.5 m) if Cable is coaxial, depending on CPUs, monitor, and video resolution—from any Affinity Port Card to any device attached to it;
- 100 ft. (30.5 m) of Expansion Cable between any two Affinity units;
- 50 ft. (15.2 m) of serial cable from the RS-232 port of any Affinity Port Card to a computer's serial port

User Controls:
- For system: Keyboard commands and on-screen menus;
- On Affinity chassis: Rear-mounted ON/OFF rocker switch(es);
  - KV13xDA models: (2);
  - All other models: (1);
- On all Expansion Cards (KV1305C and KV1306C): Board-mounted BUS/RING jumper;
- On 8-User Expansion Cards (KV1306C): (2) Board-mounted jumper blocks for user-port numbering

Indicators:
- All models: ON/OFF switch(es) are dark when ServSwitch Affinity is OFF, backlit when Affinity is ON;
- KV13xDA models: (3) Front-mounted power-supply status LEDs:
  - (1) for supply 1 (the upper transformer), lit while supply is outputting power;
  - (1) for supply 2 (the lower transformer), lit while supply is outputting power;
  - (1) for the Affinity chassis (marked "SYSTEM"), lit while either supply is outputting power unless internal diodes have failed

Connectors:
- All rear-mounted;
- On Affinity chassis: IEC 320 male power inlet(s):
  - KV13xDA models: (2);
  - All other models: (1);
- On all Affinity Port Cards (KV1300C and KV1301C):
  - (4) DB25 female for CPU connections,
  - (1) RJ-12 ("6-wire RJ-11") female for serial management;
- On 1 x 4 Port Cards (KV1301C):
  - (1) DB25 female for user connections;
- On 4-User Expansion Cards (KV1305C):
  - (2) DB15 female: (1) for input to Port Cards in slots 1 and 2, (1) for input to Port Cards in slots 3 and 4;
  - (2) DB15 male: (1) for output from Port Cards in slots 1 and 2, (1) for output from Port Cards in slots 3 and 4
- On 8-User Expansion Cards (KV1306C):
  - (4) HD15 female:
    - (1) for input to Port Cards set as KVM 1/2 or 9/10;
    - (1) for input to Port Cards set as KVM 3/4 or 11/12;
    - (1) for input to Port Cards set as KVM 5/6 or 13/14;
    - (1) for input to Port Cards set as KVM 7/8 or 15/16;
  - (4) HD15 male:
    - (1) for output from Port Cards set as KVM 1/2 or 9/10;
    - (1) for output from Port Cards set as KVM 3/4 or 11/12;
    - (1) for output from Port Cards set as KVM 5/6 or 13/14;
    - (1) for output from Port Cards set as KVM 7/8 or 15/16

Maximum Altitude: 10,000 ft. (3048 m)

Temperature Tolerance: 32 to 113°F (0 to 45°C)

Humidity Tolerance: 5 to 80% noncondensing

Enclosure: Steel

Fuses: KV13xDA models: Autoresetting switch fuses that cut in when power surges exceed the maximum ratings of the chassis

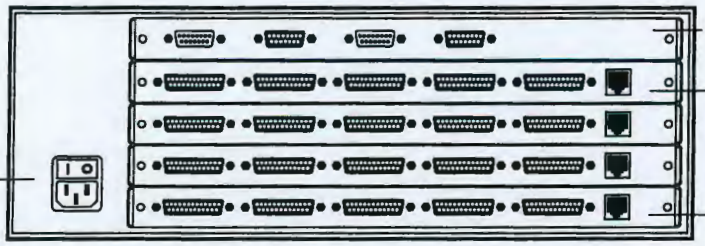
Power:
- Input: 90 to 264 VAC, 47 to 63 Hz, 700 mA from AC outlet(s) through included power cord(s) and inlet(s) into internal transformer(s):
  - KV13xDA models: Dual transformers with separate AC inlets, electrically isolated from one another;
  - All other models: Single transformer;
- Consumption: Up to 40 VA (40 watts)

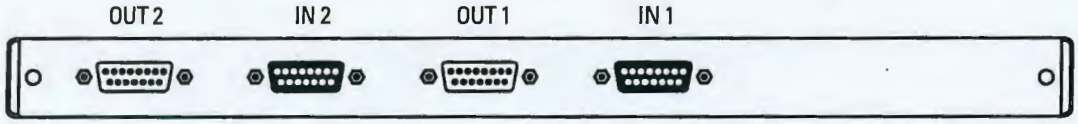
Size:
- KV139A and KV139DA chassis: 7"H (4U) x 16.7"W x 7"D (17.8 x 42.4 x 17.8 cm);
- All other Affinity chassis: 5.25"H (3U) x 16.7"W x 7"D (13.3 x 42.4 x 17.8 cm);
- Port Cards and Expansion Cards: 0.9"H x 13.9"W x 4.8"D (2.3 x 35.3 x 12.2 cm);
- Terminator Card (4-User models only): 0.4"H x 2.1"W x 0.8"D (1 x 5.3 x 2 cm)

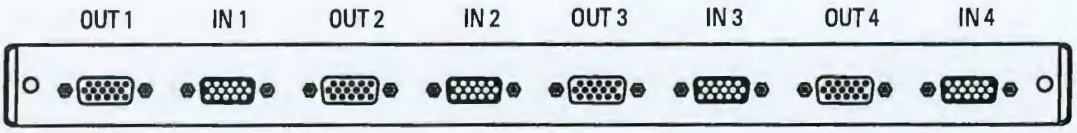
Weight:
- KV130A, KV130DA, KV138A, and KV138DA: 10.5 lb. (4.8 kg);
- KV132A: 12 lb. (5.5 kg);
- KV134A: 14 lb. (6.4 kg);
- KV139A and KV139DA: 11 lb. (5 kg);
- KV1300C, KV1301C, and KV1306C: 0.9 lb. (0.4 kg);
- KV1304C: 0.2 lb. (0.1 kg);
- KV1305C: 0.4 lb. (0.2 kg)

If you need to share access to a large number of CPUs, think about putting in an Affinity daisychain made up of 4-User Expansion Chassis (like the fully loaded one shown below) or 8- or 16-User Chassis. They come empty (no Cards installed), but you can install one Expansion Card (or two in the 16-User units) and add as many as four 0 x 4 or 1 x 4 Port Cards to them, giving you a maximum of four, eight, or sixteen user stations and sixteen CPUs attached to each unit. (Keep in mind that however many user stations a unit is designed for, only that many video paths can be open through that unit at a time. For example, a 4-User unit only has four video paths, so if there are already four users attached to a 4-User unit, and a user at another Affinity unit selects one of the 4-User unit's CPUs, one of the 4-User unit's users—and all other users on that slot—will be locked out until the new connection ends.)

The 8-User units look very similar to the 4-User unit shown here, but they accept only 8-User Expansion Cards like the one shown below. The 16-User Units accept two of the 8-User Expansion Cards. The 8-User Cards have jumper blocks that you can set to control which four KVM slots are used by the users attached to the Affinity chassis that the Card is installed in: KVM 1 through 4, 5 through 8, 9 through 12, or 13 through 16.





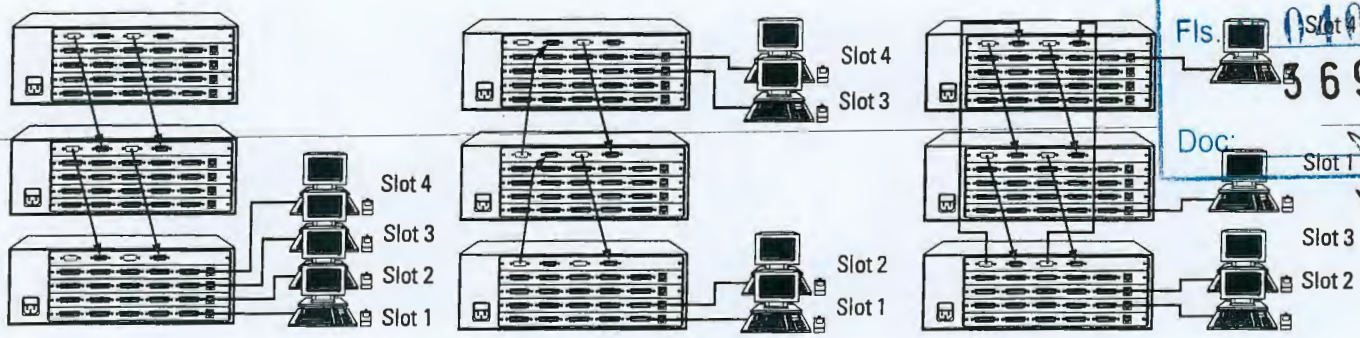


On the 4-User Expansion Cards (above, top), IN 1 and OUT 1 carry signals for the Port Cards in slots 1 and 2, while IN 2 and OUT 2 carry signals for the Port Cards in slots 3 and 4.

On the 8-User Expansion Cards (above, bottom), IN 1 and OUT 1 carry the signals for either KVM 1 and 2 or, if installed in the bottom slot of a 16-User unit, KVM 9 and 10; IN 2 and OUT 2 cary the signals for either KVM 3 and 4 or KVM 11 and 12; and so on. A pair of jumper blocks, mentioned above, determines which four KVM slots the four users on that Affinity chassis will use.

Because the control paths are carried on different connectors this way, you have maximum flexibility for designing your daisychain layout:

- If all of your users are on one Chassis, use the regular bus topology (below, left).
- If you have two users on one Chassis and two on another, use the "split bus" topology (below, middle).
- If your users are spread across several Chassis, use the ring topology (below, right).*



*It is always important to keep in mind that only one user at a time can use the bus that interconnects daisychained Affinity units, especially when you implement a ring topology. For example, when your Affinity units are interconnected in a ring, if any user on Slot 1 selects a CPU attached to an Affinity unit other than his own, no other Slot 1 user can select any CPUs.

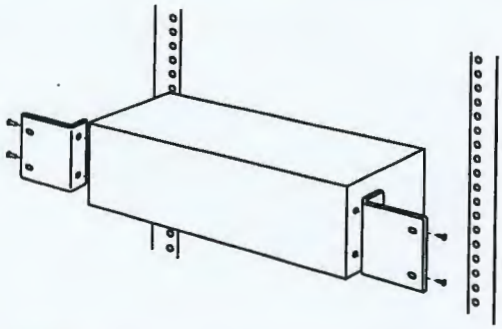
The complete package

- The ServSwitch Affinity, including any cards and blanking plates that are normally preinstalled with your model. (Blanking plates will cover all unused slots, as well as the slot on 4-User models that the tiny Terminator Card is installed in.)
- A power cord.
- *KV13xDA models only:* A second power cord.
- A 6-ft. (1.8-m) serial cable with RJ-12 ("6-wire RJ-11") plugs.
- An RJ-12 to DB9 modular adapter.
- A manual.

What else you might need

- CPU Adapter Cables, User Adapter Cables, and (if you're cascading) Expansion Cables.
- Keyboards, mice, and monitors for your users. If you're mixing platforms, we recommend true multiscan, multisync monitors capable of syncing to each CPU's video-output frequencies and compatible with all of the CPUs' video cards. Also, if one of the multiple platforms is IBM, the monitors must be able to accept both separate H/V sync and composite sync. (Such monitors are widely available.) We recommend that the monitors be able to display a maximum resolution of not less than 1280 x 1024 at a maximum refresh rate of not less than 75 Hz.
- An AC-power surge protector and uninterruptible power supply.
- Data-line surge protectors for the keyboard and mouse lines.
- *To attach an Apple Mac®:* A ServSwitch™ Micro Mac® Converter (product code KV99MCON), a G3™/G4™ or legacy Macintosh® style CPU-Extension Cable, and, if the Mac needs to see ID bits from its monitor, a Mac Video Adapter for ServSwitch (KV99MA).
- *If you purchase a 4-User Expansion Chassis or an 8- or 16-User Chassis:* Port Cards for your CPU and user-station connections.
- *To cascade a ServSwitch Affinity:* An Expansion Card.
- *To rackmount a ServSwitch Affinity:* A ServSwitch Affinity Rackmount Kit.

If you can use a screwdriver, you can install the Rackmount Kits.



Ordering Information

ITEM	CODE
ServSwitch Affinity	
4-User Expansion Chassis (Terminator Card installed, no Port Cards installed)	
Single power supply	KV130A
Dual power supply	KV130DA
4-User Standalone Chassis:	
2 Users by 8 CPUs (Terminator Card installed, 1 x 4 Port Cards installed in slots 1 and 2)	KV132A
4 Users by 16 CPUs (Terminator Card installed, 1 x 4 Port Cards installed in slots 1 through 4)	KV134A
8-User Chassis (no Cards installed)	
Single power supply	KV138A
Dual power supply	KV138DA
16-User Chassis (no Cards installed)	
Single power supply	KV139A
Dual power supply	KV139DA
Port Cards	
0 x 4 (No Users, Four CPUs)	KV1300C
1 x 4 (One User, Four CPUs)	KV1301C
4-User Terminator Card	KV1304C
4-User Expansion Card	KV1305C
8- and 16-User Expansion Card	KV1306C

Ordering Information (continued)

ITEM	CODE

NOTE: For CPU and User Cables, specify length by adding any of these suffixes to the product code (not all cables are available in all lengths):
"-0001" for 1 ft. (0.3 m, User Cables only),
"-0005" for 5 ft. (1.5 m),
"-0010" for 10 ft. (3 m),
"-0020" for 20 ft. (6.1 m),
"-0035" for 35 ft. (10.7 m),
"-0050" for 50 ft. (15.2 m),
"-0075" for 75 ft. (22.8 m), or
"-0100" for 100 ft. (30.5 m)

*You will need a **CPU Cable** for each CPU you attach:*

Standard CPU Cables, available in standard lengths up to 20 ft. (6.1 m)—Mac styles require keyboard/mouse conversion

IBM PS/2 style	EHN051
IBM PC/AT style	EHN048
Mac style with legacy DB15 video connectors	EHN215
Mac style with HD15 VGA video connectors for G3™, G4™, and similar models	EHN550

Coaxial CPU Cables—IBM and Sun styles available in all standard lengths, SGI and RS/6000 styles available in standard lengths up to 20 ft. (6.1 m), Mac styles require keyboard/mouse conversion

Universal IBM style	EHN282
Sun style with traditional 13W3 video connectors	EHN206
Sun style with VGA (HD15) video connectors	EHN515
SGI style	EHN500
RS/6000 style	EHN520
Mac style with traditional DB15 video connectors	EHN208
Mac style with HD15 VGA video connectors for G3, G4, and similar models	EHN560

ServSwitch™ Micro Mac® Converter to convert PS/2 kbd/mouse to ADB™ kbd/mouse signals	KV99MCON
For older Mac models that must see monitor ID: Mac® Video Adapter for ServSwitch™	KV99MA

*You will need a **User Cable** for each monitor/keyboard/mouse user station you attach:*

Regular (non-coaxial) User Cables, available in standard lengths up to 20 ft. (6.1 m)

IBM PS/2* style	EHN054
Sun style with VGA (HD15) video connector for multisync monitor	EHN059

Coaxial User Cables

IBM PS/2* style, available in all standard lengths except 1 ft. (0.3 m)	EHN283
Sun style with 13W3 video connector for Sun monitor, available in all standard lengths	EHN201
Sun style with VGA (HD15) video connector for multisync monitor, available in all standard lengths	EHN225
SGI style, 1 ft. (0.3 m) only	EHN501-0001
RS/6000 style, 1 ft. (0.3 m) only	EHN521-0001

*We no longer offer IBM PC/AT type User Cables for the ServSwitch Affinity, because its current firmware does not support serial mice, although it will still translate signals from PS/2 type mice into serial protocol for PC/AT CPUs.

Ordering Information (continued)

ITEM	CODE
You might also need:	
Expansion Cables for 4-User Units	
10 ft. (3 m)	KV140010
20 ft. (6.1 m)	KV140020
35 ft. (10.7 m)	KV140035
50 ft. (15.2 m)	KV140050
100 ft. (30.5 m)	KV140100
Expansion Cables for 8- and 16-User Units	
10 ft. (3 m)	KV180010
20 ft. (6.1 m)	KV180020
35 ft. (10.7 m)	KV180035
50 ft. (15.2 m)	KV180050
100 ft. (30.5 m)	KV180100
Replacement 6-wire straight-through-pinned flat-satin cable for serial management (specify length)	EL06MS-MM
Rackmount Kits	
To mount 4- or 8-User units in 19" Racks	RMK19A
To mount 4- or 8-User units in 23" Racks	RMK23A
To mount 4- or 8-User units in 24" Racks	RMK24A
To mount 16-User units in 19" Racks	RMK19A139
To mount 16-User units in 23" Racks	RMK23A139
To mount 16-User units in 24" Racks	RMK24A139
Surge protector for IBM PS/2 style keyboard and mouse lines (6-pin mini-DIN M/F)	SP519A-R2
Surge protector for IBM PC/AT style keyboard lines (5-pin DIN M/F)	SP518A-R2

Call Black Box Tech Support for help determining your best options for AC-power backup and protection.

Black Box offers the best warranty program in the industry—Fido Protection®. For more information, request **FaxBack 22512**.

CPL/AC

PREGÃO
050/2003

LOCAÇÃO DE EQUIPAMENTOS DE INFORMÁTICA INCLUINDO ASSISTÊNCIA TÉCNICA E TREINAMENTO

NEC DO BRASIL S/A – PROPOSTA ECONÔMICA VOLUME II

2003
PASTA 22

NEC

Comprovação das Especificações Exigidas no Edital 050/2003

3.5. Switch tipo 5 (Concentrador de VPNs)

23/07/03

Switch Tipo 5	
vpn3k_ds.pdf	Cisco VPN 3000 Series Concentrator
mgtproto1.pdf	Management Protocols
acspp_ds.pdf	Cisco Secure Access Control Server Solution Engine
acsqp_qp.pdf	Cisco Secure Access Control Server Solution Engine Q&A

Data Sheet

Cisco **VPN 3000** Series Concentrator

Introduction

The Cisco® VPN Series 3000 Concentrator allow corporations to take full advantage of the unprecedented cost savings, flexibility, performance, and reliability of remote access VPN connections. Corporations use VPNs to establish secure, end-to-end private network connections over a public networking infrastructure. VPNs have become the logical solution for remote-access connectivity for two main reasons:

- Deploying a remote-access VPN enables corporations to reduce communications expenses by using the local dialup infrastructures of Internet service providers.
- Remote Access VPNs allow mobile workers, telecommuters and day extenders to take advantage of broadband connectivity.

To fully realize the benefits of high-performance, remote-access VPNs, a corporation must deploy a robust, highly available VPN solution, and dedicated VPN devices are optimal for this purpose.

The Cisco VPN 3000 Series Concentrator is a best-in-class, remote-access VPN solution for enterprise-class deployment. A standards-based, asy-to-use VPN client and scalable VPN tunnel termination devices are included, as well as a management system that enables corporations to easily install, configure, and monitor their remote access VPNs. Incorporating the most advanced, high-availability capabilities with a unique purpose-built, remote-access architecture, the Cisco VPN 3000 Concentrator allows corporations to build high-performance, scalable, and robust VPN infrastructures to support their mission-critical, remote-access applications.

Unique to the industry, it is the only scalable platform to offer components that are field-swappable and can be upgraded by the customer. These components, called Scalable Encryption Processing (SEP/SEP-E) modules, enable users to easily add capacity and throughput.

The Cisco VPN 3000 Concentrator supports the widest range of VPN client software implementations, including the Cisco VPN Client, the Microsoft Windows 2000/XP L2TP/IPsec Client, the Microsoft L2TP/IPSec VPN Client for Windows 98, Windows Millennium (ME), Windows NT Workstation 4.0, and Microsoft PPTP.

Five Models

The Cisco VPN 3000 Concentrator is available in five different models:

Cisco VPN 3005 Concentrator

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

Cisco VPN 3015 Concentrator

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

Cisco VPN 3030 Concentrator

The Cisco VPN 3030 Concentrator is a VPN platform designed for medium to large organizations with bandwidth requirements from full T1/E1 through T3/E3(50 Mbps maximum performance) and up to 1500 simultaneous sessions. Specialized SEP modules perform hardware-based acceleration. The Cisco VPN 3030 is field-upgradeable to the Cisco VPN 3060. Redundant and nonredundant configurations are available.

Cisco VPN 3060 Concentrator

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

Cisco VPN 3080 Concentrator

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

Models Comparison

Table 1 The Cisco VPN 3000 Series Supports the Entire Range of Enterprise Applications

	Cisco VPN 3005	Cisco VPN 3015	Cisco VPN 3030	Cisco VPN 3060	Cisco VPN 3080
Simultaneous Users [1]	100	100	1,500	5,000	10,000
Maximum LAN-to-LAN Sessions	100	100	500	1000	1000
Encryption Throughput	4 Mbps	4 Mbps	50 Mbps	100 Mbps	100 Mbps
Encryption Method	Software	Software	Hardware	Hardware	Hardware
Available Expansion Slots	0	4	3	2	2
Encryption (SEP) Module	0	0	1	2	4
Redundant SEP	–	–	Option	Option	Yes
System Memory	32/64 MB (fixed)	128 MB	128/256 MB	256/512 MB	256/512 MB
Hardware Configuration	1U	Fixed 2U	Scalable 2U	Scalable 2U	Fixed 2U
Dual Power Supply	Single	Option	Option	Option	Yes
Client License	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited

1. For planning purposes, a simultaneous user is considered to be a remote access VPN user connected in all tunneling mode—this includes one IKE Security Association and two unidirectional IPsec SAs (Security Associations). For environments with rekeying or split tunneling, we recommend using a VPN remote access load-balancing environment with spare capacity because these particular sessions will use additional system resources that otherwise would be used to support additional users. The Cisco VPN 3000 Series Concentrator supports the entire range of enterprise applications.

Cisco VPN Client

Simple to deploy and operate, the Cisco VPN Client is used to establish secure, end-to-end encrypted tunnels to the Cisco VPN 3000 Concentrator. This thin design, IPsec-compliant implementation is provided with the Cisco VPN 3000 Concentrator and is licensed for an unlimited number of users. The client can be pre-configured for mass deployments and the initial logons require very little user intervention. VPN access policies are created and stored centrally in the Cisco VPN 3000 Concentrator and pushed to the client when a connection is established.

Features and Benefits

Product Highlights

High-Performance, Distributed-Processing Architecture

- Cisco SEP modules provide hardware-based encryption, ensuring consistent performance throughout the rated capacity (Cisco VPN 3030–3080).
- Large-scale tunneling support provided for IPsec, PPTP and L2TP/IPsec connections.

Scalability (Cisco VPN 3015–3060)

- Modular design (four expansion slots) provides investment protection, redundancy and a simple upgrade path.
- System architecture is designed to supply consistent, high-availability performance.
- All digital design provides the highest reliability and 24-hour continuous operation.
- Robust instrumentation package provides run-time monitoring and alerts.
- Microsoft compatibility offers large-scale client deployment and smooth integration with related systems.

Security

- Full support of current and emerging security standards allows for integration of external authentication systems and interoperability with third-party products.
- Firewall capabilities through stateless packet filtering and address translation to ensure the required security of a corporate LAN.
- User and group level management offers maximum flexibility.

High Availability

- Redundant subsystems and multichassis failover capabilities ensure maximum system uptime.
- Extensive instrumentation and monitoring capabilities provide network managers with real-time system status and early-warning alerts.

Robust Management

- The Cisco VPN 3000 Concentrator can be managed using any standard Web browser (HTTP or HTTPS), as well as by Telnet, SSHv1, and using a console port. Files can be accessed through HTTPS, FTP, and SSH Copy (SCP).
- Configuration and monitoring capability is provided for both the enterprise and the service provider.
- Access levels are configurable by user and groups, allowing easy configuration and maintenance of security policies. For larger scale deployments, the VPN 3000 Concentrators are supported in several Cisco network management applications. Those applications include:
  - *IP Solution Center (ISC)*—Provisions site-to-site and remote access VPN services
  - *VPN Monitor*—Monitors and reports on remote access and site-to-site VPN tunnel connections
  - *Resource Manager Essentials (RME)*—Provides operational management features such as software distribution, syslog reporting, inventory management
  - *CiscoView*—Provides real time system status monitoring

Technical Specifications

Hardware

Processor

- Motorola PowerPC Processor

Memory

- Redundant system images (Flash)
- Variable memory options (see chart)

Encryption

- *Cisco VPN 3005, 3015*—Software encryption
- *Cisco VPN 3030–3080*—Hardware encryption

Embedded LAN Interfaces

- *Cisco VPN 3005*—Two autosensing, full-duplex 10/100BASE-TX Fast Ethernet (public/untrusted, private/trusted)
- *Cisco VPN 3015–3080*—Three autosensing, full-duplex 10/100BASE-TX Fast Ethernet (public/untrusted, private/trusted and DMZ)

Instrumentation

- *Cisco VPN 3005 Front panel*—Unit status indicator
- *Cisco VPN 3005 Rear panel*—Status LEDs for Ethernet ports
- *Cisco VPN 3015-3080 Front panel*—Status LEDs for system, expansion modules, power supplies, Ethernet modules, fan
- *Cisco VPN 3015–3080 Rear panel*—Status LEDs for Ethernet modules, expansion modules, power supplies
- *Cisco VPN 3015–3080*—Activity monitor displays number of sessions, aggregate throughput, or CPU utilization; push-button selectable

Software

Client Software Compatibility

- Cisco VPN Client (IPsec) for Windows 98, ME, NT 4.0, 2000, XP, Linux (Intel), Solaris (UltraSparc 32 and 64-bit), and Mac OS X 10.2 (Jaguar), including centralized split-tunneling control and data compression
- Microsoft PPTP/MPPE/MPPC, MSCHAPv1/v2, EAP/ RADIUS pass-through for EAP/TLS and EAP/GTC support
- Microsoft L2TP/IPsec forWindows 2000/XP (including XP DHCP option for route population)
- Microsoft L2TP/IPsec for Windows 98, Windows Millennium (ME), and Windows NT Workstation 4.0
- MovianVPN (Certicom) Handheld VPN Client with ECC
- Netlock (Mac OS 8 & 9) VPN Client

Tunneling Protocols

- IPsec, PPTP, L2TP, L2TP/IPsec, NAT Transparent IPsec, Ratified IPsec/UDP (with auto-detection and fragmentation avoidance), IPsec/TCP
- Support for Easy VPN (client and network extension mode)

Encryption/Authentication

- IPsec Encapsulating Security Payload (ESP) using DES/3DES (56/168-bit) or AES (128, 192, 256-bit) with MD5 or SHA, MPPE using 40/128-bit RC4

Key Management

- Internet Key Exchange (IKE)
- Diffie-Hellman (DH) Groups 1, 2, 5, 7 (ECDH)

Routing

- RIP, RIP2, OSPF, RRI (Reverse Route Injection), static, automatic endpoint discovery, Network Address Translation (NAT), Classless Interdomain Routing (CIDR)
- IPsec fragmentation policiy control, including support for Path MTU Discovery (PMTUD)
- Interface MTU control

Third-Party Compatibility

- Certicom, iPass Ready, Funk Steel Belted RADIUS certified, NTS TunnelBuilder VPN Client (Macintosh and Windows), Microsoft Internet Explorer, Netscape Communicator, Entrust, Baltimore, SA Keon

High Availability

- VRRP protocol for multi-chassis redundancy and fail-over
- Remote Access Load Balancing clusters
- Destination pooling for client-based fail-over and connection re-establishment
- Redundant SEP modules (optional), power supplies, and fans (Cisco VPN 3015–3080)

Management

Configuration

- Embedded management interface is accessible through console port, Telnet, SSHv1, and Secure HTTP (HTTPS)
- Administrator access is configurable for five levels of authorization. Authentication can be performed externally through TACACS+
- Role-based management policy separates functions for service provider and end-user management

Monitoring

- Event logging and notification through e-mail (SMTP)
- Automatic FTP backup of event logs
- SNMP MIB-II support
- Configurable SNMP traps
- Syslog output
- System status
- Session data (including client assign IP, encryption type connection duration, client OS, version, etc)
- General statistics

Security

Authentication and Accounting Servers

- Support for redundant external authentication servers:
  - RADIUS
  - Kerberos/Active Directory authentication
  - Microsoft NT Domain authentication
  - Microsoft NT Domain authentication with Password Expiration (MSCHAPv2)

RSA Security Dynamics (SecurID Ready), including native support for RSA 5 (Load Balancing, Resiliency)

- User authorization through LDAP or RADIUS
- Internal Authentication server for up to 100 users
- X.509v3 digital certificates (including CRL/LDAP and CRL/HTTP, CRL Caching and Backup CRL Distribution Point support)
- RADIUS accounting
- TACACS+ Administrative user authentication

Internet-Based Packet Filtering

- Source and destination IP address
- Port and protocol type
- Fragment protection
- FTP session filtering
- Site-to-Site Filters and NAT (for overlapping address space)

Policy Management

- By individual user or group
  - Filter profiles (defined internally or externally)
  - Idle and maximum session timeouts
  - Time and day access control
  - Tunneling protocol and security authorization profiles
  - IP Pool
  - Authentication Servers

Certification

- FIPS 140-2 Level 2 (3.6) in process, FIPS 140-1 Level 2 (3.1), VPNC

Ports

- Console port-Asynchronous serial (DB-9)

Table 2 Physical Characteristics

Concentrator	Cisco VPN 3005	CiscoVPN 3015	Cisco VPN 3030	Cisco VPN 3060	Cisco VPN 3080
Height	1.75" (4.45cm)	3.5" (8.89cm)	3.5" (8.89cm)	3.5" (8.89cm)	3.5" (8.89cm)
Width	17.5" (44.45cm)	17.5" (4.45cm)	17.5" (4.45cm)	17.5" (4.45cm)	17.5" (4.45cm)
Depth	11.5" (29.21cm)	–	–	–	–
Unit without front bezel or SEPS/PS	–	15" (38.1cm)	15" (38.1cm)	15" (38.1cm)	15" (38.1cm)
Unit with front bezel, no SEPS/PS	–	16-3/16" (41.12 cm)	16-3/16" (41.12 cm)	16-3/16" (41.12 cm)	16-3/16" (41.12 cm)
Unit with front bezel and SEPS/PS	–	16.75" (42.55 cm)	16.75" (42.55 cm)	16.75" (42.55 cm)	16.75" (42.55 cm)
Weight	8.5 lbs(3.9kg)	27 lbs(12.3kg)	28 lbs(12.7kg)	33 lbs(15kg)	33 lbs(15kg)

Table 3 Power Type and Requirements

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

Environmental

- Temperature: 32 to 131 F (0 to 55 C) operating; –4 to 176 F (–40 to 70 C) nonoperating
- Humidity: 0 to 95 percent noncondensing

Regulatory Compliance

- CE Marking

Safety

- UL 1950, CSA

EMC

- FCC Part 15 (CFR 47) Class A, EN 55022 Class A, EN50082-1, AS/NZS 3548 Class A, VCCI Class A

Cisco Systems

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

RD/LW4512 0403

Management Protocols

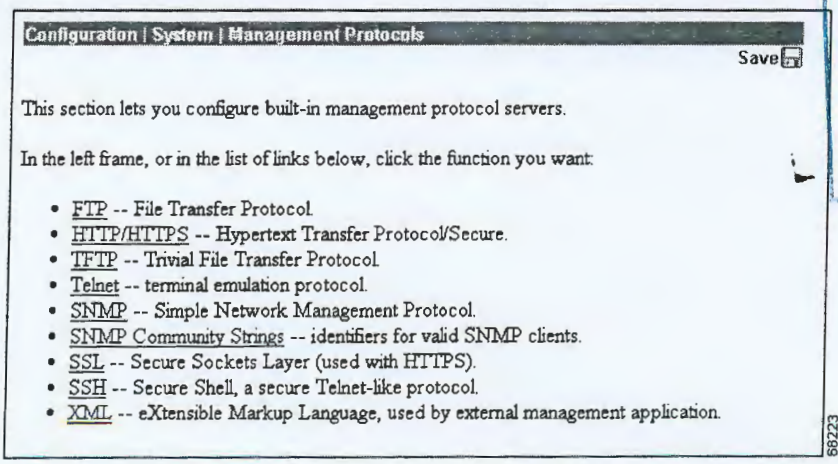
The VPN 3000 Concentrator Series includes various built-in servers, using various protocols, that let you perform typical network and system management functions. This section explains how you configure and enable those servers.

Configuration | System | Management Protocols

This section of the Manager lets you configure and enable built-in VPN Concentrator servers that provide management functions using:

- FTP: File Transfer Protocol.
- HTTP/HTTPS: Hypertext Transfer Protocol, and HTTP over SSL (Secure Sockets Layer) protocol.
- TFTP: Trivial File Transfer Protocol.
- Telnet: Terminal emulation protocol, and Telnet over SSL.
- SNMP: Simple Network Management Protocol.
- SNMP Community Strings: Identifiers for valid SNMP clients.
- SSL: Secure Sockets Layer protocol.
- SSH: Secure Shell.
- XML: Extensible Markup Language.

Figure 9-1 Configuration | System | Management Protocols Screen



Cisco Systems

Data Sheet

Cisco Secure **Access Control Server** Solution Engine

The Cisco® Secure Access Control Server (ACS) provides a comprehensive identity networking solution and secure user experience for Cisco intelligent information networks. It is the integration and control layer among all enterprise users, administrators, and the resources of the network infrastructure. The Cisco Secure ACS Solution Engine adds new security imp rovements, simplified management, and reduced total cost of ownership (TCO) for the operation of the underlying ACS service.

Introduction

The Cisco Secure ACS Solution Engine is a high-performance and highly scalable user and administrative access control solution that operates as a centralized RADIUS or TACACS+ server system for the Cisco 1111 platform. Packaged in a dedicated and secure 1-rack-unit (1-RU) hardened appliance, the Cisco Secure ACS Solution Engine provides a reduced-configuration, plug and play solution, and highly reliable platform with the unique ability to protect existing networking infrastructure through fully Web-based remote-access and configuration capabilities.

The need for security appliances is rapidly increasing in today's IT space. Security, convenience, and ease of installation and troubleshooting are the important advantages of security appliances compared to the many software-based security applications that exist in the marketplace today. The innovative, new, 1-RU, security-hardened Cisco Secure ACS Solution Engine was designed to specifically alleviate the security issue with a closed-device design that makes it substantially more difficult for intruders to penetrate than an open-platform system.

Security appliances provide an all-in-one approach that simplifies product selection, product integration, and ongoing support. By combining all necessary operating system installation and patching with the ACS software service, customers can avoid maintaining software versioning and proliferation of servers, patches, and operating system (OS) maintenance issues. This is particularly important in large networking environments where security solutions are required in remote sites with no IT professionals present to regularly manage and upgrade these solutions. In addition, a security appliance greatly simplifies support and troubleshooting in failure modes, hence enabling quick service restoration (through a one-stop support contact)—an important consideration, especially when the security application is mission-critical, a situation that is true with security authentication, authorization, and accounting (AAA) applications.

Changing network dynamics and increased security threats have influenced new opportunities in access control management solutions. As AAA becomes more relevant and the requirement to

control user access expands beyond just dialup, new trends (including expanded authentication, tracking, and audit management) are emerging that require identity-networking solutions to be pervasive, scalable, and available throughout the network.

Cisco Secure ACS extends access security by combining authentication, user or administrator access, and policy control from a centralized location, allowing for greater flexibility and mobility, increased security, and user productivity gains. As an accounting service, the Cisco Secure ACS Solution Engine reduces IT operations costs by providing detailed reporting and monitoring capabilities of network users' behavior and by keeping a record of every access connection and device configuration change across the entire network.

Cisco Secure ACS provides a centralized identity networking solution and simplified user-management experience across all Cisco devices and security-management applications. Cisco Secure ACS ensures enforcement of assigned policies by allowing network administrators to control:

- Who can log in to the network
- What privileges each user has in the network
- What accounting information is recorded in terms of security audits or account billing
- What access and command controls are enabled for each configuration administrator

Like the Cisco Secure ACS for Windows, the Cisco Secure ACS Solution Engine supports a wide array of access connection types, including wired or wireless LAN, dialup, broadband, content, storage, voice over-IP (VoIP), firewall, and virtual private networks (VPNs).

Cisco Secure ACS Solution Engine Highlights

The Cisco Secure ACS Solution Engine is a highly secure, OS-independent, and dedicated platform that offers a highly manageable access control solution with an increasingly reduced setup and troubleshooting time. The Cisco Secure ACS Solution Engine provides Plug and Play deployment, a highly reliable AAA solution, and increased TCO protection through the high availability and simplified day-to-day operation and management of the Cisco Secure ACS service. It provides the same features and functions as the Cisco Secure ACS for Windows, in a dedicated, security-hardened, application-specific appliance package. Customers with existing Windows-based Cisco Secure ACS deployments can add or upgrade to Cisco Secure ACS Solution Engines without any effect on existing AAA configurations, including remote logging and replication configurations. More information about the latest Cisco Secure ACS features is available from the Cisco Secure ACS for Windows data sheet.

To ensure the high-security posture of the Cisco Secure ACS Solution Engine, additional functions specific to operating and managing the Cisco Secure ACS Solution Engine are provided. Additionally, a Cisco Secure ACS remote agent is available with each Cisco Secure ACS Solution Engine to enable remote logging and Windows authentication. Forwarding all accounting data from the solution engine to a remote agent preserves disk space on the solution engine. It also improves AAA performance by eliminating the frequent and time-consuming disk writes required for local logging on the solution engine. Also, because a Cisco Secure ACS Solution Engine is never a member of a Microsoft Windows domain, the Cisco Secure ACS remote agent establishes the necessary Windows domain trust relationships for Windows-based authentication.

Table 1 lists additional functions provided by the Cisco Secure ACS Solution Engine. These functions are not available from the Cisco Secure ACS for Windows software product.

Table 1 Functions Provided by the Cisco Secure ACS Solution Engine

Hardened underlying operating system	• The Cisco Secure ACS Solution Engine is dedicated to run only the Cisco Secure ACS service, thereby preventing any appliance-based OS changes, additions, or configuration modifications.
Serial console interface	• A serial console interface is provided on the Cisco Secure ACS Solution Engine for initial configuration, subsequent management of IP connections, access to the Cisco Secure ACS HTML interface, and application of upgrade and recovery procedures. • The serial console interface supports both serial line and Telnet connections through which the Cisco Secure ACS service can be reimaged, reloaded, and rebooted, both locally and remotely.
Solution Engine-specific management tools	• Integrated into the existing Cisco Secure ACS HTML interface, Solution Engine-specific management tools provide generic appliance-management capabilities, including backup, recovery, software upgrades, monitoring, maintenance, and troubleshooting functions. • The Cisco Secure ACS HTML interface is accessed though a secured Secure Sockets Layer (SSL)-based connection.
Cisco Secure ACS remote agent	• The Cisco Secure ACS remote agent provides two functions: authentication against Windows domains and remote logging capabilities of user accounting records. • Administrators can provision primary and backup Cisco Secure ACS remote agents in distributed Cisco Secure ACS configurations.
Port-based packet filtering	• The Cisco Secure ACS Solution Engine implements a packet-filtering service to block traffic on all but the necessary Cisco Secure ACS-specific TCP and UDP ports.
Network Timing Protocol (NTP) support	• The Cisco Secure ACS Solution Engine has built-in NTP functions to maintain network timing synchronization and consistency with other Cisco Secure ACS appliances or network devices.

Cisco Secure ACS Solution Engine-Specific Benefits

In addition to the many benefits the Cisco Secure ACS solution brings in controlling user and administrative AAA inside your network, the Cisco Secure ACS Solution Engine, with its 1-RU hardened form factor, adds specific security and operational advantages in the following areas:

- *Security*—With a security-hardened service focused on running exclusively the Cisco Secure ACS service, the solution engine significantly increases the security posture of the Cisco Secure ACS system. All solution engine services and ports not used by the Cisco Secure ACS service are disabled to secure access to the Cisco Secure ACS Solution Engine.
- *Plug and Play solution*—The Cisco Secure ACS Solution Engine provides a record service uptime before starting to configure the Cisco Secure ACS service.
- *Manageability*—With a dedicated, exclusive, and complete Cisco Secure ACS solution, the appliance greatly simplifies manageability and support of the Cisco Secure ACS service while removing the necessity to manage any UNIX or Windows network operating systems.
- *Supportability*—With no external services or applications (other than the Cisco Secure ACS service) allowed to be installed on the solution engine, the support and the day-to-day management of the Cisco Secure ACS Solution Engine are greatly simplified.

- *Reliability*—Enabling only the services that are required by Cisco Secure ACS allows an increase in overall reliability and security of the Cisco Secure ACS service.
- *TCO*—With a turnkey security-hardened solution engine that is easily deployed, Cisco is able to guarantee full support, maintenance, and serviceability of the overall Cisco Secure ACS system—not just the Cisco Secure ACS software running on various hardware configurations, supported by third-party vendors.
- *Migration from Cisco Secure ACS UNIX*—The Cisco Secure ACS Solution Engine provides a suitable alternative for Cisco Secure ACS UNIX customers not willing to install or manage Cisco Secure ACS on the Windows OS.

System Requirements

Hardware Requirements

The Cisco Secure ACS Solution Engine is available on Cisco 1111 platforms with the following specifications:

- Pentium IV processor, 2.66 GHz
- 1 GB RAM
- 40 GB free disk space
- Two built-in 10/100 Ethernet controllers
- 1 floppy disk drive
- 1 CD-ROM drive

The Cisco Secure ACS remote agent is available in a Windows version that can be installed on a Windows 2000 Server (Windows Domain Controller or Member Server supported).

The computer running Cisco Secure ACS remote agent for Windows must meet the following minimum hardware requirements:

- Pentium III processor, 550 MHz or faster
- 256 MB RAM
- 250 MB free disk space

Ordering Information

The Cisco Secure ACS Solution Engine is available for purchase through normal Cisco sales and distribution channels worldwide. The Cisco Secure ACS Solution Engine is shipped with a preinstalled Cisco Secure ACS Software license.

For More Information

For more information about Cisco Secure ACS, visit: http://www.cisco.com/go/acs.

For specific product functions or technical questions, send e-mail to the Cisco Secure ACS product marketing group at ACS-MKT@cisco.com.

For questions about product ordering, availability, and support contract information, send e-mail to the product marketing group at ciscoworks@cisco.com.

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

203051/ETMG_04/03

04/12

Cisco Systems

Q & A

Cisco Secure **Access Control Server** Solution Engine

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

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

Q. What does Cisco Secure ACS Solution Engine do?

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

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

A. The decision to create a dedicated solution engine version of Cisco Secure ACS was made based on several factors:

- Security—The need to create a turnkey security-hardened service focused on running the Cisco Secure ACS service exclusively. The solution engine can remove all extraneous services, block all unused ports, and otherwise prevent all other access to the Cisco Secure ACS server system—dramatically increasing the security posture of Cisco Secure ACS.
- Manageability—Cisco Secure ACS Solution Engine is a dedicated, exclusive service for AAA with no ability to install or run other services or applications. This greatly facilitates the support and day-to-day management of the Cisco Secure ACS system.
- Reliability—By targeting only the operating system services required by Cisco Secure ACS, the solution engine offers greater operational reliability and security for the Cisco Secure ACS system.
- Total cost of ownership—Customers choosing Cisco Secure ACS can optimize their total cost of ownership. Cisco end-to-end support now includes

full support, maintenance, and serviceability of the Cisco Secure ACS system—not just the Cisco Secure ACS software running on various hardware configurations and supported by various third-party vendors.

- Plug and play—Cisco Secure ACS Solution Engine is shipped already installed with Cisco Secure ACS application software, greatly reducing the time it takes to set up and deploy Cisco Secure ACS in your network.
- Migration from Cisco Secure ACS UNIX—Cisco Secure ACS Solution Engine was built and targeted as a suitable migration platform for Cisco Secure ACS for Unix customers not willing to install or manage Cisco Secure ACS on a Windows server.

Q. What are the differences between the Cisco Secure ACS software server and Cisco Secure ACS Solution Engine?

A. Cisco Secure ACS Solution Engine provides the same features and functions of the Cisco Secure ACS Windows version—in a dedicated, security-hardened, application-specific option. The appliance includes features specific to the operation and management of Cisco Secure ACS, and specific software features needed to be customized or removed due to the different underlying system architectures:

Authentication

- Authentication against a Windows domain requires a Cisco Secure ACS remote agent running on a domain controller or member server. The Cisco Secure ACS remote agent is necessary to establish a Windows member or domain controller trust relationship.
- Authentication against an Open Database Connectivity (ODBC) source is not supported. Lightweight Directory Access Protocol (LDAP) authentication can be used instead.
- Authentication against One-Time Password (OTP) directories is performed using the generic RADIUS-based OTP interface on the appliance. Any OTP vendor that provides an RFC-compliant RADIUS interface can interface with Cisco Secure ACS.

User Database Synchronization

- User database synchronization with an ODBC source is not supported. Instead, the administrator can configure Cisco Secure ACS to synchronize its user database with a comma-separated values (CSV) file on a remote File Transfer Protocol (FTP) server.

ODBC Logging

- ODBC logging is not supported. Administrators can use local or remote CSV logging

Backup/Restore and Appliance Diagnostics

- Backup/restore and gathered appliance diagnostics are performed through a remote FTP server and configured using the current Cisco Secure ACS HTML graphical user interface (GUI).

Q. What additional features are available on Cisco Secure ACS Solution Engine but not available on the Windows version?

A. To ensure the highly secure posture of Cisco Secure ACS Solution Engine, functions specific to operating and managing the appliance have been added:

- Security-hardened underlying operating system.
- Port-based packet filtering, allowing connections only to the ports necessary for Cisco Secure ACS operation.
- Serial console interface for initial configuration, subsequent management of IP connections, Web interface, and application of upgrades and remote reboots. The serial console interface supports both serial line and Telnet connections.

- Backup/restore of Cisco Secure ACS data via FTP protocol.
- Recovery procedures.
- NTP (Network Time Protocol) support for maintaining network time consistency with other appliances or network devices.

Q. Are there any additions to the existing Cisco Secure ACS GUI to support Cisco Secure ACS Solution Engine?

A. Yes. New HTML pages specific to Cisco Secure ACS Solution Engine have been added to the Cisco Secure ACS GUI. These pages cover specific features around the operation and management of the solution engine and include:

- Solution Engine configuration page
- Solution Engine remote agent configuration page
- Solution Engine upgrade page
- Solution Engine status page
- Solution Engine diagnostics log view

Q. What ports and protocols access Cisco Secure ACS Solution Engine?

A. Cisco Secure ACS Solution Engine implements a packet filtering service to block the traffic on all but necessary TCP/User Datagram Protocol (UDP) ports. Only the ports listed in Table 1 are open for input traffic:

Table 1 Cisco Secure ACS Solution Engine Ports Usage

Service Name	UDP	TCP
DHCP	68	
RADIUS authentication and authorization (original draft RFC)	1645	
RADIUS accounting (original draft RFC)	1646	
RADIUS authentication and authorization (revised RFC)	1812	
RADIUS accounting (revised draft RFC)	1813	
TACACS+ AAA		49
Replication and RDBMS synchronization		2000
Cisco Secure ACS remote logging		2001
Cisco Secure ACS distributed logging (appliance only)		2003
Hypertext Transfer Protocol (HTTP) administrative access (at login)		2002
Administrative access (after login) port range		Configurable (default 1024-65535)[1]

1. ACS assigns unique port number from the range to each administration session

Q. What is the hardware platform specification for Cisco Secure ACS Solution Engine?

A. Cisco Secure ACS Solution Engine is a security-hardened Cisco Secure ACS server in a dedicated 1-RU box with the following configuration:

- Intel ISP 1100 motherboard with a 2.66-GHz Pentium 4 processor
- 1 GB of RAM
- Two built-in 10/100 Ethernet controllers
- 40-GB IDE hard drive
- One floppy drive
- One CD-ROM drive

Q. How does Cisco Secure ACS Solution Engine authenticate to Windows domains?

A. In general, to authenticate Windows NT 4.0 or Active Directory domain users, you must establish a Windows member or domain controller trust relationship. Since Cisco Secure ACS Solution Engine does not run the necessary Windows server services to establish this trust, an external Cisco Secure ACS remote agent is provided with the appliance solution, allowing the trust relationship to be established. The Cisco Secure ACS remote agent can be installed on member servers, domain controllers, or backup domain controllers. NOTE: The best practice is to install the remote agent on a full Domain Controller (DC), as this would allow it to perform its authentication functions with the least extra configuration requirements.

Q. What is the main purpose of the Cisco Secure ACS remote agent?

A. The Cisco Secure ACS remote agent has dual roles—it enables authentication against Windows domains, and it allows remote logging capabilities of user accounting records.

Q. What operating systems can the Cisco Secure ACS remote agent be installed on?

A. The Cisco Secure ACS remote agent can be installed on a Windows 2000 server (Windows Domain Controller or Member Server supported). A Solaris version of Cisco Secure ACS will be provided in the future for Sun Solaris installations. Please refer to the Cisco Secure ACS remote agent installation guide for the exact operating system versions and service packs supported.

Q. Can a Cisco Secure ACS remote agent and Cisco Secure ACS Windows coexist on the same server?

A. No. The Cisco Secure ACS remote agent cannot be installed on a server that already has Cisco Secure ACS Windows installed.

Q. Can a solution engine be configured to use several remote agents?

A. Yes. A solution engine can be configured to use one or more agents. There is no restriction that the same agent be used for Windows services and logging services. For Windows services, an appliance can point to a primary and backup agent, in the event that the primary agent is unavailable.

Q. Can a Cisco Secure ACS remote agent be shared with multiple solution engines?

A. Yes. The Cisco Secure ACS remote agent can be shared with multiple solution engines. There is no hard limit to the number of Cisco Secure ACS solution engines that can share a single remote agent, but Cisco will support configurations with up to five solution engines sharing a single Cisco Secure ACS remote agent. If user accounting records from multiple Cisco Secure ACS solution engines need to be consolidated and centralized, it is desired that all these solution engines share a single Cisco Secure ACS remote agent.

Q. Can I perform local logging on Cisco Secure ACS Solution Engine instead of using the remote logging capability of the Cisco Secure ACS remote agent?

A. Yes. However, local logging on Cisco Secure ACS Solution Engine is constrained in size, forcing log files to be recycled after seven days. The Cisco Secure ACS remote agent provides full, unconstrained logging capability to a remote server.

Q. Are there any differences in the type of Windows databases supported by the Cisco Secure ACS remote agent and the ones supported by Cisco Secure ACS Windows?

A. No. The Cisco Secure ACS remote agent supports the same Windows databases supported by Cisco Secure ACS Windows.

Q. What 802.1X authentication types does the Cisco Secure ACS remote agent support?

A. The Cisco Secure ACS remote agent supports the same 802.1X authentication types available on Cisco Secure ACS for Windows. This includes Extensible Authentication Protocol (EAP)-MD5, EAP-TLS, EAP Cisco Wireless, LEAP, PEAP-EAP-GTC, and PEAP-EAP-MSCHAPv2.

Q. Can a Cisco Secure ACS remote agent be provisioned for Cisco Secure ACS for Windows?

A. No. In its initial release, the Cisco Secure ACS remote agent only operates with Cisco Secure ACS Solution Engine. No communication is possible between a Cisco Secure ACS remote agent and a Cisco Secure ACS service on Windows. However, this limitation does not prevent Cisco Secure ACS Windows and Cisco Secure ACS Solution Engine from operating in the same network environment.

Q. What happens to the standard HTML reports on the solution engine? Do they stay the same?

A. In general, these reports stay the same. The solution engine reports will be constrained in size with no support for multiple rolled over files. The Cisco Secure ACS remote agent will provide full, unconstrained report capability on a remote FTP server.

Q. What happens with third-party software tools, such as backup services from Legato?

A. Cisco Secure ACS Solution Engine is a standalone, dedicated box for running Cisco Secure ACS. There are no interfaces or abilities to add third-party software of any kind to the box. Cisco will investigate third-party extensibility, but at present, nothing can be installed on the Cisco Secure ACS Solution Engine other than Cisco Secure ACS images and patches downloaded via FTP. For Cisco Secure ACS backup, Cisco will create an export file that is automatically exported to an external FTP server. Backup tools can be installed and used to backup the external server.

Q. Can I run Cisco Secure ACS in "mixed mode" (for example, run instances of the Cisco Secure ACS Windows and additional instances of Cisco Secure ACS Solution Engine)?

A. Yes. Cisco will support environments using both Cisco Secure ACS Windows and Cisco Secure ACS Solution Engine.

Q. How is Cisco Secure ACS replication affected with the introduction of Cisco Secure ACS Solution Engine?

A. Cisco Secure ACS replication functions will remain unchanged with the introduction of Cisco Secure ACS Solution Engine. Replication between Cisco Secure ACS Solution Engine and Cisco Secure ACS Windows, as well as replication among Cisco Secure ACS solution engines, will be supported with no impact on any of the solution engines or Windows configurations.

Q. Are there any restrictions on whether Cisco Secure ACS Windows or Cisco Secure ACS Solution Engine can be a master database in a replicated configuration?

A. No. Cisco Secure ACS Windows or Cisco Secure ACS Solution Engine can be the master databases replicating to Cisco Secure ACS Windows slaves, Cisco Secure ACS Solution Engine slaves, or both Windows and solution engine slaves at the same time.

Q. Are there any changes to single logon and password aging capabilities in Cisco Secure ACS Solution Engine?

A. No. With the appropriate Windows or domain controller trust relationships established with the Cisco Secure ACS remote agent, single logon and password aging capabilities remain unchanged from Cisco Secure ACS Windows version.

Q. How scalable is a Cisco Secure ACS Solution Engine?

A. The Cisco Secure ACS Solution Engine follows, as a minimum, the same scalability performance as a Windows-based Cisco Secure ACS server. Cisco Secure ACS guidelines and performance analysis shows that each Cisco Secure ACS server can support anywhere from 20,000 to 80,000 users per server, and can scale to support in excess of 10,000 devices, depending on configuration, platform, and usage scenarios. The real challenge in scaling a user access control framework is on the back end. Linked to a high-performance back-end database such as Oracle or Sybase, Cisco has deployed Cisco Secure ACS for Windows 2000 and NT in clustered deployments into customers with hundreds of thousands of user records.

Q. What Cisco Secure ACS Solution Engine features enhance Cisco Secure ACS reliability and remote management?

A. The operating system is configured to automatically reboot on system crash. The serial console service is configured to automatically restart if it fails. Cisco Secure ACS software implements the monitor that will restart Cisco Secure ACS services if they fail. The solution engine also provides a remote administrator command line interface (CLI). The CLI supports both serial line and Telnet connections, and the Cisco Secure ACS service can be reimaged, reloaded, upgraded, and rebooted remotely from the CLI interface.

Q. What support is there for LDAP?

A. Support for LDAP on the appliance is identical to present support from the Cisco Secure ACS Software version. Cisco Secure ACS supports user authentication against records kept in a directory server through LDAP. Cisco Secure ACS supports the most popular directory servers, including Novell and Netscape LDAP Servers, through a generic LDAP interface.

Q. Will Cisco Secure ACS Solution Engine allow "single login" for Windows networking?

A. Yes. Cisco Secure ACS can be set up so that a user will only need to enter a user name and password once. This is considered a "single login." The Cisco Secure ACS remote agent is required to be installed on a Windows network server with the necessary trust relationships to the domain defined.

Q. Does Cisco Secure ACS support OTP and token systems?

A. Yes. Cisco Secure ACS can be configured to communicate with token solutions from ActiveCard, Cryptocard, PassGo Technologies, RSA Data Security, Secure Computing, and Vasco. Cisco Secure ACS Solution Engine includes a generic RADIUS interface for expanding OTP coverage to new vendors. Any OTP vendor that provides an RFC-compliant RADIUS interface should work with Cisco Secure ACS Solution Engine.

Q. What's new in Cisco Secure ACS Version 3.2 for access control functions and features?

A. Cisco Secure ACS Version 3.2 is a minor update to Cisco Secure ACS Version 3.1. It adds the following main features:

- Cisco Secure ACS Solution Engine support
- EAP-MSCHAPv2 support within the Protected EAP (PEAP) framework (used for both wireless and wired environments)
- Machine-based authentication (through EAP-TLS and EAP-MSCHAPv2)
- PEAP authentication against the internal Cisco Secure ACS database
- EAP-TLS authentication against ODBC databases
- EAP-TLS session resume support
- Accounting support for Cisco Aironet® clients
- LDAP multithreading
- Downloadable access control lists (ACLs) for VPN solutions

Please refer to the Cisco Secure ACS Version 3.2 data sheet for more information about the features and functions introduced in this release.

Q. How is Cisco Secure ACS Solution Engine Version 3.2 licensed?

A. Cisco Secure ACS Solution Engine is licensed per server, with unlimited ports, users, and network access servers. The following solution engine packages will be available for ordering. For exact part numbers, refer to the Cisco Secure ACS Version 3.2 product bulletin at: http://www.cisco.com/go/acs

- Cisco Secure ACS Solution Engine Version 3.2
- Cisco Secure ACS Solution Engine upgrade package—Used for upgrading from software versions of Cisco Secure ACS 3.x or Cisco Secure ACS for UNIX to Cisco Secure ACS Solution Engine Version 3.2

Note: The Cisco Secure ACS Solution Engine upgrade package can be ordered when customers have deployed Cisco Secure ACS for Windows or Cisco Secure ACS for UNIX in their networks and want to upgrade to the solution engine version. Please refer to the Cisco Secure ACS Solution Engine user guide and release notes for supported upgrade paths. Current Cisco Secure ACS software maintenance entitlements do not provide a free upgrade to the Cisco Secure ACS Solution Engine.

Q. Can I upgrade to Cisco Secure ACS Version 3.2 from older software versions of Cisco Secure ACS?

A. Yes. A detailed upgrade procedure will be available to guide you through the required steps to complete an upgrade to Cisco Secure ACS Solution Engine. Please refer to the Cisco Secure ACS Solution Engine user guide for more information about the supported upgrade procedure.

Q. Can I purchase or license a backup solution engine?

A. No. An additional Cisco Secure ACS Solution Engine must be purchased as a separate Cisco Secure ACS server license to be used for recovery and backup purposes. Cisco Secure ACS servers can be run as recovery or failover servers. Because Cisco Secure ACS is a central control service in your network, Cisco highly recommends that customers configure a backup server for failover and recovery.

Q. Does Cisco Secure ACS Solution Engine operating system need to be updated when upgrading the Cisco Secure ACS firmware?

A. No. Future Cisco Secure ACS image upgrades are applied to Cisco Secure ACS Solution Engine without updating or modifying the underlying Cisco Secure ACS Solution Engine operating system.

Q. Do I need to patch the solution engine with newer operating system releases or patches?

A. No. All operating system software updates and patches are handled by Cisco Secure ACS Solution Engine upgrades performed by Cisco. Any operating system patch that requires changes to Cisco Secure ACS Solution Engine will be provided in a new upgrade/patch.

Q. Can Cisco Secure ACS Solution Engine software be upgraded remotely from a CD-ROM?

A. Yes. Cisco Secure ACS Solution Engine supports remote upgrades from CD-ROM without any FTP server posting requirements.

Q. Can Cisco Secure ACS Solution Engine support software image rollback during patch update verification?

A. Yes. Cisco Secure ACS Solution Engine can roll back to previously installed software when a software patch has been applied. This capability is used for debugging and verification purposes.

Q. What is the status of Cisco Secure ACS for UNIX?

A. Cisco Secure ACS for UNIX is expected to be discontinued, at which point an end-of-life, end-of-sale (EOL/EOS) announcement will be made. Cisco will support all existing customers and provide smooth migration paths as the new platforms become available. The EOL/EOS date has not been determined, but Cisco will provide customer support for Cisco Secure ACS for UNIX customers for a period no shorter than 24 months after the EOL/EOS date. At present, no new features or releases are planned for Cisco Secure ACS for UNIX and only critical, Priority 1 bugs will be addressed.

Q. Can I use my current Cisco Secure ACS Windows maintenance contract to get support on Cisco Secure ACS Solution Engine?

A. No. Separate hardware and software contracts need to be purchased for maintenance support on Cisco Secure ACS Solution Engine. Please refer to refer to the Cisco Secure ACS Version 3.2 product bulletin for more information. http:// www.cisco.com/go/acs

Q. How can I obtain a demo of Cisco Secure ACS Solution Engine?

A. Please contact your Cisco account manager, who will be able to arrange for a limited time demo of Cisco Secure ACS Solution Engine.

Q. Where can I find more information on Cisco Secure ACS?

A. For additional product information, visit: http://www.cisco.com/go/acs

For additional information or questions, please send e-mail to the Cisco Secure ACS product marketing group at ACS-MKT@cisco.com.

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

203051/ETMG_05/03

NEC

13.650

Comprovação das Especificações Exigidas no Edital 050/2003

3.6. Roteador tipo 1

23/07/03

Roteador Tipo 1	
3700a_ds.pdf	Cisco 3700 Series Multiservice Access Routers
camp_ds.pdf	CiscoWorks Campus Manager
rwan_op.pdf	CiscoWorks Routed WAN Management Solution 1.3

Data Sheet

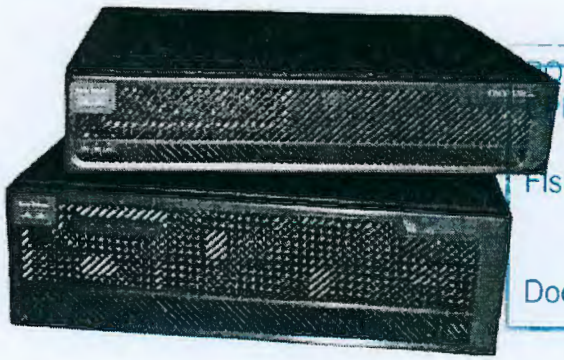
Cisco 3700 Series **Multiservice** Access Routers

Access Platform Optimized for the Modular Integration of Branch Office Applications and Services

Introduction

The Cisco® 3700 Series Multiservice Access Routers are a family of modular routers that enable flexible and scalable deployment of new e-business applications for the Full Service branch office. The Cisco 3700 Series routers optimize the branch office with high performance routing, integrated low density switching, Security, Voice, IP telephony, Video and Content Networking in a single integrated solution. This unique integrated design enables enterprise customers to incrementally adapt to evolving business needs by enabling important services delivered by Cisco IOS®, such as Quality of Service (QoS), IP Multicast, VPN, Firewall, and Intrusion Detection, with the performance required for tomorrows business challenges. The Cisco 3700 Multiservice Access Routers are based on the same modular concepts as the Cisco 3600 Series but enable dramatically higher levels of performance and service integration for the branch office.

Figure 1 The Cisco 3700 Series Multiservice Access Routers



The Cisco 3725 and Cisco 3745 provide on-board LAN/WAN connectivity, new high-density service modules (HDSM), and support for multiple Advanced Integration modules (AIMs) to deliver the highest levels of service density for the enterprise branch office today. Improving on the success of the Cisco 3600 Series' modular architecture, these highly integrated platforms deliver a compelling value proposition with by integrating components previously purchased separately, such as two fixed 10/100 LAN ports and additional memory. With the options of two or four network module slots—which can be adjusted to accept the HDSM modules—three WAN Interface Card (WIC) slots, and two on-board AIM slots, the Cisco 3700 offers many flexible options to enable high densities of services. Providing support for the majority of LAN and WAN interfaces available today on the Cisco 3600 Series platforms reinforces Cisco investment protection promise and maximizes the flexibility of these platforms for the future.

Cisco 3700 Multiservice Access Router Overview

The modular Cisco 3700 Series Multiservice Access Routers leverage network modules (NMs), WAN Interface Cards (WICs), and Advanced Integration Modules (AIMs) from the Cisco 1700, 2600, and 3600 Series Routers for WAN Access, Voice Gateway, Security, Content, and Dial applications. In addition, the Cisco 3725 and Cisco 3745 introduce a new, doublewide form factor, that provides support for the high density services modules (HDSM's). The Cisco 3745 with four network module slots can accept up to two HDSM's by removing the center guides between each pair of adjacent NM slots. The Cisco 3725, with two network module slots can accept a single HDSM in the upper network module slot by removing the blank panel and still have an available network module slot. By utilizing the new HDSM capability the Cisco 3700 Series routers are able to integrate higher port density and new, high performance services.

Figure 2 Cisco 3745 Multiservice Access Router (shown with optional interfaces)

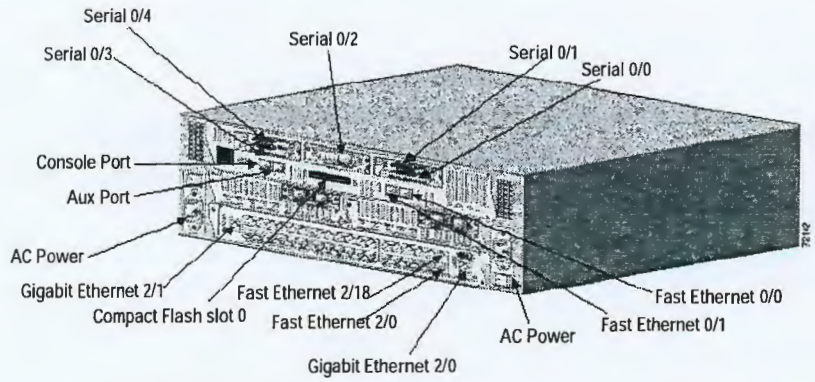
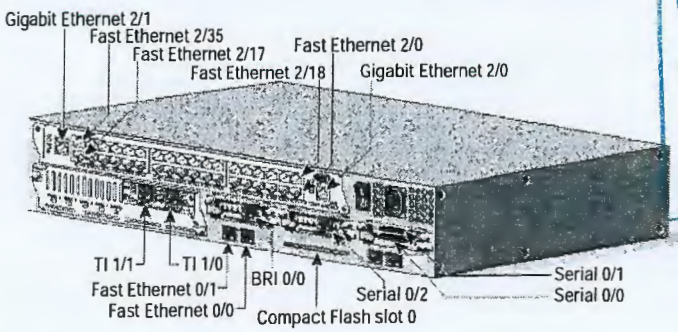


Figure 3 Cisco 3725 Multiservice Access Router (shown with optional interfaces)



Also new in the Cisco 3700 Series is the ability to support integrated In-Line Power on optional 10/100 switching modules for IP Telephony and/or Aironet Wireless LAN applications. By integrating the connectivity slots and ports on the base chassis, the Cisco 3700 Series enables the NM slots to integrate additional services in a small footprint. Both Cisco 3700 platforms offer increased Flash and DRAM default memory to accelerate and simplify future service and feature additions. In addition, the Cisco 3745 router offers additional availability features that may be required in high density, multiple services configurations.

Key features for the Cisco 3725 and 3745:

- Two Integrated 10/100 LAN ports
- Two Integrated Advanced Integration Modules (AIM) slots
- Three Integrated WAN Interface Card (WIC) slots
- Two (Cisco 3725) or four (Cisco 3745) Network Module (NM) slots
- One (Cisco 3725) or two (Cisco 3745) High Density Service Module (HDSM)-capable slots
- 32MB Compact Flash/ 128MB DRAM (default, single 128MB DIMM/SODIMM)
- Both Cisco 3725 and 3745 have a single 128MB SDRAM DIMM module and a single 32MB Compact Flash module by default
- Optional In-Line Power for 16-port EtherSwitch NM, 36-port EtherSwitch HDSM and wireless access points
- Support for all major WAN protocols and media: LL, FR, ISDN, X.25, ATM, fractional T1/E1, T1/E1, xDSL, T3/E3, HSSI
- Support for selected NMs, WICs and AIMs from the Cisco 1700, 2600 and 3600 Series
- 2 RU (Cisco 3725) or 3 RU (Cisco 3745) Rack-mountable chassis
- -24V DC power supply
- NEBS Level 3 compliance

Additional Key Features for the Cisco 3745:

- Field-replaceable motherboard, I/O board and fan tray
- Passive backplane
- Optional internal redundant power supplies (RPS — AC, DC and inline power)
- Online Insertion and Removal (OIR) of NMs and RPSs

Table 1 Cisco 3700 Series Key Features and Benefits

Feature	Benefit
Investment Protection	
Modular platform which shares interfaces with Cisco 1700, 2600, 3600	• Network interfaces are field-upgradable to accommodate future technologies – Additional services can be added on an "integrate as you grow" basis – Leverages the large existing portfolio of WICs, VICs, NMs and AIMs to reduce sparing, training, configuration and installation and maintenance costs
LAN/WAN Connectivity integrated into chassis	• More NM and HDSM slots available to add services in the future – Combination of AIMs and WICs along with NMs/HDSMs gives greater flexibility to create new configurations as requirements change
VPN and Security configurations	• Add security intrusion detection (IDS) and VPN connectivity to the router through Cisco IOS software and optional performance-enhancing data encryption AIMs. – Provides secure connectivity and perimeter security throughout the network.
Flexible voice gateway and IP Telephony configurations	• Incremental or full scale migration from legacy infrastructure to IP Telephony – Supports numerous standards-based analog and digital interfaces to PBXs and the PSTN – Sliding scale options for higher density mixed analog and digital voice gateway configurations

Table 1 Cisco 3700 Series Key Features and Benefits (Continued)

Feature	Benefit
Cisco IOS software	• Supports Cisco IOS feature sets common with the Cisco 2600 and 3600 routers – Enables end to end solutions with full support for Cisco IOS-based QoS, bandwidth management and Security mechanisms
Scalability	
Increased AIM (2) and WIC density (3)	• Services and WAN connectivity and backup can be supported without consuming an NM slot – Increased density per RU of voice, switching, WAN connectivity
Increased default memory of 32MB Compact Flash and 128MB DRAM	• A greater number of new Cisco IOS releases may be added without the need to purchase/install additional memory
New High Density Service Modules (HDSM)	• Enables higher port density and new, high performance services
Availability	
Support for Optional Redundant Power	• Accommodates optional RPS (external for Cisco 3725, internal for Cisco 3745) and minimizes network downtime
Survivable Remote Site Telephony	• Branch offices can leverage centralized call control while cost-effectively providing local branch backup redundancy for IP Telephony
Online Insertion and Removal-capable (3745 only)	• Allows network modules to be swapped or serviced with minimal impact to network availability – Allows servicing of online replacement of RPS – Online replacement of fan tray
Field-replaceable motherboard, I/O board, power supplies and fan tray (3745 only)	• High serviceability design – Additional operations and maintenance flexibility

Advanced Integration Module Options

The Cisco 3700 Series are equipped with two internal slots to support one or two field-installable AIMs. AIMs use function-specific hardware to off-load the main router CPU and accelerate processor- or resource-intensive services, yielding dramatically higher throughput and higher performance than a software-only implementation. The AIM slot has access to virtually all of the router's resources, including the main system bus. The TDM bus and the serial communications controllers make this a very flexible and powerful feature. Since the AIM is internally mounted, external slots remain available for integration of other modular components such as CSU/DSUs, WAN interfaces, or other devices such as modems, or packetized voice/fax processors.

The Data Compression AIM provides a cost-effective option for reducing recurring WAN costs and maximizes the benefit of the advanced bandwidth management features of the Cisco IOS software. With compression ratios of up to 4:1, each integrated Data Compression AIM supports 4 T1/E1s of compressed data throughput with one AIM and up to 8 T1/E1 with two AIMs. The Data Compression AIM supports industry standard LZS and Microsoft Point-to-Point Compression (MPPC) algorithms and ensures compatibility with all Cisco products supporting hardware- or software-based compression.

Three combination Voice + ATM AIM modules are available on the Cisco 3700 Series. The AIM-ATM provides asynchronous transfer mode (ATM) services to the WAN. The AIM-VOICE-30 provides digital signal processor (DSP) services, which can support up to 30 medium-complexity voice channels. The AIM-ATM-VOICE-30 combines the features from the AIM-ATM and AIM-VOICE-30 modules onto a single AIM module. These AIM modules supplement the broad portfolio of Cisco voice solutions and allow enterprises and service providers the flexibility of implementing ATM and voice solutions on the routers. These three Voice and ATM AIM modules provide a cost-effective option for reducing recurring cost and maximizing the benefits of the advanced bandwidth management features of the Cisco IOS software.

The AIM-ATM offers ATM adaptation layer 2 (AAL2) and ATM adaptation layer 5 (AAL5) support for low-density T1/E1 data and voice connections over ATM networks. It supports the following ATM-IMA capabilities: up to 4 T1/E1 of IMA with a single AIM-ATM, and 8 T1/E1 of IMA with two AIM-ATM's (maximum 4 T1/E1 IMA bundle). This AIM module allows service providers and enterprise customers to take advantage of the reliability and quality of service (QoS) available with ATM connectivity. The AIM-VOICE-30 contains DSPs that can support up to 30 medium-complexity voice channels when used with the Voice/WAN (VWIC-MFT) interface card. When the AIM-VOICE-30 can be used in a Cisco 3700, for voice over IP (VoIP) or voice over Frame Relay (VoFR) connectivity while freeing up the network module slot for other applications. The AIM-ATM-VOICE-30 combines the ATM features of AIM-ATM and voice features of AIM-VOICE-30 in a single AIM

The Data Encryption AIM's available for the Cisco 3700 Series offloads encryption processing from the CPU, providing over 10 times the performance over software-only encryption. The AIM-VPN/EP on the Cisco 3725 supports a maximum of 800 tunnels. On the Cisco 3745, the AIM-VPN/HP supports a maximum of 1,800 tunnels. The recently released AIM-VPN/EPII and AIM-VPN/HPII further extends the encryption performance of the Cisco 3700. These modules offers hardware accelerated DES/3DES and the new AES (Advanced Encryption standard) encryption at speeds up to 90-Mbps on the Cisco 3745 (max based on 1400 byte packet size). In addition the AIM-VPN/EPII and AIM-VPN/HPII support hardware-assisted layer-3 compression services where bandwidth conservation may lower network connection costs. The AIM-VPN/EPII on the Cisco 3725 supports a maximum of 8,000 tunnels, and the Cisco 3745, with the AIM-VPN/HPII supports a maximum of 10,000 tunnels.

Key Applications and Benefits

The Cisco 3700 platforms are designed for the Full Service Branch office that are deploying advanced applications, that require higher performance for voice, security, QoS, content acceleration and delivery, and high availability at the network edge by integrating functions previously addressed by a combination of platforms.

Advanced Security Services and VPN's

The Security and VPN features of the Cisco 3700 offer customers the ability to deploy proven security features such as secure VPNs, Intrusion Detection Systems (IDS), and firewalls, as well as high-speed Internet access and the ability to create extranets or demilitarized zones (DMZs). Cisco access routers deliver a rich, integrated package of routing, firewall, intrusion detection, and VPN functions for multiservice applications.

VPNs help companies reap benefits such as dramatically lowered WAN costs, improved global connectivity, and better reliability, while enabling capabilities such as secure extranet communications. Remote dial, Internet, intranet, and extranet access can all be consolidated over a single WAN connection to the Internet. The Cisco 3700 VPN solution supports the features essential to VPNs—IPSec data encryption, tunneling, broad certificate authority support for

public key infrastructure (PKI)—and advanced features such as stateful VPN failover, certificate auto-enrollment, stateful firewall, intrusion detection, and service-level validation. The Cisco 3700 Series works with optional Virtual Private Network Modules (VPN Modules) to optimize the platforms for virtual private networks (VPNs). The Cisco 3700 Series VPN Modules provide up to 10 times the performance over software-only encryption by offloading the encryption processing from the router central processing unit (CPU). The Cisco 3700 series together with the VPN module are the perfect IPSec VPN solution for connecting medium, and large branch offices to other remote locations, corporate headquarters, central-office intranets, or partner extranets.

As network security becomes increasingly critical to securing business transactions, businesses must integrate security into the network design and infrastructure. The Cisco IOS Firewall is a security-specific option for Cisco IOS software which runs on the Cisco 3700 platform. It integrates robust firewall functionality and intrusion detection for every network perimeter and enriches existing Cisco IOS security capabilities. It adds greater depth and flexibility to existing Cisco IOS security solutions—such as authentication, encryption, and failover—by delivering state-of-the-art security features such as stateful, application-based filtering; dynamic per-user authentication and authorization; defense against network attacks; Java blocking; and real-time alerts.

VPN Security Features and Voice and Video-Enabled IPSec VPN

The Cisco 3700 VPN security features are all voice and video-enabled IPSec VPN ready. The Cisco 3700 offers a VPN infrastructure capable of transporting converged voice, video, and data traffic across a secure IPSec network. The Cisco 3700 VPN platforms are able to accommodate the diverse network topologies and traffic types characteristic of multiservice IPSec VPNs, and ensure that the VPN infrastructure does not break multiservice applications deployed now or in the future.

The network architecture of the Cisco Voice and Video-Enabled IPSec VPN (V3PN) Solution takes advantage of Cisco VPN routers with Cisco IOS Software, Cisco CallManager, and IP phones. Furthermore, Cisco provides an overall deployment model for these products through Cisco AVVID (Architecture for Voice, Video and Integrated Data) for converged networking and the SAFE Blueprint for VPNs. These deployment models ensure a secure, interoperable, reliable network solution with end-to-end product support.

Content Acceleration and Delivery

Cisco 3700 Series enables key services critical to supporting the needs of today's enterprise networks. By enabling efficient delivery of rich media and web content, content acceleration and delivery services enhance user productivity while optimizing WAN bandwidth. Cisco 3700 supports the integrated Content Engine Network Module, which leverages the advanced content acceleration features of the Cisco Content Engine 5xx Series into the industry's first router-integrated content delivery system.

As enterprises learn to capitalize on the capabilities of web-based applications, HTTP traffic is assuming a larger proportion of WAN bandwidth. The Content Engine Network Module effectively accelerates applications by optimizing the delivery of bandwidth-intensive and frequently accessed content. Caching alone can offer a 40-60% savings in WAN bandwidth usage by a branch site, and the content delivery capabilities of the module enables enterprise services which maximize the productivity and efficiency of a global enterprise. Integration of the application layer services of the Content Engine Network Module with intelligent network services such as QoS, compression and IPSec offer a superior bandwidth optimization solution for the enterprise branch.

Combining intelligent caching, content filtering and content delivery capabilities with robust branch office routing helps users optimize their networks for important branch IP services such as VOIP, while greatly simplifying configuration, deployment, and operation of network services. Running Cisco Application and Content Networking System (ACNS) software, the Content Engine Network Module enables customers to extend the value of their branch router infrastructure to deliver strategic new application services – such as Employee Internet Management, Streaming Media, live and on-demand e-communications and e-learning, with no performance degradation of core routing services. Further, the Content Engine Network Module interoperates with all Cisco devices, and leverages key Cisco IOS features such as multicast and WCCP while supporting key management solutions such as CiscoWorks.

Integration of Flexible Routing and Low Density Switching

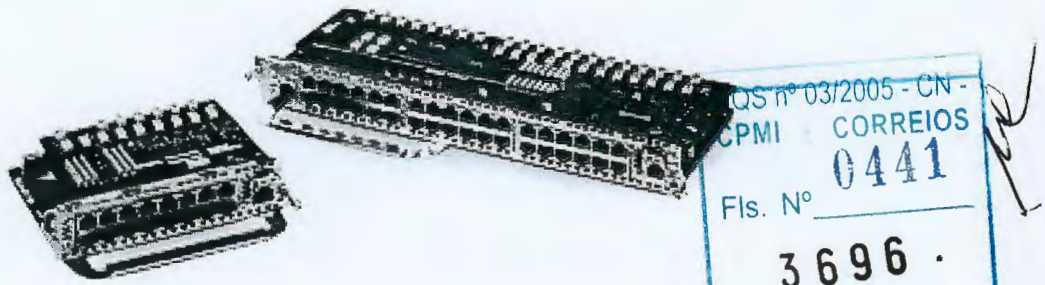
The Cisco 3700 Series offers an optional 16-port 10/100 EtherSwitch network module (NM), or an optional 36-port 10/100 EtherSwitch high density service module (HDSM), both of which leverage the proven Cisco Catalyst technology. The EtherSwitch NM/HDSM hardware supports 802.1p Layer 2 prioritization, while Cisco IOS supports Layer 3 Diff-Serv and Class of Service (CoS) markings for critical business data. Coupling Layer 2/3 prioritization techniques, with the QoS for the WAN, the Cisco 3700 Series ensures low latency for critical business applications, enabling the deployment of e-business applications.

The EtherSwitch ports can also be used to power the Cisco Aironet Access Points in the low-density-branch to deliver Wireless LAN (802.11b) access flexibility. The Cisco 3700 Series with the EtherSwitch NM/HDSM integrates Cisco IOS routing and Catalyst switching technologies in a single platform, offering a single point of management for easier configuration, troubleshooting and a lower total cost of ownership.

Key features include:

- Combination of the industry-leading Cisco IOS features with Catalyst switching technologies for wire-rate Layer 2 switching, with rich protocol and feature support.
- Integrated platform, with EtherSwitch ports for LAN, WAN flexibility, and a rich QoS toolkit for e-business applications.
- Enables simple, single point for configuration and troubleshooting, while integrating diverse technologies.
- Modular design enables scaling as business needs evolve with options for 16- or 36-port EtherSwitch module port densities.

Figure 4 Cisco 16- and 36-port EtherSwitch Modules



Single Platform Solution for Branch Office IP Telephony and Voice Gateway

As the migration to converged voice/data networks accelerates, enterprises need to deploy a platform that has the ability to immediately or gradually grow to support a wide range of traditional telephony devices in addition to newer IP telephony solutions. The Cisco 3700 Series delivers on that need by supporting legacy phone systems through a variety of scalable analog telephony connectivity options starting at two analog ports and scaling to 16, 32, 48 or 64 analog ports. Digital telephony connectivity is just as scalable with options beginning at 12 channels and scaling up to up to 240 channels. IP telephony solutions are also supported on the Cisco 3700 Series through a powerful set of features including line powered IP phone connectivity that begins with 16 ports and scales to 36, 52, or 72 ports in a single platform.

The performance-tuning of the Cisco 3700 Series enables customers to apply quality of service, bandwidth optimization and fragmentation services, along with other advanced call admission control, call control and queuing mechanisms, without sacrificing the expected data performance needed for future growth. The Cisco 3700 Series offers resilient IP telephony services, including Survivable Remote Site Telephony (SRST), H.323, SIP and MGCP, and redundant power for the system and IP phones.

With the Cisco 3700 Series, enterprises can deploy this scalable platform to support all of their telephony needs without investing in all connectivity requirements in the initial deployment. The enhanced service density of the Cisco 3700 allows enterprises the opportunity to deploy a base level configuration that will scale to the converged telephony needs of that branch when necessary. This modular telephony format mitigates future technology lockout.

Deployment of IP Telephony infrastructure solutions are facilitated by the following key Cisco 3700 features:

- Optional modular integration of an inline-powered EtherSwitch NM or HDSM, combined with analog and/or digital high-density voice gateway modules and flexible WAN connectivity for a modular, single-platform IP Telephony infrastructure
- Resilient IP Telephony services, including Survivable Remote Site Telephony (SRST), H.323, SIP and MGCP, and redundant power for system and IP phones
- Complete Cisco CallManager support for both H.323 and MGCP call control protocols makes the Cisco 3700 the ideal voice gateway
- Performance-tuned to scale both analog, and digital voice solutions and hybrid solutions
- Modular expandability enables the addition of gateway or phone aggregation ports as needed
- Integrated Time Division Multiplexing (TDM) for full Drop&Insert functionality between all WIC, Network Module and onboard AIM's

The evolution from traditional TDM voice to IP Telephony has created the requirement that branch offices be equipped to deploy IP Telephony solutions without the need to replace the branch office access platforms. The Cisco 3700 series fulfills that need by ensuring complete support for the range of voice gateway densities and IP Telephony features necessary for Enterprises' evolving branch office infrastructures.

Figure 5 Cisco 3700 Full Serivce Branch integrated capabilities

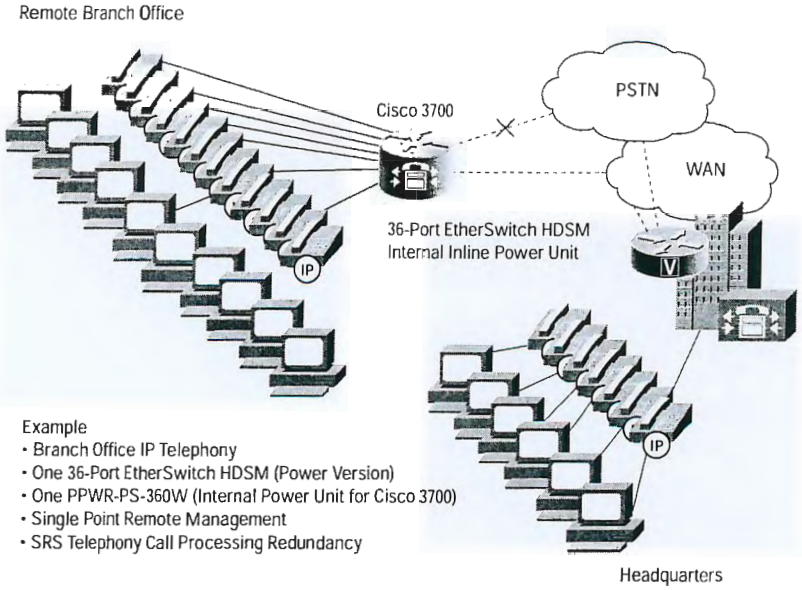
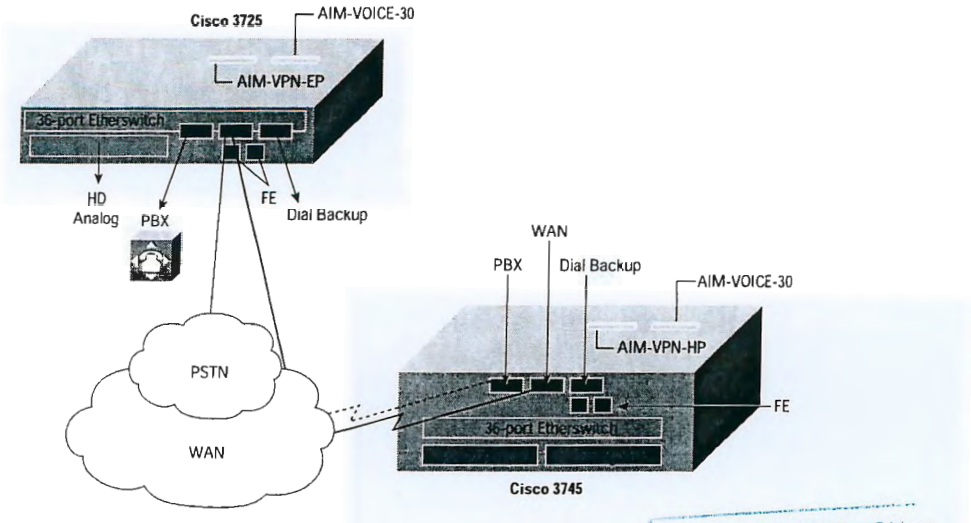


Figure 6 Full Service Branch scenarios



Cisco 3700 enables higher service densities through a versatile, wider interface form factor (using a HDSM), additional interface options with three WIC slots, CPU offload with two built-in AIM slots, and on-board LAN/WAN connectivity to free up module slots.

Table 2 Supported Interfaces for the Cisco 3700 Series

Interfaces	Description
LAN/WAN	• FE Combo NMs (NM-1FE2W, etc.) • 1 port Multimode Fiber FE NM • 1 port Gigabit Ethernet GBIC NM • 1 port ADSL WIC • 1 port G.SHDSL WIC
LAN	• 16 & 36 port EtherSwitch NMs
Serial	• 2 port Serial WIC • 1 and 2 port T1/E1 CSU/ DSU VWICs • 1 port 56k CSU/DSU WIC • 4 and 8 port Sync/Async Serial NMs • HSSI NM1 port T1 CSU/DSU WIC • 16 & 32 port Async NMs • 1 port serial WIC • 4 port serial NM • 1-port T3/E3 with Integrated DSU
ISDN/Channel	• 1 and 2 port T1/E1 Channelized/ ISDN Pri NMs • 4 and 8 port T1/E1 ISDN BRI NMsISDN BRI WICs
Voice	• Low Density Analog Voice NMs (all VICs except BRI NT/TE) • High Density Analog Voice NM • High density T1/ E1 Digital Voice NMs • BRI NT/TE VIC • DSP AIM
ATM	• 4 and 8 port T1/E1 NMs • 1 port DS3 / E3 NMs • SAR AIM • SAR/DSP AIM
Modem	• Digital Modem NMs • 1 and 2 port Analog Modem WICs • 4 and 8 port Analog Modem NMs
Services	
Security, VPN and Compression	• EP & HP Encryption AIMs • EP & HP II Encryption AIMs • COMPR4 AIM • Layer 2 Data Compression • Intrusion Detection NM
Content Delivery	• Content Engine NM

Specifications

Table 3 Cisco 3700 Series Specifications

Description	Specification
Processor Type	• Cisco 3725—MIPS RISC processor • Cisco 3745—MIPS RISC processor
Performance	• Cisco 3725—100kpps • Cisco 3745—225kpps
Flash Memory (Compact Flash)	• Internal: 32MB (default), expandable to 128MB • External: 32MB, 64MB,128MB options
System Memory	• 128MB (SDRAM default)—expandable to 256MB
Integrated WIC slots	• 3
Onboard AIM (internal)	• 2
Console port	• 1 (up to 115.2 kbps)
Aux port	• 1 (up to 115.2kbps)
Minimum Cisco IOS Release	• Cisco IOS 12.2(8) T
Onboard LAN ports	• 2 10/100 Fast Ethernet ports
Redundant Power Supply Support	• Cisco 3725—Universal DC (24VDC to 60VDC), PWR600-AC-RPS External RPS • Cisco 3745—Internal Redundant options for AC and Universal DC (24VDC to 60VDC)
Rack Mounting	• Yes, 19' and 23" options
Power requirements	
Power Supply	• Cisco 3725— – 135W Maximum AC to DC power supply – 495W Maximum with optional power supply:,-48V@360W) AC to DC power supply • Cisco 3745— – 230W Maximum ()AC-DC Power Supply – 590W Maximum (Per AC Input) with optional power supply -48V@360W) AC-DC power
Heat Dissipation	• Cisco 3725— – 135W Maximum 460.661 BTU/hour – 495W Maximum 1689.089 BTU/hour • Cisco 3745— – 230W Maximum 784.829 BTU/hour – 590W Maximum 2013.257 BTU/hour
Output	• Cisco 3725— – (optional -48V@7.5A) • Cisco 3745— – (optional -48V@7.5A)

Table 3 Cisco 3700 Series Specifications (Continued)

Description	Specification
AC input voltage	• 100 to 240VAC
Frequency	• 47-63Hz
AC input current	• Cisco 3725— – 2A max @ 100VAC;1A max @ 240VAC (215W Maximum) with optional power supply: – 7A Max@100VAC;3.5A max @ 240VAC (665W Maximum) • Cisco 3745— – 5A max @ 100VAC;2.5A max @ 200VAC (365W Maximum) with optional power supply: – 10A max @100VAC;5A max@200VAC (815W Maximum)
Environmental Specifications	
Operating temperature	• 32 to 104 F (0 to 40 C)
Nonoperating temperature	• -40 to 185 F (-40 to 85 C)
Relative humidity	• 5-95% noncondensing
Operation altitude	• Up to 6500 ft (2000m), derate 1C per 1,000 ft.
Dimensions (HxWxD)	• Cisco 3725—3.5 x 17.1 x 14.7 in. • Cisco 3745—5.25 x 17.25 x 16 in.
Weight (without NMs or WICs or additional Power Supplies)	• Cisco 3725—14 lbs. • Cisco 3745—32 lbs.
Regulatory Compliance	
Safety	• UL 1950 • CAN/CSA-C22.2 No. 950 • EN 60950 • IEC 60950 • TS 001
EMC	• FCC Part 15 • ICES-003 Class A • EN55022 Class A • CISPR22 Class A • AS/NZS 3548 Class A • VCCI Class A

Table 3 Cisco 3700 Series Specifications (Continued)

Description	Specification
Telecom	• FCC Part 68 • Canada CS-03 • JATE • RTTE Directive
Interface Support	
High Density Service Modules	NMD-36-ESW, NMD-36-ESW-2GIG, NMD-36-ESW-PWR, NMD-36-ESW-PWR-2G
Network Modules	NM-16ESW, NM-16ESW-PWR, NM-16ESW-1GIG, NM-16ESW-PWR-1GIG, NMD-36-ESW, NMD-36-ESW-PWR, NMD-36-ESW-2GIG, NMD-36-ESW-2G, NM-1FE-FX-V2, NM-1FE2W, NM-2FE2W, NM-1FE1R2W, NM-2W, NM-1HSSI, NM-4A/S, NM-4B-S/T, NM-4B-U, NM-8A/S, NM-8B-S/T, NM-8B-U, NM-1CT1, NM-1CT1-CSU, NM-2CT1, NM-2CT1-CSU, NM-1CE1B, NM-1CE1U, NM-2CE1U, NM-2CE1B, NM-4E1-IMA, NM-4T1-IMA, NM-8E1-IMA, NM-8T1-IMA, NM-1A-T3, NM-1A-E3, NM-1V, NM-2V, NM-HDA-4FXS, NM-HDV-1T1-12, NM-HDV-1E1-12, NM-HDV-1E1-30, NM-HDV-1E1-30E, NM-HDV-2E1-60, NM-HDV-1T1-24, NM-HDV-2T1-48, NM-HDV-1T1-24E, NM-HDV-2T1-48, NM-6DM, NM-12DM, NM-18DM, NM-24DM, NM-30DM, NM-16A, NM-32A, NM-1A-OC3MM, NM-1A-OC3SMI, NM-1A-OC3SML, NM-1A-OC3MM-EP, NM-1A-OC3SMI-EP, NM-1A-OC3SML-EP, NM-1GE, NM-1T3/E3, NM-CE-BP-SCSI-K9, NM-CE-BP-20G-K9, NM-CE-BP-40G-K9, NM-4T, NM-8AM, NM-16AM
WICs, VWICs, and VICs	WIC-2T, WIC-2A/S, WIC-1B-S/T, WIC-1B-U, WIC-1DSU-56K4, VWIC-1MFT-T1, VWIC-2MFT-T1, VWIC-2MFT-T1-DI, VWIC-1MFT-E1, VWIC-2MFT-E1, VWIC-2MFT-E1-DI, VWIC-1MFT-G703, VWIC-2MFT-G703, WIC-1ADSL, WIC-1AM, WIC-2AM, VIC-2DID, VIC-2FXS, VIC-2FXO, VIC-2FXO-EU, VIC-2FXO-M1, VIC-2FXO-M2, VIC-2FXO-M3, VIC-2E/M, VIC-2CAMA, VIC-2BRI-S/T-TE, WIC-1T, WIC-1DSU-T1, WIC-1SHDSL, VIC-2BRI-NT/TE
AIMs	AIM-VPN-HP, AIM-VPN-EP, AIM-VPN/EPII, AIM-VPN/HPII, AIM-ATM, AIM-VOICE-30, AIM-ATM-VOICE-30, AIM-COMPR4

Ordering Information

The Cisco 3700 Series is orderable through the following part numbers:

Part Number	Description
CISCO3725	3700 Series, 2-Slot, Dual FE, Multiservice Access Router
CISCO3745	3700 Series, 4-Slot, Dual FE, Multiservice Access Router

13635 A.

Summary

The Cisco 3700 Series Multiservice Access Routers enable flexible and scalable deployment of new e-business applications in an integrated branch office access platform. The Cisco 3700 Series is ideal for sites and solutions requiring the highest levels of integration at the edge for Branch Office IP Telephony, voice gateway, and integrated flexible routing with low-density switching solutions. In addition, the Cisco 3700 Series provides a consolidated service infrastructure and high service density in a compact form factor that enables the incremental integration of branch applications and services.

Service and Support

The award-winning Cisco Service and Support offerings provide presales network audit planning, design consulting, network implementation, operational support, and network optimization. By including service and support when purchasing Cisco 3700 products, customers can confidently deploy a converged network architecture using Cisco expertise, experience, and resources.

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

Web: 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

04.03 BW9112

Comprovação das Especificações Exigidas no Edital 050/2003

3.7. Roteador tipo 2

23/07/03

Roteador Tipo 2	
c1751_ds.pdf	Cisco 1751 Modular Access Router

Cisco Systems

Data Sheet

Cisco **1751** Modular Access Router

Cisco 1751 Modular Access Router is ideally suited to help you evolve your organization into an e-Business. It supports e-Business features such as VPNs; secure Internet, intranet, and extranet access with optional firewall technology; broadband DSL and cable connectivity; and multiservice voice/video/data/fax integration. The Cisco 1751 Modular Access Router offers:

- Flexibility to adapt to changing requirements
- Modularity that allows you to individually configure the system to meet specific business needs
- Investment protection with features and performance to support new WAN services such as broadband DSL and cable access, multiservice voice/data integration, and VPNs
- Integration of multiple network functions, including an optional firewall VPN, and data service unit/channel service unit (DSU/CSU) to simplify deployment and management

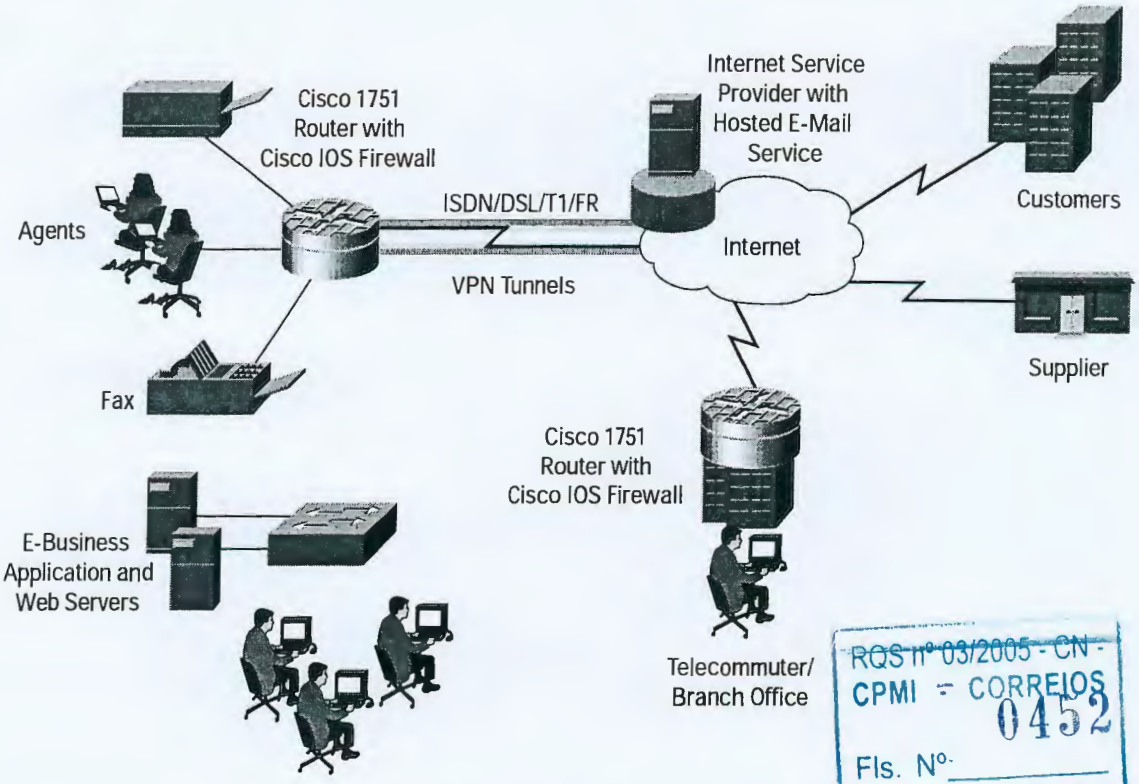
The Cisco 1751 Router delivers these capabilities with the power of Cisco IOS Software in a modular integrated access solution. The Cisco 1751 Router provides a cost-effective solution to support e-Business applications through a comprehensive feature set including support for:

- Multiservice voice/fax/data integration
- Secure Internet, intranet, and extranet access with VPN and firewall
- Integrated broadband DSL connectivity
- VLAN support (IEEE 802.1Q)

The Cisco 1751 Router, a member of the Cisco 1700 Family, features a modular architecture that enables cost-effective upgrades and additions of WAN and voice interfaces. Integrated network services and functions, such as optional firewall, DSU/CSU, and VPN features, reduce the complexity of deploying and managing e-Business solutions. The Cisco 1751 Router offers investment protection when your business needs it, with a RISC architecture and features to support new technologies and applications such as voice/video/data/fax integration and VPNs. See Figure 2.

Figure 1
The Cisco 1751 Router delivers a versatile e-Business WAN access solution.

Figure 2
Cisco 1751 Routers provide all necessary capabilities to connect to the Internet and communicate with vendors, customers, and other employees and offices.



The Cisco 1751 Router is available in two models that enable you to easily tailor an access solution to suit your e-Business requirements today and in the future. See Table 1.

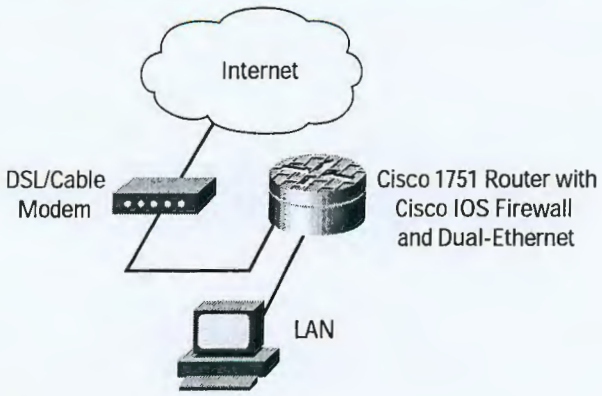
Table 1 The Cisco 1751 Modular Access Router

Cisco 1751 Base Model	Includes everything an office needs for data networking now (16 MB Flash, 32 MB DRAM, and Cisco IOS IP software feature set), with a simple upgrade path to full voice functionality. WAN interface cards are available separately.
Cisco 1751-V Multiservice Model	Includes all the features needed for immediate integration of data and voice services with support for up to two voice channels (32 MB Flash and 64 MB DRAM, one DSP (PVDM-256K-4), and Cisco IOS IP Plus Voice feature set). Voice and WAN interface cards are available separately.

All Cisco 1751 models offer three modular slots for voice and data interface cards, an autosensing 10/100BaseT Fast Ethernet LAN port supporting standards-based IEEE 802.1Q VLAN, a console port, and an auxiliary port. The Cisco 1751 Router supports the same WAN interface cards as the Cisco 1600, 1700, 2600, and 3600 Series routers, and the same voice interface cards and voice-over-IP (VoIP) technology as the Cisco 1700, 2600, and 3600 Series routers. This simplifies support requirements. The WAN interface cards support a wide range of services, including synchronous and asynchronous serial, Integrated Services Digital Network Basic Rate Interface (ISDN BRI), ADSL,

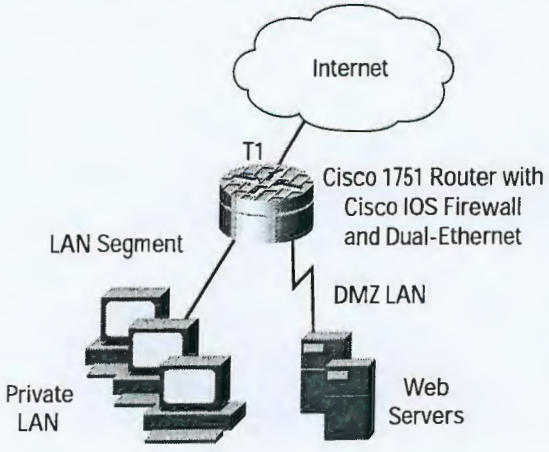
and serial with DSU/CSU options for primary and backup WAN connectivity. The voice interface cards support Foreign Exchange Office (FXO), Foreign Exchange Station (FXS), Network and User Side Voice BRI (ISDN BRI NT/TE), Ear & Mouth (E&M), direct inward dial (DID), and T1/E1 Multiflex VWICs. Additionally, an Ethernet interface card provides the Cisco 1751 Router with dual-Ethernet capability to support the external broadband modem devices. See Figure 3.

Figure 3
Cisco 1751 Router Incorporating Ethernet WAN Interface Card (WIC) Deployed with Broadband Modem



In addition, dual-Ethernet capability on the Cisco 1751 Router enables the creation of perimeter/DMZ (demilitarized zone) LANs to enhance security by physically separating private and public data. See Figure 4.

Figure 4
Cisco 1751 Router Incorporating Ethernet WIC to Deploy Perimeter/DMZ LAN



Combined, these interfaces support a comprehensive set of applications, including multiservice voice/video/data/fax integration, Frame Relay, ISDN BRI, SMDS, X.25, broadband DSL and cable services, and VPNs.

Key Benefits

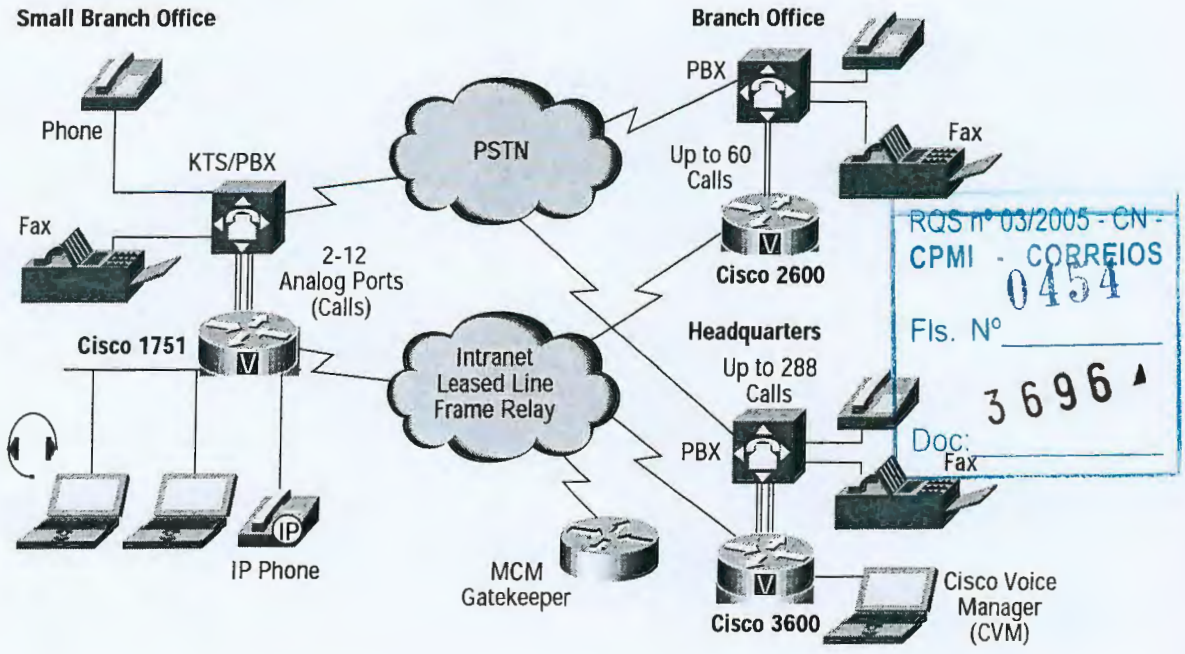
The Cisco 1700 Series routers support the value of end-to-end Cisco network solutions with the following benefits:

Flexibility—The modular Cisco 1751 Router adapts easily to fit the needs of growing businesses. Interchangeable WAN interface cards enable easy additions or changes in WAN technologies without requiring a forklift upgrade of the entire platform. Modular data and voice slots enable users to tailor data and voice services as needed. With the ability to use the same field-upgradable WAN and voice interface cards across multiple Cisco access router platforms, the Cisco 1751 Router reduces requirements for spare parts inventory and support training.

Multiservice Access—For businesses that want to become e-Businesses and incorporate applications that integrate multiservice voice/video/data/fax capabilities now or in the future, the Cisco 1751 Router offers a flexible, cost-effective answer. The Cisco 1751 Router enables network managers to save on long-distance interoffice billing costs. It also interoperates with next-generation voice-enabled applications such as integrated messaging and Web-based call centers. The Cisco 1751 Router works with the existing telephone infrastructure—phones, fax machines, key telephone systems (KTS) units, and PBX (including digital PBXs)—minimizing capital costs. See Figure 5.

Figure 5

Voice/video/data/fax integration. The Cisco 1751 Router integrates data and voice capabilities, significantly lowering toll charges for small- and medium-sized businesses and enterprise small branch offices.



Lower Cost of Ownership—The Cisco 1751 Router provides a complete solution for integrated voice and data access in a single product, eliminating the need to install and maintain a large number of separate devices. You can combine optional functions—including a voice gateway, dynamic firewall, VPN tunnel server, DSU/CSU, ISDN network

termination-1 (NT1) device, and more—to reduce deployment and management costs. This solution can be managed remotely using network management applications such as CiscoWorks2000 and CiscoView or any SNMP-based management tool.

Investment Protection—The Cisco 1751 Router RISC architecture, Cisco IOS Software, and modular slots provide solid investment protection. The Cisco 1751 incorporates services such as multiservice voice/video/data/fax integration, VPNs, and broadband DSL and cable communications to enable today's successful e-Business. An internal expansion slot on the mother- board offers the ability to support hardware-assisted IPSec data encryption at T1/E1 speeds.

For a complete list of Cisco 1751 Router features and benefits, see Table 2.

Table 2 Key Features and Benefits

Features	Benefits
Flexibility	
Full Cisco IOS Software support, including multiprotocol routing (IP, IPX, Apple Talk, IBM/SNA) and bridging	• Provides the industry's most robust, scalable, and feature-rich internetworking software support using the de facto standard networking software for the Internet and private WANs • Part of the Cisco end-to-end network solution
Integrated Voice and Data Networking	
Cisco 1751 router chassis accepts both WAN and voice interface cards	• Reduces long-distance toll charges by allowing the data network to carry interoffice voice and fax traffic • Works with existing handsets, key units, and PBXs, eliminating the need for a costly phone-equipment upgrade
Modular Architecture	
Accepts an array of WAN and voice interface cards	• Adds flexibility and investment protection
WAN interface cards and voice interface cards are shared with Cisco 1600, 1700, 2600, and 3600 routers	• Reduce cost of maintaining inventory • Lower training costs for support personnel • Protect investments through re-use on various platforms
Autosensing 10/100 Fast Ethernet	• Simplifies migration to Fast Ethernet performance in the office
Expansion Slot on Motherboard	• Allows expandability to support hardware-assisted encryption at T1/E1 speeds • Allows support for future technologies
Dual DSP Slots	• Allow expandability to support additional voice channels
Security	
The Cisco IOS Firewall Feature Set includes context-based access control for dynamic firewall filtering, denial-of-service detection and prevention, Java blocking, real-time alerts, Intrusion Detection System (IDS), and encryption	• Allows internal users to access the Internet with secure, per-application-based, dynamic access control, while preventing unauthorized Internet users from accessing the internal LAN

Table 2 Key Features and Benefits (Continued)

Features	Benefits
IPSec DES and 3DES	• Enable creation of VPNs by providing industry-standard data privacy, integrity, and authenticity as data traverses the Internet or a shared public network • Supports up to 168-bit encryption
Hardware-Based Encryption Using Optional VPN Module	• Supports wire-speed encryption up to T1/E1 speeds
Device Authentication and Key Management	
IKE, X.509v3 digital certification, and support for certificate enrollment protocol (CEP) with certification authorities (CAs) such as Verisign and Entrust	• Ensure proper identity and authenticity of devices and data • Enable scalability to very large IPSec networks through automated key management
User Authentication	
PAP/CHAP, RADIUS, TACACS+	• Support all leading user identity verification schemes
VPN Tunneling	
IPSec, GRE, L2TP, L2F	• Offer choice of standards-based tunneling methods to create VPNs for IP and non-IP traffic • Allow standards-based IPSec or L2TP client to interoperate with Cisco IOS tunneling technologies • Fully interoperable with public certificate authorities and IPSec standards-based products • Part of the scalable Cisco end-to-end VPN solution portfolio
Cisco Easy VPN client	• Allows the router to act as remote VPN client and have VPN policies pushed down from the VPN concentrator
Cisco Unified VPN Access Server	• Allows the router to terminate remote access VPNs initiated by mobile and remote workers running Cisco VPN client software on PCs; and allows the router to terminate site-site VPNs initiated by IOS routers using the Cisco Easy CPN client feature
Management	
IEEE 802.1Q VLAN Support	• VLANs enable efficient traffic separation, provide better bandwidth utilization, and alleviate scaling issues by logically segmenting the physical LAN infrastructure into different subnets
Manageable via SNMP (CiscoView, CiscoWorks2000), Telnet, and console port	• Allow central monitoring, configuration, and diagnostics for all functions integrated in the Cisco 1751 router, reducing management time and costs
Cisco SDM	• Simplifies router and security configuration through smart wizards to enable customers to quickly and easily deploy, configure and monitor a Cisco access router without requiring knowledge of Cisco IOS Command Line Interface (CLI)

Table 2 Key Features and Benefits (Continued)

Features	Benefits
Ease of Use and Installation	
Cisco ConfigMaker, SETUP configuration utility, AutoInstall, color-coded ports/cables, and LED status indicators	• Simplifies and reduces deployment time and costs with graphical LAN/VPN policy configurator; command-line, context-sensitive configuration questions; and straightforward cabling • LEDs allows quick diagnostics and troubleshooting
Network Address Translation (NAT) and Easy IP	• Simplifies deployment and reduces Internet access costs
QoS	
CAR, Policy Routing, WFQ, PQ/CBWFQ, GTS, RSVP, DSCP, cRTP, MLPPP and LFI	• Allocates WAN bandwidth to priority applications for improved performance
Reliability and Scalability	
Cisco IOS Software, dial-on-demand routing, dual-bank Flash memory, scalable routing protocols such as OSPF, EIGRP, and HSRP	• Improves network reliability and enables scalability to large networks
Broadband Connectivity Options	
ADSL and cable connectivity deliver business-class broadband access	• Leverage broadband access technologies like cable and DSL to increase WAN connectivity speeds and reduce WAN access costs • The Cisco 1751 supports ADSL connectivity with ADSL WIC • Cable connectivity with the Cisco 1751 and optional integrated Cisco uBR910 Series Cable DSU deliver business-class broadband access
Device Integration	
Integrated router, voice gateway, firewall, encryption, VPN tunnel server, DSU/CSU, and NT1 in a single device	• Reduce costs and simplifies management

Cisco IOS Technology

Internet and Intranet Access

Cisco IOS Software provides an extensive set of features that make the Cisco 1751 Router ideal for flexible, high-performance communications across both intranets and the Internet:

- Multiprotocol routing (IP, IPX, and AppleTalk), IBM/SNA, and transparent bridging over ISDN, asynchronous serial, and synchronous serial such as leased lines, Frame Relay, SMDS, Switched 56, X.25, and X.25 over ISDN D
- WAN optimization—including dial-on-demand routing (DDR), bandwidth-on-demand (BOD) and OSPF-on-demand circuit, Snapshot routing, compression, filtering, and spoofing to reduce WAN costs

Security

Cisco IOS Software supports an extensive set of basic and advanced network security features, including access control lists (ACLs); user authentication, authorization, and accounting (such as PAP/CHAP, TACACS+, and RADIUS); and data encryption. To increase security, the integrated Cisco IOS Firewall Feature Set protects internal LANs from attacks with context-based access control (CBAC) and Intrusion Detection (IDS), while IPSec tunneling with data encryption standard DES and 3DES encryption provide standards-based data privacy, integrity, and authenticity as data travels through a public network. Additionally, remote management applications, such as Cisco Security Device Manager (SDM), make it easier than ever to deploy and monitor security applications on your Cisco router.

The Cisco 1700 Series routers support the Cisco Easy VPN client feature that allows the routers to act as remote VPN clients. As such, these devices can receive predefined security policies from the headquarters' VPN head-end, thus minimizing configuration of VPN parameters at the remote locations. This solution makes deploying VPN simpler for remote offices with little IT support or for large deployments where it is impractical to individually configure multiple remote devices. While customers wishing to deploy and manage site-to-site VPN would benefit from Cisco Easy VPN client because of its simplification of VPN deployment and management, managed VPN service providers and enterprises who must deploy and manage numerous remote sites and branch offices with IOS routers for VPN will realize the greatest benefit.

The Cisco 1700 Series routers also support the Cisco Unified VPN Access Server feature that allows a Cisco 1700 router to act as a VPN head-end device. In site-to-site VPN environments, the Cisco 1700 router can terminate VPN tunnels initiated by the remote office routers using the Cisco Easy VPN client. Security policies can be pushed down to the remote office routers from the Cisco 1700 Series routers. In addition to terminating site-to-site VPNs, a Cisco 1700 Series router running the Unified VPN Access Server can terminate remote access VPNs initiated by mobile and remote workers running Cisco VPN client software on PCs. This flexibility makes it possible for mobile and remote workers, such as sales people on the road, to access company intranet where critical data and applications exist.

For remote access, VPNs, Layer 2 Forwarding (L2F), and Layer 2 Tunneling Protocol (L2TP) combine with IPSec encryption to provide a secure multiprotocol solution for IP, IPX, and AppleTalk traffic, and more. Mobile users can dial in to a service provider's local point of presence (POP) and data is "tunneled" (or encapsulated inside a second protocol such as IPSec or L2TP) back to the Cisco 1751 router to securely access the corporate network via the Internet.

Cisco IOS Software QoS Features

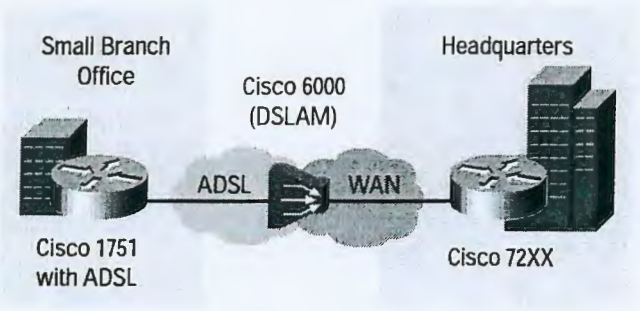
Through Cisco IOS Software, the Cisco 1751 Router delivers quality of service (QoS) capabilities, including Resource ReSerVation Protocol (RSVP), Weighted Fair Queuing (WFQ), Committed Access Rate (CAR), and IP Precedence. These features enable businesses to prioritize traffic on their networks by user, application, traffic type, and other parameters, to ensure that business-critical data and delay-sensitive voice are appropriately prioritized.

Because the Cisco 1751 Router provides robust voice compression, up to 8 voice calls can occupy a single 64K data channel simultaneously, without compromising data performance. Cisco IOS voice compression technology integrates data and voice traffic to enable efficient use of existing data networks.

High-Performance Architecture for VPNs and Broadband Service

A robust RISC architecture and Cisco IOS features enable the Cisco 1751 Router to support VPN applications with tunneling and security, as well as DSL, cable, and other broadband access technologies. An internal slot on the Cisco 1751 motherboard supports an optional VPN module that provides hardware-assisted IPSec DES and 3DES encryption at T1/E1 speeds. The Cisco 1751 Router equipped with the WIC-1ADSL supports VPN over ADSL service. See Figure 6. The Cisco 1751 Router with the uBR910 series cable DSU supports business-class broadband cable access. The Ethernet WIC (WIC-1ENET) provides an alternate method of deploying DSL/cable Internet access with the use of an external modem. In some cases, the ISP provides the broadband modem.

Figure 6
The Cisco 1751Router, deployed in conjunction with the ADSL WIC, enables SMB and small branch customers to reap the benefits of ADSL.



Network Management and Ease of Installation

The Cisco 1751 Router supports a range of network-management and ease-of-installation tools:

- The Cisco Security Device Manager (SDM) is an intuitive, web-based device management tool embedded within the Cisco IOS access routers. SDM simplifies router and security configuration through smart wizards to enable customers to quickly and easily deploy, configure and monitor a Cisco access router without requiring knowledge of Cisco IOS Command Line Interface (CLI). For more information visit www.Cisco.com/go/sdm.
- Cisco ConfigMaker is a Windows wizard-based tool designed to configure a small network of Cisco routers, switches, hubs, and other network devices from a single PC. This tool makes it easy to configure value-add security features such as the Cisco IOS Firewall Feature Set, IPSec encryption, and network address translation (NAT); establish VPN policies (including QoS and security); and configure the Dynamic Host Configuration Protocol (DHCP) server.
- CiscoWorks for Windows, a comprehensive network management solution for small to medium sized networks that provides Web-based network monitoring and device configuration management.
- CiscoWorks2000, the industry-leading Web-based network management suite from Cisco, simplifies tasks such as network inventory management and device change, rapid software image deployment, and troubleshooting.
- For service providers, Cisco Service Management (CSM) provides an extensive suite of service management solutions to enable planning, provisioning, monitoring, and billing.

13623
A.

Extending Cisco End-to-End Solutions

As part of the comprehensive Cisco end-to-end networking solution, the Cisco 1700 Series routers enable businesses to extend a cost-effective, seamless network infrastructure to the small branch office. The Cisco 1700 Family of access routers includes the Cisco 1751 Router and Cisco 1721 Router—a modular device optimized for data-only connections. WAN cards work with both devices, as well as with Cisco 1600, 2600, and 3600 Series routers. They are powered by Cisco IOS Software for robust WAN service between branches and central offices in organizations with multiple sites. Both feature RISC-based processors to provide performance for encryption and support for emerging broadband technologies.

The Cisco 1751 Router also shares VoIP technology and analog voice interface cards with Cisco 2600 and 3600 Series routers. This feature provides an end-to-end solution for multiservices communications between offices, simplifying inventory needs and leveraging IT expertise across more devices in an organization.

For a complete list of physical interfaces, see Tables 3, 4, 5, and 6.

Table 3 Physical Interfaces/Architecture

One 10/100 BaseT Fast Ethernet Port (RJ45)	Automatic speed detection; automatic duplex negotiation; VLAN support
One Voice Interface Card Slot	Supports a single voice interface card with two ports per card
Two WAN Interface Card/Voice Interface Card Slots	Supports any combination of up to two WAN interface cards or voice interface cards
Ethernet WAN Interface Cards	Supports PPP and PPPoE; operates in full and half-duplex modes
One Auxiliary (AUX) Port	RJ-45 jack with RS232 interface (plug compatible with Cisco 2500 Series AUX port); asynchronous serial DTE with full modem controls (CD, DSR, RTS, CTS); asynchronous serial data rates up to 115.2 kbps
One Console Port	RJ-45 jack with RS232 interface (plug compatible with Cisco 1000/1600/ 2500 series console ports); asynchronous serial DTE; transmit/receive rates up to 115.2 kbps (default 9600 bps, not a network data port); no hardware handshaking such as RTS/CTS
One Internal Expansion Slot	Supports hardware-assisted services such as encryption (up to T1/E1)
RISC Processor	Motorola MPC860P PowerQUICC at 48MHz

Table 4 WAN Support

Asynchronous Serial Interfaces on Serial WAN Interface Cards	Interface speed: up to 115.2 Kbps; asynchronous serial protocols: Point-to-Point Protocol (PPP), Serial Line Internet Protocol (SLIP); asynchronous interface; EIA/TIA-232
ISDN WAN Interface Cards	ISDN dialup and ISDN leased line (IDSL) at 64 and 128 Kbps; encapsulation over ISDN leased line; Frame Relay and PPP
ADSL WAN Interface Cards	Supports ATP adaption Layer 5 (AAL5) services and applications; interoperates with Alcatel DSLAM with Alcatel chipset and Cisco 6130/ 6260 DSLAM with Globespan chipset; ANSI T1.413 issue 2 and ITU 992.1 (G.DMT) compliant

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0460
Doc: 3696
459

Table 5 WAN Interface Cards for the Cisco 1751 Router

Module	Description
WIC-1T	One serial, async, and sync (T1/E1)
WIC-2T	Two serial, async, and sync (T1/E1)
WIC-2A/S	Two low-speed serial (up to 128 kbps), async, and sync
WIC-1B-S/T	One ISDN BRI S/T
WIC-1B-U	One ISDN BUI U with integrated NT1
WIC-1DSU-56K4	One integrated 56/64-kbps, four-wire DSU/CSU
WIC-1DSU-T1	One integrated T1/fractional T1 DSU/CSU
WIC-1ADSL	One-port ADSL interface
WIC-1ENET	One-port 10BaseT Ethernet Interface
WIC-1SHDSL	One-port G.SHDSL interface
WIC-1AM	One-port V.90 analog modem WIC
WIC-2AM	Two-portV.90 analog modem WIC

Table 6 Voice Interface Cards for the Cisco 1751

VIC-2FXS	Two-port FXS voice/fax interface card for voice/fax network module
VIC-2DID	Two-port DID (direct inward dial) voice/fax interface card
VIC-2FXO	Two-port FXO voice/fax interface card for voice/fax network module
VIC-2FXO-EU	Two-port FXO voice/fax interface card for Europe
VIC-2FXO-MI	Two-port FXO voice/fax interface card with battery reversal detection and Caller ID support (for US, Canada, and others) [enhanced version of the VIC-2FXO]
VIC-2FXO-M2	Two-port FXO voice/fax interface card with battery reversal detection and Caller ID support (for Europe) [enhanced version of the VIC-2FXO-EU]
VIC-2FXO-M3	Two-port FXO voice/fax interface card for Australia
VIC-2E/M	Two-port E&M voice/fax interface card for voice/fax network module
VIC-2BRI-NT/TE	Two-port network Side ISDN BRI interface
VIC-4FXS/DID [1]	Four-port FXS and DID voice/fax interface card
VWIC-1MFT-T1	One-port RJ-48 multiflex trunk - T1
VWIC-2MFT-T1	Two-port RJ-48 multiflex trunk - T1
VWIC-2MFT-T1-DI	Two-port RJ-48 multiflex trunk - T1 with drop and insert
VWIC-1MFT-E1	One-port RJ-48 multiflex trunk - E1
VWIC-2MFT-E1	Two-port RJ-48 multiflex trunk - E1

Table 6 Voice Interface Cards for the Cisco 1751

VWIC-2MFT-E1-DI	Two-port RJ-48 multiflex trunk - E1 with drop and insert
VWIC-1MFT-G703	One-port RJ-48 multiflex trunk - E1 G.703
VWIC-2MFT-G703	Two-port RJ-48 multiflex trunk - E1 G.703

1. The Cisco 1751 can support three VIC-4FXS/DID cards with a maximum of four ports in DID mode

Voice Implementation Requirements

The Cisco 1751 Modular Access Router supports FXO, FXS, E&M, ISDN BRI VICs, and T1/E1 multiflex V/WICs.

The FXO interface allows an analog connection to the central office of the Public Switched Telephone Network (PSTN). The FXS interface connects basic telephone service phones (home phones), fax machines, key sets, and PBXs through ring voltage and dial tone. The E&M interface allows connection for PBX trunk lines (tie lines). The ISDN-BRI NT/TE VIC is used to connect to the PSTN or a PBX/KTS, whereas the T1/E1 multiflex V/WIC (multiflex V/WIC) supports both data and voice services. The multiservice-ready Cisco 1751-V router version includes all the features needed for immediate integration of data and voice services:

- One DSP—(PVDM-256K-4)
- 32-MB Flash memory
- 64-MB DRAM
- Cisco IOS IP/VOX Plus feature set

VICs and WICs are available separately.

The Cisco 1751 and Cisco 1751-V routers have two DSP module slots on the motherboard and a maximum of eight DSPs are supported per router.

DSP Requirements

Cisco 1751 routers support 3 types of DSP images: high complexity (HC), medium complexity (MC) and Flexi-6. HC and MC are used for analog[1] and BRI (VIC-2BRI-NT/TE) VICs; Flexi-6 is used for T1/E1 VWICs[2] and BRI VIC. MC is introduced in Cisco 1751 starting from Cisco IOS 12.2(8)YN release, which will merge into 12.3(1)T. Therefore, please make sure to use Cisco 12.2(8) YN or later releases when using MC. In addition, starting from 12.2(8)YN release, the default DSP image for BRI VIC is changed from HC to Flexi-6. Table 7 lists the default images for each type of VICs; Table 8 lists IOS support for each DSP image. Table 9 lists the number of channels supported by one DSP (PVDM-256K-4) for each codec type.

Please use the following rules for calculating DSP requirements on the Cisco 1751:

1. For the Early Deployment (ED) releases: Cisco IOS 12.2(2)XK, 12.2(4)XW, 12.2(4)XL, 12.2(4)XM, 12.2(4)YA, 12.2(4)YB, 12.2(8)YL, 12.2(8)YM and 12.2(11)YT, or T train releases prior to 12.3(1)T:

1. Analog VICs include VIC-2FXS, VIC-2FXO, VIC-2FXO-M1, VIC-2FXO-M2, VIC-2FXO-M3, VIC-2FXO-EU, VIC-2E/M, VIC-2DID, VIC-4FXS/DID

2. T1/E1 VWICs include VWIC-1MFT-T1, VWIC-2MFT-T1, VWIC-2MFT-T1-DI, VWIC-1MFT-E1, VWIC-2MFT-E1, VWIC-2MFT-E1-DI, VWIC-1MFT-G703, VWIC-2MFT-G703

- a. Each 2-port analog VIC requires 1 DSP (PVDM-256K-4)
- b. Each VIC-2BRI-NT/TE requires 2 DSPs (PVDM-256K-8)
- c. For VWICs, refer to Table 9. For example, 12 G.711 digital T1/E1 voice calls require two DSPs; 12 G.729 calls require four DSPs
- d. Total DSP requirement is the sum of a, b and c. The DSP resources can not be shared between analog VICs, BRI VIC and VWICs.

2. For the Early Deployment (ED) releases: Cisco IOS 12.2(8)YN or later (Note: not including 12.2(11)YT) or T train releases 12.3(1)T or later, please always refer to the DSP Calculator in the following link:

   http://www.cisco.com/cgi-bin/Support/DSP/cisco_prodsel.pl

The DSP calculator optimizes the DSP resources for your configuration and suggests CLI configurations.

Table 7 DSP Firmware for each type of VICs

VIC Type	Firmware Support
2-port Analog VICs	HC (default), MC (starting from 12.2(8)YN)
4-port Analog VIC	HC, MC (default, starting from 12.2(8)YN)
VIC-2BRI-NT/TE	HC (default for ED releases prior to 12.2(8)YN or T train releases prior to 12.3(1)T); MC; Flexi-6 (default for ED releases 12.2(8)YN or later or T train releases 12.3(1)T or later);
T1/E1 VWICs	Flexi-6 (default)

Table 8 Cisco IOS support for DSP firmware

Firmware Support	IOS Release Support
HC	In all orderable IOS Releases
MC	ED Releases: Cisco IOS 12.2(8)YN or later [1] T Train Releases: Cisco IOS 12.3(1)T or later
Flexi-6	For T1/E1 VWICs: • ED Releases: Cisco IOS 12.2(4)YB or later [2] • T Train Releases: 6th releases of 12.2T or later For VIC-2BRI-NT/TE: • ED Releases: Cisco IOS 12.2(8)YN or later [3] • T Train Releases: Cisco IOS 12.3(1)T or later

1. It doesn't include Cisco 12.2(11)YT. 12.2(11)YT doesn't support MC.
2. It doesn't include Cisco 12.2(11)YT. 12.2(11)YT doesn't support Flexi-6.
3. It doesn't include Cisco 12.2(11)YT. 12.2(11)YT doesn't support Flexi-6.

Table 9 The number of channels supported by one DSP (PVDM-256K-4) per codec type

	Firmware		
Codec	HC (for analog & BRI VICs)	MC (for analog & BRI VICs)	Flexi 6 (for VWICs & BRI VIC[1])

Table 9 The number of channels supported by one DSP (PVDM-256K-4) per codec type

	Firmware		
G.711	2	4	6
G.729ab[2] /G.729a	2	4	3
G.726	2	4	3
G.723	2	-	2
G.728	2	-	2
Fax Relay	2	4	3

1. BRI VIC support in Flexi-6 starts from 12.2(8)YN or 12.3(1)T.
2. G.729 and G.729b is not supported in MC or Flexi-6 images.

Table 10 DSP Modules Available on Cisco 1751

Modules	DSPs
PVDM-256K-4	1 DSP Module
PVDM-256K-8	2 DSP Modules
PVDM-256K-12	3 DSP Modules
PVDM-256K-16HD	4 DSP Modules
PVDM-256K-20HD	5 DSP Modules

Cisco IOS Software Feature Sets

The Cisco 1751 Router supports a choice of Cisco IOS Software feature sets. Each feature set requires specific amounts of Flash and DRAM memory in the product. For default memory configurations, please see Table 11.

Table 11 Cisco 1751 Router Memory Defaults and Maximums

Model Number	Default FLASH/Maximum FLASH	Default DRAM/Maximum DRAM
Cisco 1751	16 MB/16 MB	32 MB/96 MB
Cisco 1751-V Multiservice Model	32 MB/32 MB	64 MB/128 MB

The Cisco 1751 Router supports a choice of Cisco IOS Software feature sets with rich data features as well as data/voice features (Table 12). Each feature set requires specific amounts of RAM and Flash memory in the product.

- Cisco IOS IP base feature sets include: NAT, OSPF, RADIUS, and NHRP.
- Plus feature sets contain L2TP, L2F, the Border Gateway Protocol (BGP), IP Muliticast, Frame Relay SVC, RSVP, the NetWare Link Services Protocol (NLSP), AppleTalk SMRP, the Web Cache Control Protocol (WCCP), and the Network Timing Protocol (NTP).

- Encryption is offered in special encryption feature sets (Plus IPSec 56, and Plus IPSec 3DES). The VPN encryption module requires an IOS IP Plus IPSec image.
- DSL support is only in the Plus feature sets.

Table 12 Cisco IOS Features

Cisco 1751 Router Data Software Feature Sets for Cisco IOS Release 12.1.(5)YB		
Feature Name	**Product Code**	**CD Number**
IP	S17C-12105YB	CD17-C-12.1.5=
IP ADSL	S17C7-12105YB	CD17-C-12.1.5=
IP Plus ADSL	S17C7P-12105YB	CD17-C7P-12.1.5=
IP Plus IPSec 56 (DES) ADSL	S17C7L-12105YB	CD17-C7L-12.1.5=
IP Plus IPSec 3DES ADSL	S17C7K2-12105YB	CD17-C7K2-12.1.5=
IP/FW/IDS	S17CH-12105YB	CD17-CH-12.1.5=
IP/FW/IDS Plus IPSec 56 (DES) ADSL	S17C7HL-12105YB	CD17-C7HL-12.1.5=
IP/IPX	S17B-12105YB	CD17-B-12.1.5=
IP/IPX/FW/IDS Plus ADSL	S17B7HP-12105YB	CD17-B7HP-12.1.5=
IP/FW/IDS Plus IPSec 3DES ADSL	S17C7HK2-12105YB	CD17-C7HK2-12.1.5=
IP/IPX/AT/IBM	S17Q-12105YB	CD17-Q-12.1.5=
IP/IPX/AT/IBM Plus ADSL	S17Q7P-12105YB	CD17-Q7P-12.1.5=
IP/IPX/AT/IBM/FW/IDS Plus IPSec 56 (DES) ADSL	S17Q7HL-12105YB	CD17-Q7HL-12.1.5=
IP/IPX/AT/IBM/FW/IDS Plus IPSec 3DES ADSL	S17Q7HK2-12105YB	CD17-Q7HK2-12.1.5=
Cisco 1751 Router Data/Voice Software Feature Packs for Cisco IOS Release 12.1.(5)YB		
Feature Name	**Product Code**	**CD Number**
IP/Voice Plus	S17CVP-12105YB	CD17-C7VP-12.1.5=
IP/Voice Plus ADSL	S17C7VP-12105YB	CD17-C7VP-12.1.5=
IP/Voice Plus IPSec 56 (DES) ADSL	S17C7VL-12105YB	CD17-C7VL-12.1.5=
IP/Voice/FW/IDS Plus ADSL	S17C7HV-12105YB	CD17-C7HV-12.1.5=
IP/Voice/FW/IDS Plus IPSec 56 ADSL	S17C7HVL-12105YB	CD17-C7HVL-12.1.5=
IP/Voice Plus IPSec 3DES ADSL	S17C7VK2-12105YB	CD17-C7VK2-12.1.5=
IP/Voice/FW/IDS Plus IPSec 3DES ADSL	S17C7HVK2-12105YB	CD17-C7HVK2-12.1.5=
IP/IPX/Voice/FW/IDS Plus ADSL	S17B7HPV-12105YB	CD17-B7HPV-12.1.5=
IP/IPX/AT/IBM/FW/IDS Voice Plus IPSec 56 (DES) ADSL	S17Q7HVL-12105YB	CD17-Q7HVL-12.1.5=
IP/IPX/AT/IBM/FW/IDS/Voice Plus IPSec 3DES ADSL	S17Q7HVK2-12105YB	CD17-Q7HVK2-12.1.5=

Other IOS Features Include:

QoS Features

- Frame Relay Fragmentation (FRF.12)
- IP Precedence
- Generic Traffic Shaping (GTS)
- Frame Relay Traffic Shaping (FRTS)
- Weighted Random Early Detection (WRED)
- DSCP Marking
- Compressed RTP
- Multiple Link PPP & Link Fragmentation and Interleaving
- Resourse Reservation Protocol (RSVP)
- Queuing Techniques: Weighted Fair Queuing (WFQ), Priority Queuing (PQ), Low Laterey Queuing (LLQ) and Custom Queuing (CQ)
- Preclassification for IPSec Tunneling

Voice Support

- VoIP
- VoFR
- VoATM
- Fax Pass Through
- Fax Relay
- Modem Pass Through

VoIP Protocol Support

- H.323 V2
- Media Gateway Control Protocol 1.0
- Session Initiation Protocol 2.0

Codec Support

- G.711
- G.729
- G.729a
- G.723.1
- G.726
- G.728

Technical Specifications

Dimensions

- Width: 11.2 in. (28.4 cm)
- Height: 4.0 in. (10.0 cm)
- Depth: 8.7 in. (22.1 cm)
- Weight (minimum): 3.0 lb (1.36 kg)
- Weight (maximum): 3.5 lb (1.59 kg)

Power

- Locking connector on power socket
- External Power Brick
- AC Input Voltage: 100 to 240 VAC
- Frequency: 50 - 60 Hz
- AC Input Current: rated 1 A, measured 0.5 A
- Power Dissipation: 20W (maximum)

Environmental

- Operating Temperature: 32 to 104 F (0 to 40 C)
- Nonoperating Temperature: –4 to 149 F (–20 to 65 C)
- Relative Humidity: 10 to 85% noncondensing operating; 5 to 95% noncondensing, nonoperating

Safety

- Regulatory Approvals
  - UL 1950, 3rd Edition
  - CSA 22.2 No 950-95, 3rd Edition
  - EN60950 with A1 through A4 and A11
  - EN41003
  - TCA TS001–1997
  - AS/NZS 3260 with A1 through A4
- IEC 60950 with A1 through A4 and all country deviations
- NOM-019-SCFI
- GB4943
  - ETSI 300-047
  - BS 6301 (power supply) EMI
  - AS/NRZ 3548 Class B
- CNS-13438
  - FCC Part 15 Class B
  - EN60555-2 Class B

- EN55022 Class B
- VCCI Class II
- CISPR-22 Class B

- EN55024 comprised of:
  - IEC 1000-4-2 (EN61000-4-2)
  - IEC 1000-4-3 (ENV50140)
  - IEC 1000-4-4 (EN61000-4-4)
  - IEC 1000-4-5 (EN61000-4-5)
  - IEC 1000-4-6 (ENV50141)
  - IEC 1000-4-11
  - IEC 1000-3-2 Network Homologation
  -
- Europe: CTR2, CTR3, TBR21
- Canada: CS-03
- United States: FCC Part 68
- pan: Jate NTT
- Australia/New Zealand: TS013/TS-031, TS002, TS003
- Hong Kong: CR22

Service and Support

Leading-edge technology deserves leading-edge support. Service and support for the Cisco 1751 is available on a one-time or an annual contract basis. Support options range from help desk assistance to proactive, onsite consultation. All support contracts include:

- Major Cisco IOS Software updates in protocol, security, bandwidth, and feature improvements
- Full access to Cisco.com for technical assistance, electronic commerce, and product information
- 24-hour-a-day access to the industry's largest dedicated technical support staff

A support contract maximizes the value of your technology investment throughout its lifecycle, ensuring optimum performance and availability. Augment your internal staff's capabilities by taking full advantage of Cisco expertise.

Contact your local sales office for further information.

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 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

ETMG 202903_01/03

NEC
13613
A.

Comprovação das Especificações Exigidas no Edital 050/2003

4. Servidores corporativos

23/07/03

0469

NEC

13612
A.

Comprovação das Especificações Exigidas no Edital 050/2003

4.1. Servidores Intel

23/07/03

NEC

1361

Comprovação das Especificações Exigidas no Edital 050/2003

4.1.1. Servidores Intel tipo 1

23/07/03

xSeries 440

$40,299.00 IBM List Price

Model Name: **86877RX**

Part Number: **86877RX**

Accessories & Upgrades

← Servers

Intel-based servers

Rack-optimized

Universal

Appliance

Storage

Accessories & upgrades

Services

Support

Certification

Education and training

News and awards

Library

HW/SW compatibility

Technical Details

Architecture

Form factor:	Rack
Orientations allowed:	Horizontal
Bus type/architecture:	
Slots x bays total (free):	6(6) x 4(2)
Expansion bus type:	PCI

Multimedia

Media device type:	CD-ROM
Media speed:	24X Max
Media interface type:	EIDE
Media data transfer rate:	2500KBps
Media average access time:	110ms
Media transport type:	Front tray loading
Recordable:	No
Removable:	Yes
Audio features:	
Multimedia features:	

Expansion Options

Slots total (free) and type:	2(2) 64 Bit Active PCI-X 100 MHz Hot Swap, 2 (2) 64 Bit Active PCI-X 133 MHz Hot Swap, 2(2 64 Bit Active PCI-X 66 MHz Hot Swap
3.5" bays	1(0) SL, 2(2) SL
- accessible (free) and height:	
- not accessible (free) and height:	
5.25" bays	1(0) SL
- accessible (free) and height:	
- not accessible (free) and height:	
Plug and play support:	Yes
Parallel ports (type):	
Serial ports (type):	1 (RS485), 3 (USB)
Expansion ports:	Keyboard, Mouse, RJ-45

Graphics Subsystems

Graphics Chip Set Model & Mfr.:	S3 Savage4 LT
Graphics Data Width:	128-bit
Graphics Type:	--
Default Memory Address:	
Video RAM Std (MB):	8MB
Video RAM Max (MB):	8MB
Video RAM Type:	SDRAM
Graphics Bus Interface:	PCI
Resolution Max (Video RAM Std), NI:	1024x768
Resolution Max (Video RAM Max), NI:	1600x1200
Colors Max (Video RAM Std):	16777216
Colors Max (Video RAM Max):	65536
Graphics features:	DDC-2B compliant

Hard Disk

Hard Disk 1:

Number of installed hard disks:	
Hard disk size[1]:	--
Hard disk controller:	Adaptec 7899 Integrated Dual Channel Ultra160 SCSI
Hard disk type:	Open bay
Total possible device types:	
Max internal hard disk capacity:	146.8GB
Average seek time:	--
Average latency:	--
RAID levels supported:	
Hot swappable drive bays:	2
Cache size:	--
Number of platters:	
Platter RPM:	
Burst transfer rate:	
Sustained data trans rate (low; high):	--
Additional storage features:	
Optional hard disk available:	

Memory

Memory (RAM) std/max:	2GB / 32768MB
RAM speed:	133MHz
Optional RAM configuration:	512:1024 DIMMs
RAM type:	PC133 SDRAM
RAM slots total (available):	16 DIMM (12 DIMM)

Networking

Network interface:	Gigabit Ethernet- Integrated
Network speed:	10Mbps, 100Mbps, 1000Mbps
Network features:	RJ-45 connector (for 10Base-T/100Base-TX), 10Base-T/100Base-TX port

Power Management

Power supply:	1050Watts
Power supply type:	110-220 volt Hot Swap Redundant 2 Std.
Power supply additional:	
Heat emissions:	361W
Sound emissions:	62dB
Cooling system:	4 fans
UPS:	Yes
Power management features4:	

System Management

Adapter:	Remote Supervisor Adapter
Software:	Power-on password Privileged access password Selectable boot Unattended start-up
Features:	Ethernet and Fast Ethernet Compatible Networks; Network Speed of 100Mbps/10Mbps PCI Interface Bus; RJ11 Connectors; RJ45 Connectors; RS 232 Connectors; RS 485 Connectors; RS-232 Connectors; 32-bit Data/Address Width

Processor

Processor (CPU)2:	Intel Xeon MP
Processor internal clock speed2:	2.00GHz
Front Side Bus:	400MHz
Processor manufacturer:	Intel
Math co-processor:	
L1 internal CPU cache:	--
L2 internal CPU cache:	512KB
L2 external CPU cache std:	--
L2 external CPU cache type:	
Upgradable processor:	
Processor upgrade options:	
Processor upgrade method:	Add processor option
BIOS type:	Flash
Number of processors std/max:	4/8
SMP capable (multiple processors):	Yes
Multi-processor bus (slots/speed):	--
L3 cache:	2MB

Security

AssetCare features:	IBM Director Remote I/O ServerGuide
Security features:	Power-on password Privileged access password Selectable boot Unattended start-up
VPD support:	

Software

Tested operating systems:	Microsoft Windows NT 4.0 Enterprise Edition, Microsoft Windows 2000 Advanced Server, Microsoft Windows 2000 Server, Novell Netwar 6.0, Red Hat Linux Advanced Server 2.1, SuSE 8.0, VMware ESX Server v1.5
Operating system provided:	
Communication/networking applications:	
Device drivers/utilities:	
Multimedia applications:	
Productivity applications:	
Other applications provided:	

Standard Features

Pointing device type:	
Standard diskette size:	3.5" 1.44MB
Keyboard type standard:	
I20 Compliant:	
Product approvals/certifications4:	VCCI Class A (Japan); TUV-GS; UL-1950; CE MARK; CISPR-22 Class A; CSA C22.2 No. 950; FCC Class A - Part 15; ICES-003 Class A (Canada); IEC-60950 Certificate/Report; IEC-950; NOM 019; BSMI (Taiwan); C-Tick Mark (AS/NZS 3548 Class A)

Warranty

Limited Warranty period and type:	One year parts and labor IBM On-Site Repair (IOR)

Weight & Dimentions

Weight:	110lbs
Travel weight:	--
Height:	7in
Height with stand:	--
Width:	19in
Width with stand:	--
Depth:	27.5in
Operating Temperature (C) (low; high):	10; 35
Relative Humidity (%) (low; high):	8; 80

Other

Recommendation:	

▶ Important Legal Information

Doc 7

1360 7

United States

73.4GB 10K Ultra 160 SCSI Hot Swap SL HDD

$639.00 IBM List Price

Part Number: **06P5756**

eserver

IIII

Take advantage of IBM's latest SCSI hard disk drive (HDDs) technology with optional high- spee high-density 10,000rpm Ultra160 SCSI slim-line HDDs in hot-swap xSeries servers and IntelliStation workstations. These 3.5-inch, hot-swap HDD options can double xSeries storage capacities for those who need high-speed data storage for demanding enterprise server and workstation applications. These HDDs store a tremendous amount of data in a slim-line form factor. This optimizes the storage capacities of supported servers, while providing excellent storage subsystem performance.

Features & Benefits:

• Ÿ 10,000rpm HDDs -- Deliver solid reliability and excellent performance
Ÿ Ultra160 SCSI interface -- wide bandwidth for streaming data transfers
Ÿ Available in hot-swap version:
- Converged hot-swap drive tray -- Supports xSeries servers, Netfinity servers, IntelliStation workstations, and EXP storage units with hot-swap bays
Ÿ Predictive Failure Analysis (PFA) -- Can alert you of a problem before it occurs

Technical Details

Characteristics

Interface bus:	SCSI
Form factor:	SL
Storage capacity:	73.4GB
Data width:	16-bit
Buffer size:	8KB
Read/write head technology:	
Number of platters:	
Predictive failure monitor:	Yes
Buffer parity checking:	
Logical parms (heads, cyl, sectors):	
BER:	
Disk type:	
Cables:	
Max data transfer rate (burst):	
Sustained data transfer rate (low; high):	--
Drive interface type:	Ultra160 SCSI
Average access time:	7.89ms
Average data transfer rate:	--
Power consumption:	--
Seek time:	4.9ms
Platter RPM:	10000rpm
Other Information:	

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. -Nº 0476
Doc: 3696

Compatibility

Restrictions:	
Hardware prerequisites:	
System Units	
_ IBM Systems:	xSeries 220, xSeries 330, xSeries 232, xSeries 225, xSeries 230, xSeries 240, xSeries 250, xSeries 340, xSeries 342, xSeries 350, xSeries 360, xSeries 370, xSeries 440, xSeries 235, xSeries 255, xSeries 345
_ Non-IBM systems:	
Operating system requirements:	
Adapters:	

0475

13606
UA

Mounting kit etc.:	
Supported software:	
Product approvals/certifications4:	
Energy Star Compliant:	

Warranty [3]

Limited Warranty period and type:	-- --

Weight & Dimensions [6]

Weight:	1.3lbs
Travel weight:	--
Height:	1in
Width:	4in
Depth:	5.75in
Operating Temperature (C) (low; high):	
Relative Humidity (%) (low; high):	
Ship Information	--
Box 1	
Weight:	
Height:	--
Width:	--
Depth:	--
Box 2	--
Weight:	
Height:	--
Width:	--
Depth:	--
Special ship information:	

Important Legal Information

Doc 8

13605

Servers
Intel-based servers
Rack-optimized
Universal
Appliance
Storage
Accessories & upgrades
Services
Support
Certification
Education and training
News and awards
Library
HW/SW compatibility

IBM TotalStorage FC2-133 Host Bus Adapter

$1,485.00 IBM List Price

Model Name:

Part Number: **24P0960**

eserver

This host bus adapter option is a 64-bit, low-profile adapter that supports auto-sensing for 1Gbp or 2Gbps operations on point-to-point FC-AL-2 and switched fabric topologies with FC SCSI (FCP and IP protocols. It provides a full 133 MHz, PCI-X based solution incorporating improved storag interoperability, broad heterogenous host and NOS support. This option attaches FAStT Storage Servers to IBM eServer xSeries and other Intel-based servers.

Features & Benefits:

- Features integrated adapter management software
- Implements the latest 2Gb and PCI-X technologies
- Operates in any PCI or PCI-X slot
- Backward compatible with previous generations of FAStT host bus adapters

Technical Details

Compatibility

Restrictions:	
Supported software:	
Hardware prerequisites	
IBM systems:	xSeries 250, xSeries 300, xSeries 330, xSeries 340, xSeries 350, xSeries 370, xSeries 225, xSeries 235, xSeries 335, xSeries 345, xSeries 450
Non-IBM systems:	
Operating system requirements:	
Adapters:	
Mounting Kit etc.:	
Product Approvals	
Product approval/certifications4:	
Energy Star Compliant:	No

Technical Information

Warranty [3]

Limited Warranty period and type:	Three year Customer Carry-in Exchange

Weight & Dimentions [6]

Weight:	--
Travel weight:	--
Height:	--
	--
Width:	--
	--
Depth:	--
Operating Temperature (C) (low; high):	10; 32
Relative Humidity (%) (low; high):	8; 80
Ship Information	--
Box 1	
Weight:	
Height:	--
Width:	--
Depth:	--
Box 2	--
Weight:	

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0478
Doc: 3696

0477

Height:	--
Width:	--
Depth:	--
Special ship information:	

Other

Recommendation:

Important Legal Information

Doc 9

13603 A

Select a country

Select a language

Personal computing support

Search PC support

Warranty

Automated solutions

Online assistant

Submit a question

Discussion forums

Support phone list

Site feedback

Site help

Related links:

Business Partner support

IBM PC Institute

IBM Publications Center

Find a Business Partner

IBM Supports Microsoft Service Packs

NetXtreme 1000T Dual Port Ethernet Adapter - Overview

Applicable countries and regions

Prin

- Parts Information
- Files
- Publications

At a Glance
The new IBM NetXtreme 1000 T Dual Ethernet Adapter enables high performance network connections for the IBM eServer xSeries. Server performance is optimized to ensure that system I/O is not a bottleneck in high-performance networking applications.

- First Dual Port PCI-X 10/100/1000 Ethernet Adapter offering based on the latest Broadcom BCM5704 technology for xSeries
- Dual Port option provides dual Ethernet ports at up to 64-bit/133 MHz PCI-X performance in a single PCI/PCI-X slot to free up other slots in the system
- Hardware/software commonality with xSeries BCM570x on-board and adapter technologies
- Dual port architecture frees up one slot for constrained PCs xSeries servers
- 64-bit PCI and PCI-X support for faster transmissions with lower CPU utilization
- Low-profile capability (comes with both standard bracket and low profile bracket
- PCI hot-plug lets you remove/replace server network interface cards (NICs) without taking the server offline
- Automatic link aggregation and load balancing
- Smart Load Balancing allows heterogeneous failover
- Remote boot feature for remote system setup and maintenance
- PCI 2.2 Wake on LAN enables remote management

Warranty
3 year Limited - customer carry-in exchange

Packaging
You will receive one box containing the following items:

- NetXtreme 1000 T Dual Port Ethernet Adapter

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0480
Doc: 3696

Product dates

Worldwide

- Announce date: 15 Apr 2003
- Planned availability date: 30 Apr 2003

Technical specifications

Physical, environmental, and compatibility specifications as known at time of announcement

Weight:

- lbs: .167
- kg: .076

Height:

- inches: 6.6
- mm: 167.4

Width:

- inches: 2.54
- mm: 64.41

Depth:

- inches: 0.55
- mm: 13.86

Operating temperature

- Between 0 degrees celsius and 55 degrees celsius
- Between 32 degrees fahrenheit and 131 degrees fahrenheit

Relative humidity

- Operating: between 5% and 95%

Agency approvals

- FCC
- C-Tick
- VCCI
- UL
- Taiwan BSMI
- Korea MIC

ENERGY STAR-Compliant
No

Hardware Compatibility

The NetXtreme 1000 T Dual Port Ethernet Adapter is supported on the following IBM systems:

System Description	Machine Type	Model
xSeries 440	8687	All
xSeriex 380	8683	All
xSeries 360	8686	All
xSeries 350	8682	All
xSeries 345	8670	All
xSeries 335	8676, 8830	All
xSeries 330	8674, 8675	All
xSeries 305	8673	All
xSeries 255	8685	All

xSeries 250	8665	All
xSeries 230	8658	All
xSeries 225	8647	All
xSeries 220	8645	All
xSeries 205	8480	All
xSeries 235	8671	All
xSeries RXE-100	8684	All
IntelliStation E-Pro	6204, 6214, 6216, 6226	All
IntelliStation M-Pro	6219, 6229, 6849, 6850	All
IntelliStation Z-Pro	6221, 6894	All

Supported operating systems

- Microsoft Windows.NET
- Microsoft Windows 2000
- Microsoft Windows NT 4.0
- Microsoft Windows XP
- Novell NetWare
- SCO Open UNIX 8
- Linux

Compatibility
PCI-X is backwards compatible with conventional PCI products, which enables existing adapters to operate within a PCI environment. PCI-X adapters can be used in either PCI-X systems or a conventional PCI environment; however, the bus speed will default to the speed of the slowest adapter.

Applicable countries and regions

Worldwide

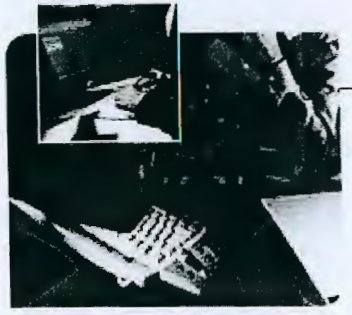
Back to top

Document id: MIGR-50474
Last modified: 2003-07-15

Microsoft Windows Server 2003

Windows Server Catalog

Home Page | Hardware



Featured Product

Digi PortServer TS 4 W

Digi International Inc.

Digi device and terminal servers provide Serial to Ethernet connectivity for any serial device.

Welcome to the Windows Server Catalog

Find the latest hardware designed especially for the Windows Server 2003 family

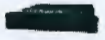
More Windows Server Catalog Links

- More Information about the Windows Server Catalog
- For Independent Hardware Vendors
- For Independent Software Vendors
- Hardware Compatibility List

Windows Catalog

Find products built for the Windows XP

More Featured Products



APC Smart-UPS Rack Mount 3000VA 2U (120V) for HP - APC3RB
American Power Conversion Corporation

MAXDATA PLATINUM Server 1210
MAXDATA AG

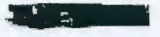
ProLiant BL40p 6/2.0GHz (4P)
Hewlett-Packard Company

ProLiant DL580 G2 6/1.6 GHz (1P)
Hewlett-Packard Company

APC Smart-UPS RM 1500VA 2U USB & Serial fro Dell (100V) Model DLA1500RMJ2U
American Power

ProLiant DL580 G2 6/2.0 GHz (1P)
Hewlett-Packard Company

APC Smart-UPS 1500VA USB & Serial for Dell (120V) Model DLA1500
American Power Conversion Corporation



ProLiant DL560 6/2.0GHz (4P), ProLiant DL560 6/1.9GHz (4P), ProLiant DL560 6/1.5GHz (4P)
Hewlett-Packard Company

Certified for Microsoft® Windows® Server 2003

Designed for Microsoft® Windows® Server 2003

Software
Look for the "Certified for Windows" logo for third-party tested applications that deliver a high-quality computing experience with the Windows Server 2003 family.

Hardware
Look for the "Designed for Windows" logo for products that deliver a high-quality computing experience with the Windows Server 2003 family.

operating system in the Windows Catalog

Conversion Corporation

The product pictures and descriptions are provided by the manufacturers of the products. The Windows Server Catalog is provided for informational purposes only and Microsoft makes no representations and warranties, either express, implied, or statutory, regarding the products, manufacturers, compatibility of the products available within, or the Windows Server Catalog. Information within the Windows Server Catalog, including products listed and compatibility data, is subject to change without notice. This program testing in no way guarantees compatibility between data, systems, or software and in no way replaces necessity of full testing of the products listed in the Windows Server Catalog. Acutal end user compatibility may vary. The inclusion of a product or manufacuturer does not imply endorsement of Microsoft of the product or manufacturer.

The links in this catalog will let you leave Microsoft's site. These sites are not under the control of Microsoft and Microsoft is not responsible for the contents of any linked site or any link contained in a linked site, or any changes or updates to such sites. Microsoft is not responsible for webcasting or any other form of transmission received from any linked site. Microsoft is providing these links to you only as a convenience, and the inclusion of any link does not imply endorsement of Microsoft of the site or the products contained therein.

Last Updated: 2003/7/21 12:19:59 PM

Contact Us | About the Windows Server Catalog | For Manufacturers

NEC

13598

Comprovação das Especificações Exigidas no Edital 050/2003

4.1.2. Servidores Intel tipo 2

23/07/03

0484

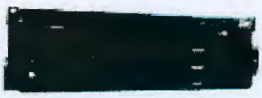
xSeries 360

Servers
Intel-based servers
Rack-optimized
Universal
Appliance
Storage
Accessories & upgrades
Services
Support
Certification
Education and training
News and awards
Library
HW/SW compatibility

$15,679.00 IBM List Price

Model Name: **86869RX**

Part Number: **86869RX**



Accessories & Upgrades

IIII

Technical Details

Architecture

Form factor:	Rack
Orientations allowed:	Horizontal
Bus type/architecture:	PCI
Slots x bays total (free):	6(6) x 5(3)
Expansion bus type:	

Multimedia

Media device type:	CD-ROM
Media speed:	24X Max
Media interface type:	EIDE
Media data transfer rate:	2500KBps
Media average access time:	110ms
Media transport type:	Front tray loading
Recordable:	No
Removable:	Yes
Audio features:	
Multimedia features:	

Expansion Options

Slots total (free) and type:	2(2) 64 Bit PCI-X 100MHz up to 133MHz, 4(4) 64-Bit PCI-X 66MHz
3.5" bays	3(3) SL, 1(0) SL
- accessible (free) and height:	
- not accessible (free) and height:	
5.25" bays	1(0) SL
- accessible (free) and height:	
- not accessible (free) and height:	
Plug and play support:	
Parallel ports (type):	
Serial ports (type):	1 (RS485), 3 (USB)
Expansion ports:	Video, Keyboard, Mouse, RJ-45

Graphics Subsystems

Graphics Chip Set Model & Mfr.:	S3 Savage4 LT
Graphics Data Width:	128-bit
Graphics Type:	--
Default Memory Address:	
Video RAM Std (MB):	8MB
Video RAM Max (MB):	8MB
Video RAM Type:	SDRAM
Graphics Bus Interface:	PCI
Resolution Max (Video RAM Std), NI:	1024x768
Resolution Max (Video RAM Max), NI:	1600x1200
Colors Max (Video RAM Std):	16777216
Colors Max (Video RAM Max):	65536
Graphics features:	DDC-2B compliant

Hard Disk

Hard Disk 1:

Number of installed hard disks:	
Hard disk size[1]:	--
Hard disk controller:	Integrated Ultra160 SCSI
Hard disk type:	Open bay

Total possible device types:	
Max internal hard disk capacity:	220.2GB
Average seek time:	--
Average latency:	--
RAID levels supported:	
Hot swappable drive bays:	3
Cache size:	--
Number of platters:	
Platter RPM:	
Burst transfer rate:	
Sustained data trans rate (low; high):	--
Additional storage features:	
Optional hard disk available:	

Memory

Memory (RAM) std/max:	2GB / 16GB
RAM speed:	100MHz
Optional RAM configuration:	
RAM type:	PC1600 DDR SDRAM
RAM slots total (available):	8 DIMM (4 DIMM)

Networking

Network interface:	Ethernet-Integrated
Network speed:	100Mbps, 10Mbps
Network features:	

Power Management

Power supply:	370Watts
Power supply type:	110-220 volt Hot Swap Redundant Auto Restart 2 Std.
Power supply additional:	
Heat emissions:	361W
Sound emissions:	63dB
Cooling system:	6 fans
UPS:	
Power management features4:	

System Management

Adapter:	Remote Supervisor Adapter
Software:	Power-on password Privileged access password Selectable boot Unattended start-up
Features:	32-bit Data/Address Width; Ethernet and Fast Ethernet Compatible Networks; Network Speed of 100Mbps/10Mbps; PCI Interface Bus; RJ11 Connectors; RJ45 Connectors; RS 232 Connectors; RS 485 Connectors; RS-232 Connectors

Processor

Processor (CPU)2:	Intel Xeon MP
Processor internal clock speed2:	2.00GHz
Front Side Bus:	400MHz
Processor manufacturer:	Intel
Math co-processor:	
L1 internal CPU cache:	--
L2 internal CPU cache:	512KB
L2 external CPU cache std:	--
L2 external CPU cache type:	
Upgradable processor:	
Processor upgrade options:	
Processor upgrade method:	Add processor option
BIOS type:	Flash BIOS
Number of processors std/max:	2/4
SMP capable (multiple processors):	Yes
Multi-processor bus (slots/speed):	--
L3 cache:	2MB

Security

AssetCare features:	IBM Director System Management Features and Tools
Security features:	Power-on password Privileged access password Selectable boot Unattended start-up
VPD support:	

Software

Tested operating systems:	Caldera Open UNIX 8.0.0, Caldera OpenLinux

Operating system provided:	Server 3.1.1, Microsoft Windows NT 4.0 Server, Microsoft Windows 2000 Advanced Server, Microsoft Windows 2000 Server, Novell Netware 6.0, Novell NetWare 5.1, Open Server 5.0.6a, Red Hat Linux 7.3, SuSE 7.2, VMware ESX Server v1.5
Communication/networking applications:	
Device drivers/utilities:	
Multimedia applications:	
Productivity applications:	
Other applications provided:	

Standard Features

Pointing device type:	
Standard diskette size:	3.5" 1.44/1.2/0.72MB
Keyboard type standard:	
I20 Compliant:	
Product approvals/certifications4:	NOM 019; TUV-GS; UL-1950; BSMI (Taiwan); C-Tick Mark (AS/NZS 3548 Class A); CE Mark (EN55022 Class A, EN60950, and EN50082-1); CISPR-22 Class A; CSA C22.2 No. 950; FCC Class A - Part 15; ICES-003 Class A (Canada); IEC-60950 Certificate/Report; IEC-950; Japan VCCI, Class A

Warranty

Limited Warranty period and type:	Three year parts and labor Onsite

Weight & Dimentions

Weight:	70lbs
Travel weight:	--
Height:	5.25in
Height with stand:	--
Width:	17.4in
Width with stand:	--
Depth:	27.6in
Operating Temperature (C) (low; high):	10; 35
Relative Humidity (%) (low; high):	8; 80

Other

Recommendation:	

▶ Important Legal Information

73.4GB 10K Ultra 160 SCSI Hot Swap SL HDD

Technical Detai
·Compatibility
·Warranty
·Weight & Dimen

Accessories & upgrades
News & awards
Library
Software
Solutions
Compatibility
Warranty info

$639.00 IBM List Price

Part Number: **06P5756**

@server

1111

Take advantage of IBM's latest SCSI hard disk drive (HDDs) technology with optional high- speed, high-density 10,000rpm Ultra160 SCSI slim-line HDDs in hot-swap xSeries servers and IntelliStation workstations. These 3.5-inch, hot-swap HDD options can double xSeries storage capacities for those who need high-speed data storage for demanding enterprise server and workstation applications. These HDDs store a tremendous amount of data in a slim-line form factor. This optimizes the storage capacities of supported servers, while providing excellent storage subsystem performance.

Features & Benefits:

• Ÿ 10,000rpm HDDs -- Deliver solid reliability and excellent performance
Ÿ Ultra160 SCSI interface -- wide bandwidth for streaming data transfers
Ÿ Available in hot-swap version:
- Converged hot-swap drive tray -- Supports xSeries servers,
Netfinity servers, IntelliStation workstations, and EXP storage units with hot-swap bays
Ÿ Predictive Failure Analysis (PFA) -- Can alert you of a problem before it occurs

Technical Details

Characteristics

Interface bus:	SCSI
Form factor:	SL
Storage capacity:	73.4GB
Data width:	16-bit
Buffer size:	8KB
Read/write head technology:	
Number of platters:	
Predictive failure monitor:	Yes
Buffer parity checking:	
Logical parms (heads, cyl, sectors):	
BER:	
Disk type:	
Cables:	
Max data transfer rate (burst):	
Sustained data transfer rate (low; high):	--
Drive interface type:	Ultra160 SCSI
Average access time:	7.89ms
Average data transfer rate:	--
Power consumption:	--
Seek time:	4.9ms
Platter RPM:	10000rpm
Other Information:	

Compatibility

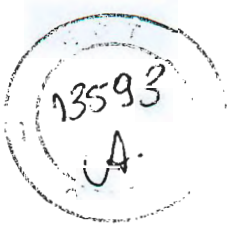
Restrictions:	
Hardware prerequisites:	
System Units	
_ IBM Systems:	xSeries 220, xSeries 330, xSeries 232, xSeries 225, xSeries 230, xSeries 240, xSeries 250, xSeries 340, xSeries 342, xSeries 350, xSeries 360, xSeries 370, xSeries 440, xSeries 235, xSeries 255, xSeries 345
_ Non-IBM systems:	
Operating system requirements:	
Adapters:	
Mounting kit etc.:	
Supported software:	
Product approvals/certifications4:	
Energy Star Compliant:	

Warranty [3]

Limited Warranty period and type:	-- --

Weight & Dimensions [6]

Weight:	1.3lbs
Travel weight:	--
Height:	1in
Width:	4in
Depth:	5.75in
Operating Temperature (C) (low; high):	
Relative Humidity (%) (low; high):	
Ship Information	--
Box 1	
Weight:	
Height:	--
Width:	--
Depth:	--
Box 2	--
Weight:	
Height:	--
Width:	--
Depth:	--
Special ship information:	



▶ Important Legal Information

IBM TotalStorage FC2-133 Host Bus Adapter

Technical Detai
·Compatibility
·Technical Inform
·Warranty
·Weights & Dime
·Other

$1,485.00 IBM List Price

Model Name:

Part Number: **24P0960**

eserver

IIII

This host bus adapter option is a 64-bit, low-profile adapter that supports auto-sensing for 1Gbps or 2Gbps operations on point-to-point FC-AL-2 and switched fabric topologies with FC SCSI (FCP) and IP protocols. It provides a full 133 MHz, PCI-X based solution incorporating improved storage interoperability, broad heterogenous host and NOS support. This option attaches FAStT Storage Servers to IBM eServer xSeries and other Intel-based servers.

Features & Benefits:

- Features integrated adapter management software
- Implements the latest 2Gb and PCI-X technologies
- Operates in any PCI or PCI-X slot
- Backward compatible with previous generations of FAStT host bus adapters

Technical Details

Compatibility

Restrictions:	
Supported software:	
Hardware prerequisites IBM systems:	xSeries 250, xSeries 300, xSeries 330, xSeries 340, xSeries 350, xSeries 370, xSeries 225, xSeries 235, xSeries 335, xSeries 345, xSeries 450
Non-IBM systems:	
Operating system requirements:	
Adapters:	
Mounting Kit etc.:	
Product Approvals	
Product approval/certifications4:	
Energy Star Compliant:	No

Technical Information

Warranty [3]

Limited Warranty period and type:	Three year Customer Carry-in Exchange

Weight & Dimentions [6]

Weight:	--
Travel weight:	--
Height:	--
	--
Width:	--
	--
Depth:	--
Operating Temperature (C) (low; high):	10; 32
Relative Humidity (%) (low; high):	8; 80
Ship Information	--
Box 1	
Weight:	
Height:	--
Width:	--
Depth:	--
Box 2	--
Weight:	
Height:	--
Width:	--
Depth:	--

Special ship information:

Other
| Recommendation:

▶ Important Legal Information

NetXtreme 1000T Dual Port Ethernet Adapter - Overview

Applicable countries and regions

Printable version

- Parts Information
- Files
- Publications

At a Glance
The new IBM NetXtreme 1000 T Dual Ethernet Adapter enables high performance network connections for the IBM eServer xSeries. Server performance is optimized to ensure that system I/O is not a bottleneck in high-performance networking applications.

- First Dual Port PCI-X 10/100/1000 Ethernet Adapter offering based on the latest Broadcom BCM5704 technology for xSeries
- Dual Port option provides dual Ethernet ports at up to 64-bit/133 MHz PCI-X performance in a single PCI/PCI-X slot to free up other slots in the system
- Hardware/software commonality with xSeries BCM570x on-board and adapter technologies
- Dual port architecture frees up one slot for constrained PCs xSeries servers
- 64-bit PCI and PCI-X support for faster transmissions with lower CPU utilization
- Low-profile capability (comes with both standard bracket and low profile bracket
- PCI hot-plug lets you remove/replace server network interface cards (NICs) without taking the server offline
- Automatic link aggregation and load balancing
- Smart Load Balancing allows heterogeneous failover
- Remote boot feature for remote system setup and maintenance
- PCI 2.2 Wake on LAN enables remote management

Warranty
3 year Limited - customer carry-in exchange

Packaging
You will receive one box containing the following items:

- NetXtreme 1000 T Dual Port Ethernet Adapter

Product dates

Worldwide

- Announce date: 15 Apr 2003
- Planned availability date: 30 Apr 2003

Technical specifications

Physical, environmental, and compatibility specifications as known at time of announcement

Weight:

- lbs: .167
- kg: .076

Height:

- inches: 6.6
- mm: 167.4

Width:

- inches: 2.54
- mm: 64.41

Depth:

- inches: 0.55
- mm: 13.86

Operating temperature

- Between 0 degrees celsius and 55 degrees celsius
- Between 32 degrees fahrenheit and 131 degrees fahrenheit

Relative humidity

- Operating: between 5% and 95%

Agency approvals

- FCC
- C-Tick
- VCCI
- UL
- Taiwan BSMI
- Korea MIC

ENERGY STAR-Compliant
No

Hardware Compatibility

The NetXtreme 1000 T Dual Port Ethernet Adapter is supported on the following IBM systems:

System Description	Machine Type	Model
xSeries 440	8687	All
xSeriex 380	8683	All
xSeries 360	8686	All
xSeries 350	8682	All
xSeries 345	8670	All
xSeries 335	8676, 8830	All
xSeries 330	8674, 8675	All
xSeries 305	8673	All
xSeries 255	8685	All
xSeries 250	8665	All
xSeries 230	8658	All
xSeries 225	8647	All
xSeries 220	8645	All
xSeries 205	8480	All
xSeries 235	8671	All
xSeries RXE-100	8684	All

IntelliStation E-Pro	6204, 6214, 6216, 6226	All
IntelliStation M-Pro	6219, 6229, 6849, 6850	All
IntelliStation Z-Pro	6221, 6894	All

Supported operating systems

- Microsoft Windows.NET
- Microsoft Windows 2000
- Microsoft Windows NT 4.0
- Microsoft Windows XP
- Novell NetWare
- SCO Open UNIX 8
- Linux

Compatibility
PCI-X is backwards compatible with conventional PCI products, which enables existing adapters to operate within a PCI environment. PCI-X adapters can be used in either PCI-X systems or a conventional PCI environment; however, the bus speed will default to the speed of the slowest adapter.

Applicable countries and regions

Worldwide

Back to top

Document id: MIGR-50474
Last modified: 2003-07-15

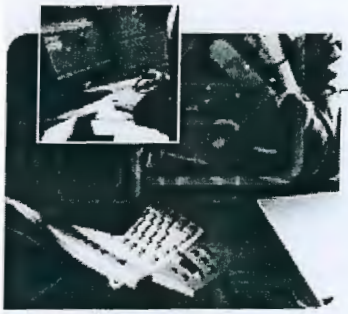
Windows Server 2003

Windows Server Catalog

Microsoft

1358 7 A

Home Page | Hardware



Featured Product

APC Smart-UPS RM 750VA 1U USB & Serial (230V) Model SUA750RMI1U

American Power Conversion Corporation

APC Smart-UPS offers performance power protection for servers, networks and workstations.

Certified for Microsoft® Windows® Server 2003

Designed for Microsoft® Windows® Server 2003

Software
Look for the "Certified for Windows" logo for third-party tested applications that deliver a high-quality computing experience with the Windows Server 2003 family.

Hardware
Look for the "Designed for Windows" logo for products that deliver a high-quality computing experience with the Windows Server 2003 family.

Welcome to the Windows Server Catalog

Find the latest hardware designed especially for the Windows Server 2003 family

More Windows Server Catalog Links

- More Information about the Windows Server Catalog
- For Independent Hardware Vendors
- For Independent Software Vendors
- Hardware Compatibility List

Windows Catalog

Find products built for the Windows XP operating system in the Windows Catalog

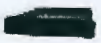
More Featured Products

SiiRUS Classic DP VI Infrastructure Server
PCS Industries Limited

CyberPower Power 525VA, 120V, Model CPS525AVR
Cyber Power System Inc.

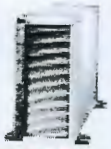
SiiRUS Classic DP VI Business Server
PCS Industries Limited

APC Smart-UPS Rack Mount 3000VA 2U (120V) for HP - APC3RB
American Power Conversion Corporation



APC Smart-UPS 3000VA (230V) for HP - APC3IB
American Power Conversion Corporation

ProLiant DL580 G2 6/1.6 GHz (1P)
Hewlett-Packard Company



MAXDATA PLATINUM Server 1210
MAXDATA AG

ProLiant BL40p 6/2.0GHz (4P)
Hewlett-Packard Company

Last Updated: 2003/7/21 12:19:59 PM

Contact Us | About the Windows Server Catalog | For Manufacturers

13586
VA

NEC

13585
A.

Comprovação das Especificações Exigidas no Edital 050/2003

4.1.3. Servidores Intel tipo 3

United States

Select a country

- Servers
- **Intel processor-based servers**
- Rack-optimized
- Universal
- High-performance scalable
- Blade servers
- Storage
- Systems Management
- Accessories & upgrades
- Services
- Support
- Certification
- Education and training
- News and awards
- Literature
- HW/SW compatibility
- Solutions

Shopping help

- Warranty info
- Shop by part number
- View cart
- Open saved carts
- Estimate shipping
- Estimate leasing
- Order status
- Returns policy
- Shopping guarantee

Related links:

- Home / home office
- Small & Medium Business
- Government
- Education

xSeries 235

IBM Web Price
$3,269.00*
$116.00 /mo. for 36 mos. SuccessLease® for Small Business***
Availability: **Within 2 weeks****

Customize

Monitor sold separately

xSeries 235 overview | View all models | More info | Visual tour

→ Help me decide → Call me now

General	
Model name	86718AX
Description	xSeries 235
IBM Web Price*	$3,269.00
SuccessLease® for Small Business***	$116.00/mo. for 36 mos.
Architecture	
Form factor	Tower
Orientations allowed	Vertical
PCMCIA support	Yes
Slots x bays total (free)	6(6) x 10(8)
Processor	
Processor (CPU)	Intel® Xeon™
Processor internal clock speed	3.06 GHz
Planar clock speed	533 MHz
SMP processors std	1
SMP processors max	2
Processor manufacturer	Intel®
Processor upgrade options	Faster Xeon processor
SMP capable (multiple processors)	Yes
BIOS type	Flash
Memory	
Memory (RAM) std	512 MB
RAM speed	266MHz
Optional RAM configuration	128:256:512:1024:2048MB DIMMS (must be installed in sets of 2)
RAM type	PC2100 DDR SDRAM
RAM slots total	6 DIMM
RAM slots available	4 DIMM
Hard disk	
Number of installed hard disks	0
Hard disk size	0 GB
RAID levels supported	1
Hot swappable drive bays	6/3
Hard disk controller	Integrated Dual Channel Ultra320 SCSI
Hard disk type	Open bay
Max Hard Drive Capacity	1314 GB
Graphics subsystem	

Graphics type	2D
Graphics chipset	ATI Rage XL
Graphics data width	64
Video RAM type	SDRAM
Video RAM std	8 MB
Video RAM max	8 MB
Max resolution (with std video RAM)	1600 X 1200
Max resolution (with max video RAM)	1600x1200
Max colors (with std video RAM)	16777216
Graphics bus interface	PCI

Multimedia

CD-ROM speed	48X Max
CD-ROM interface type	EIDE
CD-ROM data transfer rate	4000 KBps
CD-ROM average access time	85 ms
CD-ROM transport type	Front tray loading

Communications

Network interface	Gigabit Ethernet- Integrated
Network speed	10Mbps, 100Mbps, 1000Mbps

Standard features

Standard diskette size	3.5" 1.44/1.2/0.72 MB

Power management

Power supply	660
Power supply type	Hot Swap Redundant Auto Start/Sensing 2 Std.
Heat emissions	121 W
Sound emissions	65 dB
Cooling system	6 fans

Dimensions

Weight	101 lbs
Height	17.31 inches
Width	8.5 inches
Depth	27.6 inches

Security

Security features	Mechanical locks, Power-on password, Remote-control password, Selectable boot, Unattended startup

Warranty

Limited Warranty period	Three year
Type of Service	Onsite Repair

Expansion options

Slots total (free) and type	1(1) 32 Bit PCI 33 MHz, 2(2) 64 Bit Active PCI-X 133 MHz Hot Swap, 3(3) 64 Bit PCI-X 100MHz
3.5 inch bays - accessible (free) and height	1(0) SL, 6(6) SL
5.25 inch bays - accessible (free) and height	3(2) SL
Plug and Play support	Yes
Serial ports (type)	2(9-pin 16550A NS compatible), 3(USB)
Expansion ports	Keyboard port, Mouse port, Parallel, RJ-45, Video

Monitor

Monitor Included	No

Customize

Still can't find what you're looking for?

Select one of the following

You can choose one of the options above, or call us at **1-888-SHOP-IBM**.

*Price does not include tax or expedited shipping and is subject to change without notice. Reseller prices may vary. IBM does not warrant non-IBM products. PCs shown here, except for Servers and Network Stations, ship with an operating system. All offers subject to availability. IBM reserves the right to alter product offerings and specifications at any time without notice. IBM is not responsible for photographic or typographic errors.

** An estimated ship date will be included with your order confirmation e-mail. Availability does not determine when your order will ship since inventory status may change before your order is final (following the receipt of any credit or payment authorization) as other orders are processed. "In stock" indicates we currently have at least one of the item in stock. Orders are normally held until all the products on the order are in inventory. "Within 2 weeks" indicates that the product should be available in inventory within 2 weeks. "Within 2-4 Weeks" indicates that the product should be available in inventory in 2-4 weeks. To obtain the latest information about the availability of a specific part number, please call 1-888-SHOP-IBM.

*** SuccessLease® for Small Business is offered and administered in the US and Canada by third party providers of business financing who are approved by IBM Global Financing. All terms are provided by third party providers of business financing who are approved by IBM Global Financing.; example of monthly lease payments based on a 36 month term, prespecified purchase option at end of lease, to qualified business customers installing in the US and are for planning purposes only, actual payments may vary. A documentation fee and first month payment due at signing. Any taxes are additional. Other terms and financing structures are available. $750 minimum lease order applies.
SuccessLease® for Small Business

Important Legal Information

Doc 2

TPC Transaction Processing Performance Council

The TPC defines transaction processing and database benchmarks and delivers trusted results to the industry.

13581 A

- Home
- Results
- Benchmarks
  - TPC-C
  - **- Results**
  - - Description
  - - FAQ
  - TPC-H
  - TPC-R
  - TPC-W
  - Obsolete
  - - TPC-A
  - - TPC-B
  - - TPC-D
- Technical Articles
- Related Links
- What's New
- About the TPC
- Who We Are
- Member Login

TPC-C Result Highlights

IBM eServer xSeries 235 1P c/s

Benchmark Stats

Result ID:	103071001
Result Status:	In Review
TPC-C Rev:	5.1
Report Date:	07/10/03

System Information

Total System Cost	46,539 US $
TPC-C Throughput	18,936
Price/Performance	2.46 US $
Availability Date	07/10/03
Database Manager	Microsoft SQL Server 2000 Standard Ed.
Operating System	Microsoft Windows Server 2003 Standard Edition
Transaction Monitor	Microsoft COM+

Server Information

CPU:	Intel Xeon DP 3.06GHz
# of CPUs:	1
Cluster:	N

Client Information

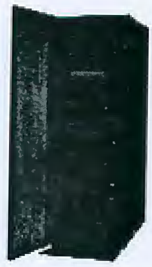
# of clients:	1
CPU:	Intel Xeon DP 2.4GHz
CPUs per client:	1

- Executive Summary (242 KB)
- Full Disclosure Report (1492 KB)

top

Home Results Benchmarks Technical Articles Related Links What's New
About the TPC Who We Are Privacy Policy About Pricing

NetBAY42 Enterprise Rack Cabinet



IBM Web Price
$2,649.00*

Availability: **In stock****

Add to cart

- Servers
- **Intel processor-based servers**
- Rack-optimized
- Universal
- High-performance scalable
- Blade servers
- Storage
- Systems Management
- Accessories & upgrades
- Services
- Support
- Certification
- Education and training
- News and awards
- Literature
- HW/SW compatibility
- Solutions

Shopping help
- Warranty info
- Shop by part number
- View cart
- Open saved carts
- Estimate shipping
- Estimate leasing
- Order status
- Returns policy
- Shopping guarantee

Related links:
- Home / home office
- Small & Medium Business
- Government
- Education

New NetBAY rack cabinets provide a comprehensive selection of rugged, rack solutions tailored for "deep" servers and high-density installations. Cabinet provides 42U of rack space with depth capacity to support "deep" servers up to 28 inches. All models feature a perforated-steel front door to optimize cooling while maintaining security by lock and key. These NetBAY rack cabinets support all current rack-mountable IBM eServer xSeries and Netfinity servers.

Features and Benefits:

Includes side panels and a stabilizer kit
Robust design allows shipping with preconfigured servers
Perforated front door provides improved air flow for a fan-free environment
Lockable front and rear doors maximize security
Provides the most room of all NetBAY racks for cable management

General	
Model name	930842S
Description	NetBAY42 Enterprise Rack Cabinet
IBM Web Price*	$2,649.00
Compatibility	
Restrictions	When servicing or sliding devices out of the NetBAY42 ER or EX, it is required that the front stabilizer plate be used in accordance with the instructions included in the installation/safety publications.
Hardware prerequisites (System unit)	Netfinity 4500R, Netfinity 4500R Rack Mounted models, Netfinity 5100, Netfinity 5100 Rack Mounted models, Netfinity 5000, Netfinity 5000 Rack Mounted models, Netfinity 5500, Netfinity 5500 M10, Netfinity 5500 M10 Rack Mounted models, Netfinity 5500 M20,
Hardware prerequisites (Mounting kit etc.)	Cable requirements are dependent upon the devices installed in the NetBAY42 ER cabinets.
Product approvals/certifications	CSA C22.2 No. 950 Third Edition, IEC-950/EN 60950 Second Edition, UL-1950 Third Edition
Characteristics	
Space	42
Type of cabinet	Type A 19" (EIA standard 310-D)
Memory	
Memory (RAM) std	--
Power management	
Sound emissions	
Dimensions	

Weight	575 lbs
Height	79.5 inches
Width	25.5 inches
Depth	43.3 inches

Security

Security features	Lockable front/rear door, Lockable side panels

Warranty

Limited Warranty period	Three year
Type of Service	Customer Carry-in

Add to cart

*Price does not include tax or expedited shipping and is subject to change without notice. Reseller prices may vary. IBM does not warrant non-IBM products. PCs shown here, except for Servers and Network Stations, ship with an operating system. All offers subject to availability. IBM reserves the right to alter product offerings and specifications at any time without notice. IBM is not responsible for photographic or typographic errors.

** An estimated ship date will be included with your order confirmation e-mail. Availability does not determine when your order will ship since inventory status may change before your order is final (following the receipt of any credit or payment authorization) as other orders are processed. "In stock" indicates we currently have at least one of the item in stock. Orders are normally held until all the products on the order are in inventory. "Within 2 weeks" indicates that the product should be available in inventory within 2 weeks. "Within 2-4 Weeks" indicates that the product should be available in inventory in 2-4 weeks. To obtain the latest information about the availability of a specific part number, please call 1-888-SHOP-IBM.

Important Legal Information

13579 A.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0504
Doc: 3696

Doc 4

← Servers

Intel processor-based servers

Rack-optimized

Universal

High-performance scalable

Blade servers

Storage

Systems Management

Accessories & upgrades

Services

Support

Certification

Education and training

News and awards

Literature

HW/SW compatibility

Solutions

Shopping help

Warranty info

Shop by part number

View cart

Open saved carts

Estimate shipping

Estimate leasing

Order status

Returns policy

Shopping guarantee

Related links:

Home / home office

Small & Medium Business

Government

Education

5UX24D Tower to Rack Kit III

eserver

IBM Web Price
$455.00*

Availability: **Within 2 weeks****

Add to cart

This 5Ux24D tower-to-rack option is designed for use with the IBM eServer xSeries 235 and 232 servers. It contains all the necessary hardware to install either of these servers in a standard 19-inch EIA rack cabinet, such as one of the NetBAY Enterprise racks or the NetBAY Standard racks.

Features and Benefits:

Redeployment enablement: as your needs change this kit allows you great flexibility in the placement of the x235
Comes complete with all necessary hardware

General	
Model name	59P4211
Description	5UX24D Tower to Rack Kit III
IBM Web Price*	$455.00
Memory	
Memory (RAM) std	--
Power management	
Sound emissions	
Warranty	
Limited Warranty period	Three year
Type of Service	Customer Carry-in Exchange

Add to cart

*Price does not include tax or expedited shipping and is subject to change without notice. Reseller prices may vary. IBM does not warrant non-IBM products. PCs shown here, except for Servers and Network Stations, ship with an operating system. All offers subject to availability. IBM reserves the right to alter product offerings and specifications at any time without notice. IBM is not responsible for photographic or typographic errors.

** An estimated ship date will be included with your order confirmation e-mail. Availability does not determine when your order will ship since inventory status may change before your order is final (following the receipt of any credit or payment authorization) as other orders are processed. "In stock" indicates we currently have at least one of the item in stock. Orders are normally held until all the products on the order are in inventory. "Within 2 weeks" indicates that the product should be available in inventory within 2 weeks. "Within 2-4 Weeks" indicates that the product should be available in inventory in 2-4 weeks. To obtain the latest information about the availability of a specific part number, please call 1-888-SHOP-IBM.

Important Legal Information

Doc 6

United States

13517

73.4GB 10K Ultra 160 SCSI Hot Swap SL HDD

$639.00 IBM List Price

Part Number: **06P5756**

eserver

Take advantage of IBM's latest SCSI hard disk drive (HDDs) technology with optional high- spee high-density 10,000rpm Ultra160 SCSI slim-line HDDs in hot-swap xSeries servers and IntelliStation workstations. These 3.5-inch, hot-swap HDD options can double xSeries storage capacities for those who need high-speed data storage for demanding enterprise server and workstation applications. These HDDs store a tremendous amount of data in a slim-line form factor. This optimizes the storage capacities of supported servers, while providing excellent storage subsystem performance.

Features & Benefits:

• Ÿ 10,000rpm HDDs -- Deliver solid reliability and excellent performance
Ÿ Ultra160 SCSI interface -- wide bandwidth for streaming data transfers
Ÿ Available in hot-swap version:
- Converged hot-swap drive tray -- Supports xSeries servers, Netfinity servers, IntelliStation workstations, and EXP storage units with hot-swap bays
Ÿ Predictive Failure Analysis (PFA) -- Can alert you of a problem before it occurs

Technical Details

Characteristics

Interface bus:	SCSI
Form factor:	SL
Storage capacity:	73.4GB
Data width:	16-bit
Buffer size:	8KB
Read/write head technology:	
Number of platters:	
Predictive failure monitor:	Yes
Buffer parity checking:	
Logical parms (heads, cyl, sectors):	
BER:	
Disk type:	
Cables:	
Max data transfer rate (burst):	
Sustained data transfer rate (low; high):	--
Drive interface type:	Ultra160 SCSI
Average access time:	7.89ms
Average data transfer rate:	--
Power consumption:	--
Seek time:	4.9ms
Platter RPM:	10000rpm
Other Information:	

Compatibility

Restrictions:	
Hardware prerequisites:	
System Units	
_ IBM Systems:	xSeries 220, xSeries 330, xSeries 232, xSeries 225, xSeries 230, xSeries 240, xSeries 250, xSeries 340, xSeries 342, xSeries 350, xSeries 360, xSeries 370, xSeries 440, xSeries 235, xSeries 255, xSeries 345
_ Non-IBM systems:	
Operating system requirements:	
Adapters:	

Mounting kit etc.:	
Supported software:	
Product approvals/certifications4:	
Energy Star Compliant:	

Warranty [3]

Limited Warranty period and type:	-- --

Weight & Dimensions [6]

Weight:	1.3lbs
Travel weight:	--
Height:	1in
Width:	4in
Depth:	5.75in
Operating Temperature (C) (low; high):	
Relative Humidity (%) (low; high):	
Ship Information	--
Box 1	
Weight:	
Height:	--
Width:	--
Depth:	--
Box 2	--
Weight:	
Height:	--
Width:	--
Depth:	--
Special ship information:	

Important Legal Information

13576
A

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0507
Doc: 3696

← Servers

Intel processor-based servers

Rack-optimized

Universal

High-performance scalable

Blade servers

Storage

Systems Management

Accessories & upgrades

Services

Support

Certification

Education and training

News and awards

Literature

HW/SW compatibility

Solutions

Shopping help

Warranty info

Shop by part number

View cart

Open saved carts

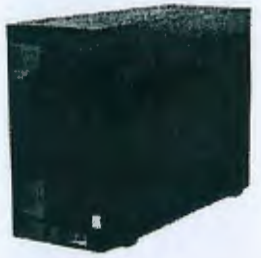
Estimate shipping

Estimate leasing

xSeries 235

IBM Web Price
$3,269.00*
$116.00 /mo. for 36 mos. SuccessLease® for Small Business***
Availability: **Within 2 weeks****

Customize



Monitor sold separately

xSeries 235 overview | View all models | More info | Visual tour

IBM server

→ Help me decide → Call me now

General	
Model name	86718AX
Description	xSeries 235
IBM Web Price*	$3,269.00
SuccessLease® for Small Business***	$116.00/mo. for 36 mos.

Architecture	
Form factor	Tower
Orientations allowed	Vertical
PCMCIA support	Yes
Slots x bays total (free)	6(6) x 10(8)

Processor	
Processor (CPU)	Intel® Xeon™
Processor internal clock speed	3.06 GHz
Planar clock speed	533 MHz
SMP processors std	
SMP processors max	
Processor manufacturer	Intel®
Processor upgrade options	Faster Xeon processor

Order status
Returns policy
Shopping guarantee

Related links:

Home / home office
Small & Medium Business
Government
Education

Processor upgrade options	Faster Xeon processor
SMP capable (multiple processors)	Yes
BIOS type	Flash

Memory

Memory (RAM) std	512 MB
RAM speed	266MHz
Optional RAM configuration	128:256:512:1024:2048MB DIMMS (must be installed in sets of 2)
RAM type	PC2100 DDR SDRAM
RAM slots total	6 DIMM
RAM slots available	4 DIMM

Hard disk

Number of installed hard disks	0
Hard disk size	0 GB
RAID levels supported	1
Hot swappable drive bays	6/3
Hard disk controller	Integrated Dual Channel Ultra320 SCSI
Hard disk type	Open bay
Max Hard Drive Capacity	1314 GB

Graphics subsystem

Graphics type	2D
Graphics chipset	ATI Rage XL
Graphics data width	64
Video RAM type	SDRAM
Video RAM std	8 MB
Video RAM max	8 MB
Max resolution (with std video RAM)	1600 X 1200
Max resolution (with max video RAM)	1600x1200
Max colors (with std video RAM)	16777216
Graphics bus interface	PCI

Multimedia

CD-ROM speed	48X Max
CD-ROM interface type	EIDE
CD-ROM data transfer rate	4000 KBps
CD-ROM average access time	85 ms
CD-ROM transport type	Front tray loading

Communications

Network interface	Gigabit Ethernet- Integrated

E-mail this page

Hot deals

→ Clearance corner

Volume discounts

Call me now

TeleWeb hotline:
1-866-426-0472

Network speed	10Mbps, 100Mbps, 1000Mbps
Standard features	
Standard diskette size	3.5" 1.44/1.2/0.72 MB
Power management	
Power supply	660
Power supply type	Hot Swap Redundant Auto Start/Sensing 2 Std.
Heat emissions	121 W
Sound emissions	65 dB
Cooling system	6 fans
Dimensions	
Weight	101 lbs
Height	17.31 inches
Width	8.5 inches
Depth	27.6 inches
Security	
Security features	Mechanical locks, Power-on password, Remote-control password, Selectable boot, Unattended startup
Warranty	
Limited Warranty period	Three year
Type of Service	Onsite Repair
Expansion options	
Slots total (free) and type	1(1) 32 Bit PCI 33 MHz, 2(2) 64 Bit Active PCI-X 133 MHz Hot Swap, 3(3) 64 Bit PCI-X 100MHz
3.5 inch bays - accessible (free) and height	1(0) SL, 6(6) SL
5.25 inch bays - accessible (free) and height	3(2) SL
Plug and Play support	Yes
Serial ports (type)	2(9-pin 16550A NS compatible), 3 (USB)
Expansion ports	Keyboard port, Mouse port, Parallel, RJ-45, Video
Monitor	
Monitor Included	No

Still can't find what you're looking for?

Select one of the following

You can choose one of the options above, or call us at **1-888-SHOP-IBM**.

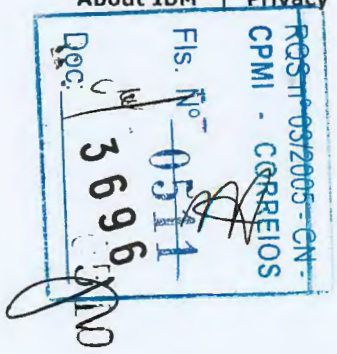
*Price does not include tax or expedited shipping and is subject to change without notice. Reseller prices may vary. IBM does not warrant non-IBM products. PCs shown here, except for Servers and Network Stations, ship with an operating system. All offers subject to availability. IBM reserves the right to alter product offerings and specifications at any time without notice. IBM is not responsible for photographic or typographic errors.

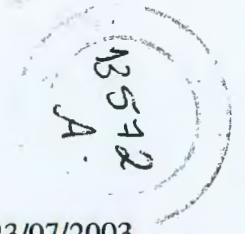
** An estimated ship date will be included with your order confirmation e-mail. Availability does not determine when your order will ship since inventory status may change before your order is final (following the receipt of any credit or payment authorization) as other orders are processed. "In stock" indicates we currently have at least one of the item in stock. Orders are normally held until all the products on the order are in inventory. "Within 2 weeks" indicates that the product should be available in inventory within 2 weeks. "Within 2-4 Weeks" indicates that the product should be available in inventory in 2-4 weeks. To obtain the latest information about the availability of a specific part number, please call 1-888-SHOP-IBM.

*** SuccessLease® for Small Business is offered and administered in the US and Canada by third party providers of business financing who are approved by IBM Global Financing. All terms are provided by third party providers of business financing who are approved by IBM Global Financing.; example of monthly lease payments based on a 36 month term, prespecified purchase option at end of lease, to qualified business customers installing in the US and are for planning purposes only, actual payments may vary. A documentation fee and first month payment due at signing. Any taxes are additional. Other terms and financing structures are available. $750 minimum lease order applies.
SuccessLease® for Small Business

Important Legal Information

About IBM | **Privacy** | **Legal** | **Contact**





Doc 7

1354

Select a country

Select a language

Personal computing support

Search PC support

Warranty

Automated solutions

Online assistant

Submit a question

Discussion forums

Support phone list

Site feedback

Site help

Related links:

Business Partner support

IBM PC Institute

IBM Publications Center

Find a Business Partner

IBM Supports Microsoft Service Packs

NetXtreme 1000T Dual Port Ethernet Adapter - Overview

Applicable countries and regions

Prin

- Parts Information
- Files
- Publications

At a Glance
The new IBM NetXtreme 1000 T Dual Ethernet Adapter enables high performance network connections for the IBM eServer xSeries. Server performance is optimized to ensure that system I/O is not a bottleneck in high-performance networking applications.

- First Dual Port PCI-X 10/100/1000 Ethernet Adapter offering based on the latest Broadcom BCM5704 technology for xSeries
- Dual Port option provides dual Ethernet ports at up to 64-bit/133 MHz PCI-X performance in a single PCI/PCI-X slot to free up other slots in the system
- Hardware/software commonality with xSeries BCM570x on-board and adapter technologies
- Dual port architecture frees up one slot for constrained PCs xSeries servers
- 64-bit PCI and PCI-X support for faster transmissions with lower CPU utilization
- Low-profile capability (comes with both standard bracket and low profile bracket
- PCI hot-plug lets you remove/replace server network interface cards (NICs) without taking the server offline
- Automatic link aggregation and load balancing
- Smart Load Balancing allows heterogeneous failover
- Remote boot feature for remote system setup and maintenance
- PCI 2.2 Wake on LAN enables remote management

Warranty
3 year Limited - customer carry-in exchange

Packaging
You will receive one box containing the following items:

- NetXtreme 1000 T Dual Port Ethernet Adapter

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0512
Doc: 3696

Product dates

Worldwide

- Announce date: 15 Apr 2003
- Planned availability date: 30 Apr 2003

Technical specifications

Physical, environmental, and compatibility specifications as known at time of announcement

3511

13570
A.

Weight:

- lbs: .167
- kg: .076

Height:

- inches: 6.6
- mm: 167.4

Width:

- inches: 2.54
- mm: 64.41

Depth:

- inches: 0.55
- mm: 13.86

Operating temperature

- Between 0 degrees celsius and 55 degrees celsius
- Between 32 degrees fahrenheit and 131 degrees fahrenheit

Relative humidity

- Operating: between 5% and 95%

Agency approvals

- FCC
- C-Tick
- VCCI
- UL
- Taiwan BSMI
- Korea MIC

ENERGY STAR-Compliant
No

Hardware Compatibility

The NetXtreme 1000 T Dual Port Ethernet Adapter is supported on the following IBM systems:

System Description	Machine Type	Model
xSeries 440	8687	All
xSeriex 380	8683	All
xSeries 360	8686	All
xSeries 350	8682	All
xSeries 345	8670	All
xSeries 335	8676, 8830	All
xSeries 330	8674, 8675	All
xSeries 305	8673	All
xSeries 255	8685	All

xSeries 250	8665	All
xSeries 230	8658	All
xSeries 225	8647	All
xSeries 220	8645	All
xSeries 205	8480	All
xSeries 235	8671	All
xSeries RXE-100	8684	All
IntelliStation E-Pro	6204, 6214, 6216, 6226	All
IntelliStation M-Pro	6219, 6229, 6849, 6850	All
IntelliStation Z-Pro	6221, 6894	All

Supported operating systems

- Microsoft Windows.NET
- Microsoft Windows 2000
- Microsoft Windows NT 4.0
- Microsoft Windows XP
- Novell NetWare
- SCO Open UNIX 8
- Linux

Compatibility
PCI-X is backwards compatible with conventional PCI products, which enables existing adapters to operate within a PCI environment. PCI-X adapters can be used in either PCI-X systems or a conventional PCI environment; however, the bus speed will default to the speed of the slowest adapter.

Applicable countries and regions

Worldwide

Back to top

Document id: MIGR-50474
Last modified: 2003-07-15

Microsoft Windows Server 2003

Windows Server Catalog

Microsoft

Home Page | Hardware

Featured Product

ProLiant DL560 6/2.0GHz (4P), ProLiant DL560 6/1.9GHz (4P), ProLiant DL560 6/1.5GHz (4P)
Hewlett-Packard Company

The ProLiant DL560 is the first 4-way server in an ultra-dense 2U form factor.

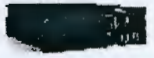
More Featured Products

APC Smart-UPS 3000VA (230V) for HP - APC3IB
American Power Conversion Corporation

SiiRUS Classic DP VI Business Server
PCS Industries Limited

MAXDATA PLATINUM Server 1210
MAXDATA AG

Digi PortServer TS 4 W
Digi International Inc.



ProLiant DL580 G2 6/1.6 GHz (1P)
Hewlett-Packard Company

APC Smart-UPS RM 1500VA 2U USB & Serial fro Dell (100V) Model DLA1500RMJ2U
American Power Conversion Corporation

APC Smart-UPS Rack Mount 3000VA 2U (120V) for HP - APC3RB
American Power Conversion Corporation

CyberPower Power 525VA, 120V, Model CPS525AVR
Cyber Power System Inc.

Welcome to the Windows Server Catalog

Find the latest hardware designed especially for the Windows Server 2003 family

More Windows Server Catalog Links

- More Information about the Windows Server Catalog
- For Independent Hardware Vendors
- For Independent Software Vendors
- Hardware Compatibility List

Windows Catalog

Find products built for the Windows XP

Certified for Microsoft® Windows® Server 2003

Designed for Microsoft® Windows® Server 2003

Software
Look for the "Certified for Windows" logo for third-party tested applications that deliver a high-quality computing experience with the Windows Server 2003 family.

Hardware
Look for the "Designed for Windows" logo for products that deliver a high-quality computing experience with the Windows Server 2003 family.

operating system in
the Windows Catalog

The product pictures and descriptions are provided by the manufacturers of the products. The Windows Server Catalog is provided for informational purposes only and Microsoft makes no representations and warranties, either express, implied, or statutory, regarding the products, manufacturers, compatibility of the products available within, or the Windows Server Catalog. Information within the Windows Server Catalog, including products listed and compatibility data, is subject to change without notice. This program testing in no way guarantees compatibility between data, systems, or software and in no way replaces necessity of full testing of the products listed in the Windows Server Catalog. Acutal end user compatibility may vary. The inclusion of a product or manufacuturer does not imply endorsement of Microsoft of the product or manufacturer.

The links in this catalog will let you leave Microsoft's site. These sites are not under the control of Microsoft and Microsoft is not responsible for the contents of any linked site or any link contained in a linked site, or any changes or updates to such sites. Microsoft is not responsible for webcasting or any other form of transmission received from any linked site. Microsoft is providing these links to you only as a convenience, and the inclusion of any link does not imply endorsement of Microsoft of the site or the products contained therein.

Last Updated: 2003/7/21 12:19:59 PM

Contact Us | About the Windows Server Catalog | For Manufacturers

NEC

13566 LA

Comprovação das Especificações Exigidas no Edital 050/2003

4.2. Servidores RISC

23/07/03

NEC

1356 5

Comprovação das Especificações Exigidas no Edital 050/2003

4.2.1. Servidores RISC tipo 1

23/07/03

						delivery	2250069	3750	3.10
						stock_level	2250061	1187	2.57
152	431539	250699	3472	18.5%	<0.01	new_order	22516201	9069	3.07
						payment	22516186	3218	2.85
						order_status	2251612	358	2.70
						delivery	2251615	3727	2.90
						stock_level	2251618	1211	2.85

SPECjbb2000 Version: [SPECjbb2000 1.02, December 14, 2001]

UltraSPARC PROCESSORS

UltraSPARC®III Processor

UltraSPARC III Processor

» Features, Functions & Benefits
» Specifications
» Detailed View
» FAQs
» In the Spotlight

Related:

» Throughput Computing
» In the News
» Documentation
» Innovation
» Technology Resources

See Also:

» N1
» Solaris Operating Environment
» Sun ONE Studio Compiler Collection

The 3rd generation 64-bit UltraSPARC® III Cu processor is Sun's award-winning workstation and server processor, designed with advanced RAS features, 100% binary compatibility and unparalleled scalability, enabling Sun systems to deliver industry-leading real-world application performance that makes the net work.

MICROPROCESSOR REPORT ANALYST'S Best Server/ Workstation Processor UltraSPARC III CHOICE

Contact Me

The demands of enterprise and high performance computing mandate highly reliable and scalable 64-bit systems. UltraSPARC III based systems offer customers investment protection already built in with CPU features including copper interconnect for improved signaling and best-in-class power consumption, shortened 90 nanometer gate length for faster performance, mixed speeds in a chassis, thermal and electrical footprint preservation enabling simple upgrade paths and industry-leading RAS. UltraSPARC III based systems are optimized to meet, or exceed, customer expectations providing real-world performance and reduced Total Cost of Ownership (TCO).

→ **Product Bulletin PDF** → **UltraSPARC Family Brochure PDF**

Key Features and Benefits

Key Applications:
Mission-critical enterprise, HPC, and compute-intensive workstation applications.

Key Specifications:

- Architecture: 64-bit SPARC® V9 with VIS Instruction Set
- 4-way Superscalar
- 14-stage, Non-Stalling Pipeline

- Integrated Memory Controller
- L1 Caches : Integrated instruction (32KB) & data (64KB)
- L2 Cache : Up to 8MB external (on-chip controller and address tags)
- Advanced RAS features
- MP Scalability: Over 1000 CPUs/system
- System Bus: Sun Fireplane Interconnect at 150MHz
- Clock frequencies: 900MHz - 1.2GHz

Key Benefits:
Optimal multiprocessor performance, high availability and scalability for mission-critical and high-performance systems in the network.

Key Products:
The UltraSPARC® III processor is an integral part of Sun systems which range from technical workstations to mainframe-class servers. All Sun systems run seamlessly on the SPARC® and Solaris platform, protecting your investment in system hardware while providing flexibility and scalability for your business needs. Key products powered by UltraSPARC III technology include: Sun Fire High-End Servers, Sun Fire Midframe Servers, Sun Fire Workgroup Servers, and Sun Blade 2000 Performance Workstations.

Find out more about other members of the UltraSPARC processor family:

- UltraSPARC IIIi
- UltraSPARC IIi
- UltraSPARC IIe

1. This page meets my need. disagree ○ ○ ○ ○ ○ ○ ○ agree

2. This page was easy to find. disagree ○ ○ ○ ○ ○ ○ ○ agree

SPECjbb2000

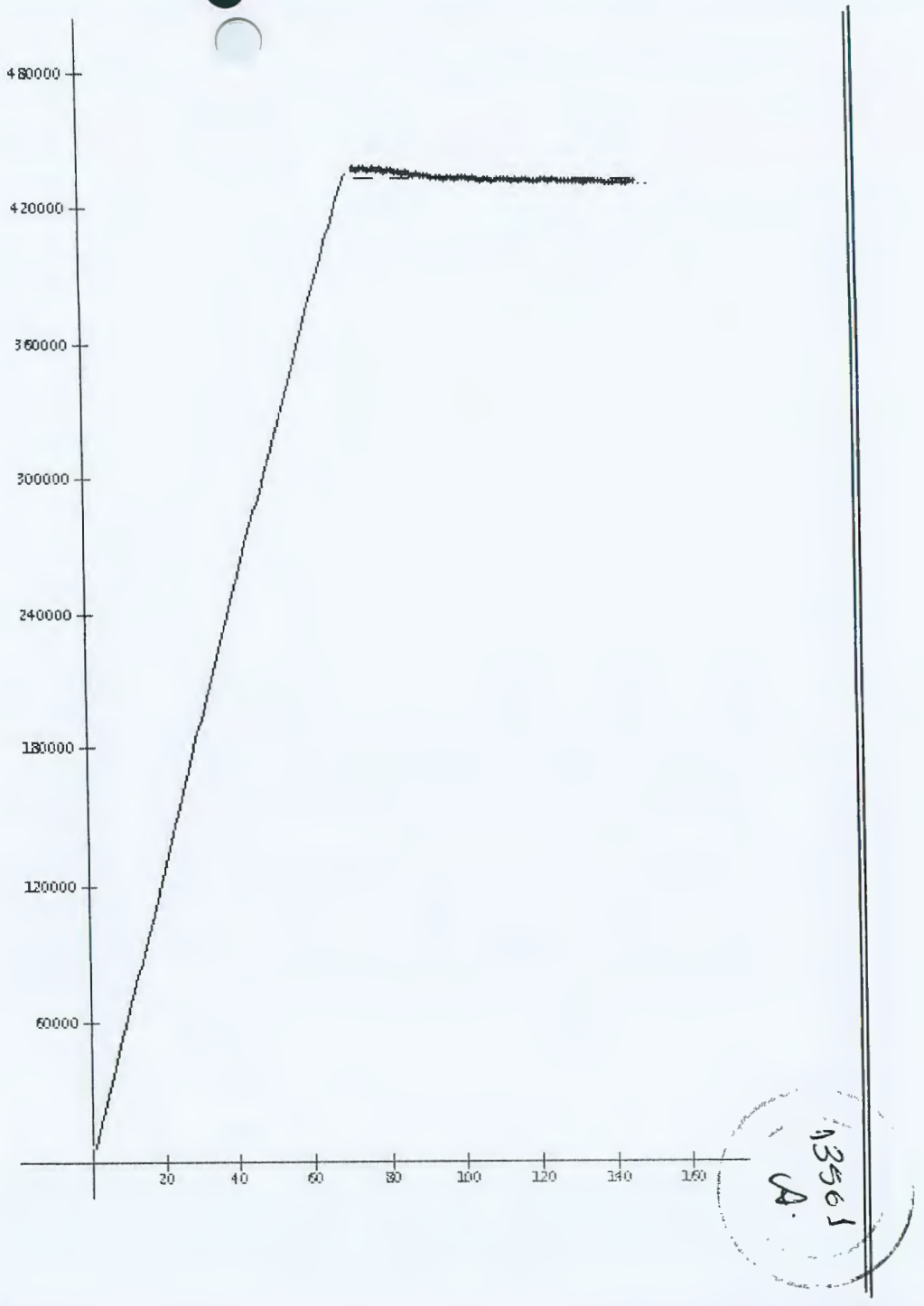
SPECjbb2000 = 433166 ops/s

Sun Microsystems, Inc. Sun Fire 15K

Sun Microsystems, Inc. HotSpot 64-Bit Server VM on Solaris/SPARC, version 1.4.0_01

Warehouses	Ops/s	Incl. in metric
1	6164	
2	12412	
3	18681	
4	24626	
5	30851	
6	37013	
7	43556	
8	49560	
9	56036	
10	61636	
11	68395	
12	73992	
13	80015	
14	86711	
15	93366	
16	99443	
17	105236	
18	110818	
19	118154	
20	124474	
21	129982	
22	136383	
23	142578	
24	148687	
25	155088	

26	161582
27	167592
28	173535
29	180166
30	187009
31	193057
32	199225
33	205330
34	211280
35	217367
36	223655
37	230620
38	236290
39	242523
40	248485
41	254863
42	261020
43	268037
44	274362
45	279701
46	285690
47	291568
48	298333
49	304486
50	310423
51	316176
52	322823
53	328259
54	334740



55	341364	
56	346317	
57	353857	
58	359057	
59	365598	
60	371215	
61	377941	
62	382899	
63	389591	
64	395399	
65	400890	
66	407336	
67	412030	
68	417047	
69	423860	
70	428707	
71	433599	
72	436717	
73	436428	
74	437534	*
75	436143	*
76	437219	*
77	437089	*
78	436712	*
79	437185	*
80	436265	*
81	437064	*
82	436071	*
83	436479	*

84	436144	*
85	435393	*
86	435699	*
87	435007	*
88	435357	*
89	434565	*
90	434448	*
91	435112	*
92	434269	*
93	434172	*
94	434100	*
95	433548	*
96	433530	*
97	432968	*
98	432906	*
99	433169	*
100	433431	*
101	432476	*
102	433058	*
103	432999	*
104	433053	*
105	432648	*
106	432910	*
107	432423	*
108	431838	*
109	432335	*
110	432470	*
111	431956	*
112	432266	*

113	432379	*
114	432567	*
115	432758	*
116	432084	*
117	432650	*
118	431677	*
119	432194	*
120	432111	*
121	431944	*
122	432075	*
123	431878	*
124	432317	*
125	432337	*
126	431955	*
127	432242	*
128	431665	*
129	432037	*
130	431422	*
131	431697	*
132	431588	*
133	431672	*
134	431721	*
135	431147	*
136	431341	*
137	432043	*
138	431690	*
139	431814	*
140	431771	*
141	431299	*

142	431284	*
143	431111	*
144	431606	*
145	431205	*
146	431136	*
147	431605	*
148	431383	*
149	430903	
150	431436	
151	431243	
152	431539	
SPECjbb2000	**(from 74 to 148)**	**433166 ops/s**

SPEC license # 6	**Tested by:** Sun Microsystems, Inc.	**Test date:** Apr 9, 2002

Hardware	
Hardware Vendor	Sun Microsystems, Inc.
Vendor URL	http://www.sun.com
Model	Sun Fire 15K
Processor	UltraSPARC-III Cu
MHz	1050
# of Procs	72
Memory (MB)	294912
Primary cache	32KB(I)+64KB(D)
Secondary cache	8MB(I+D) off chip
Other cache	

Software	
Software Vendor	Sun Microsystems, Inc.
Vendor URL	http://www.sun.com
Java Precompiler Version	
Java Precompiler Command Line	
Java Precompiler Way Of Excluding Classes	
JVM Version	HotSpot 64-Bit Server VM on Solaris/SPARC, version 1.4.0_01
JVM Command Line	java -server -d64 -Xbatch -Xss256k -XX:+UseISM -XX:+AggressiveHeap -classpath ./jbb.jar:./jbb_no_precompile.jar:./check.jar:./reporter.jar spec.jbb.JBBmain -propfile SPECjbb.props
JVM Initial Heap Memory (MB)	258048
JVM Maximum Heap Memory (MB)	258048

Filesystem	UFS
Disks	1 x 18GB SCSI (classes); 1 x 18GB SCSI (OS)
Other hardware	

JVM CLASSPATH	./jbb.jar: ./jbb_no_precompile.jar: ./check.jar: ./reporter.jar
JVM BOOTCLASSPATH	/var/jbb/j2re1.4.0_01/lib/rt.jar: /var/jbb/j2re1.4.0_01/lib/i18n.jar: /var/jbb/j2re1.4.0_01/lib/sunrsasign.jar: /var/jbb/j2re1.4.0_01/lib/jsse.jar: /var/jbb/j2re1.4.0_01/lib/jce.jar: /var/jbb/j2re1.4.0_01/lib/charsets.jar: /var/jbb/j2re1.4.0_01/classes
OS Version	Solaris 8 update 7
System state	normal
Other software	

Test Information	
Tested by	Sun Microsystems, Inc.
SPEC license #	6
Test location	SAE; Beaverton, Oregon
Test date	Apr 9, 2002
H/w available	Aug-2002
JVM available	Jun-2002
OS available	Feb-2002
Other s/w available	

Tuning

Operating system tunings

- /etc/system:
  - autoup=345600
  - tune_t_fsflushr=345600
  - set shmsys:shminfo_shmmax=0xffffffffffffffff
  - set shmsys:shminfo_shmseg=0x800
-
- environment:
  - LD_LIBRARY_PATH=/usr/lib/lwp

Notes

Command line options are described at http://java.sun.com/docs/hotspot

Details of Runs

		Total heap (MB)				Time (in seconds)

Warehouses	Thrput	Size	Used	Thread spread %	% > 120s	transaction type	Count	total	max
1	6164	250699	33.1	<0.01%	<0.01	new_order	321599	68.9	<0.01
						payment	321599	23.9	.066
						order_status	32160	2.68	<0.01
						delivery	32159	9.26	<0.01
						stock_level	32161	1.00	.091
2	12412	250699	60.5	.731%	<0.01	new_order	647578	139	<0.01
						payment	647578	47.6	<0.01
						order_status	64758	5.19	<0.01
						delivery	64757	19.8	<0.01
						stock_level	64759	18.9	<0.01
3	18681	250699	75.2	1.55%	<0.01	new_order	974765	207	<0.01
						payment	974772	72.1	<0.01
						order_status	97476	8.33	<0.01
						delivery	97475	29.5	<0.01
						stock_level	97477	28.3	<0.01
4	24626	250699	111	1.27%	<0.01	new_order	1284917	276	<0.01
						payment	1284925	96.7	<0.01
						order_status	128493	11.0	<0.01
						delivery	128493	38.7	<0.01
						stock_level	128491	37.2	<0.01
5	30851	250699	117	2.71%	<0.01	new_order	1609692	343	<0.01
						payment	1609688	123	<0.01
						order_status	160969	13.8	<0.01
						delivery	160970	48.6	<0.01
						stock_level	160967	45.8	<0.01
6	37013	250699	163	2.82%	<0.01	new_order	1931223	414	<0.01
						payment	1931207	145	<0.01
						order_status	193123	16.3	<0.01

						delivery	193121	58.2	<0.01
						stock_level	193120	55.4	<0.01
7	43556	250699	160	4.13%	<0.01	new_order	2272622	480	<0.01
						payment	2272620	170	<0.01
						order_status	227262	19.1	<0.01
						delivery	227259	69.1	<0.01
						stock_level	227261	66.0	<0.01
8	49560	250699	217	3.86%	<0.01	new_order	2585903	551	<0.01
						payment	2585883	195	<0.01
						order_status	258587	21.4	<0.01
						delivery	258590	78.0	<0.01
						stock_level	258589	74.5	<0.01
9	56036	250699	200	3.23%	<0.01	new_order	2923819	620	<0.01
						payment	2923818	219	<0.01
						order_status	292385	24.6	<0.01
						delivery	292385	87.5	<0.01
						stock_level	292384	82.9	<0.01
10	61636	250699	264	5.89%	<0.01	new_order	3216052	688	<0.01
						payment	3216060	243	.020
						order_status	321609	26.8	<0.01
						delivery	321604	97.8	<0.01
						stock_level	321607	93.8	<0.01
11	68395	250699	243	5.84%	<0.01	new_order	3568480	755	<0.01
						payment	3568479	271	<0.01
						order_status	356851	29.8	<0.01
						delivery	356848	108	<0.01
						stock_level	356849	102	<0.01
12	73992	250699	315	4.05%	<0.01	new_order	3860579	823	<0.01
						payment	3860580	295	<0.01

						order_status	386055	32.4	<0.01
						delivery	386055	118	<0.01
						stock_level	386061	110	<0.01
13	80015	250699	285	4.98%	<0.01	new_order	4174815	895	<0.01
						payment	4174821	317	<0.01
						order_status	417481	35.0	<0.01
						delivery	417481	127	<0.01
						stock_level	417481	120	<0.01
14	86711	250699	366	6.10%	<0.01	new_order	4524347	962	<0.01
						payment	4524348	343	<0.01
						order_status	452435	37.8	<0.01
						delivery	452434	137	<0.01
						stock_level	452435	130	<0.01
15	93366	250699	329	5.49%	<0.01	new_order	4871514	1028	<0.01
						payment	4871505	369	<0.01
						order_status	487153	41.1	<0.01
						delivery	487152	148	<0.01
						stock_level	487150	139	<0.01
16	99443	250699	421	5.47%	<0.01	new_order	5188694	1097	<0.01
						payment	5188686	392	<0.01
						order_status	518865	43.2	<0.01
						delivery	518871	158	<0.01
						stock_level	518863	149	<0.01
17	105236	250699	371	4.01%	<0.01	new_order	5491028	1171	.011
						payment	5491030	414	<0.01
						order_status	549103	45.8	<0.01
						delivery	549101	167	<0.01
						stock_level	549103	158	<0.01
18	110818	250699	469	3.04%	<0.01	new_order	5782048	1242	<0.01

						payment	5782042	438	<0.01
						order_status	578200	48.4	<0.01
						delivery	578204	174	<0.01
						stock_level	578202	168	<0.01
19	118154	250699	414	5.86%	.010	new_order	6165164	1307	<0.01
						payment	6165177	465	<0.01
						order_status	616517	51.4	<0.01
						delivery	616518	185	<0.01
						stock_level	616518	175	<0.01
20	124474	250699	526	6.69%	<0.01	new_order	6494900	1372	<0.01
						payment	6494910	491	<0.01
						order_status	649493	53.8	<0.01
						delivery	649489	197	<0.01
						stock_level	649490	185	<0.01
21	129982	250699	450	4.27%	<0.01	new_order	6781921	1443	.026
						payment	6781918	514	<0.01
						order_status	678193	56.5	<0.01
						delivery	678191	205	<0.01
						stock_level	678190	196	<0.01
22	136383	250699	571	8.80%	<0.01	new_order	7115959	1512	<0.01
						payment	7115951	537	<0.01
						order_status	711594	59.3	<0.01
						delivery	711600	216	<0.01
						stock_level	711585	205	<0.01
23	142578	250699	495	9.38%	<0.01	new_order	7439079	1582	<0.01
						payment	7439075	560	<0.01
						order_status	743908	61.1	<0.01
						delivery	743910	227	<0.01
						stock_level	743909	215	<0.01

24	148687	250699	621	20%	<0.01	new_order	7757797	1650	<0.01
						payment	7757781	585	<0.01
						order_status	775781	64.6	<0.01
						delivery	775780	237	<0.01
						stock_level	775783	223	<0.01
25	155088	250699	539	13.0%	<0.01	new_order	8091678	1713	<0.01
						payment	8091667	612	<0.01
						order_status	809164	67.4	<0.01
						delivery	809164	249	<0.01
						stock_level	809168	233	<0.01
26	161582	250699	676	8.22%	.010	new_order	8431223	1788	<0.01
						payment	8431225	633	<0.01
						order_status	843118	69.1	<0.01
						delivery	843119	257	<0.01
						stock_level	843119	243	<0.01
27	167592	250699	578	6.95%	<0.01	new_order	8744731	1857	<0.01
						payment	8744733	659	<0.01
						order_status	874473	72.8	<0.01
						delivery	874474	267	<0.01
						stock_level	874471	249	<0.01
28	173535	250699	719	5.31%	<0.01	new_order	9054666	1931	<0.01
						payment	9054687	680	<0.01
						order_status	905465	75.0	<0.01
						delivery	905463	275	<0.01
						stock_level	905462	260	<0.01
29	180166	250699	624	9.93%	<0.01	new_order	9400559	1996	<0.01
						payment	9400571	706	<0.01
						order_status	940063	77.8	<0.01
						delivery	940053	286	<0.01

						stock_level	940059	270	<0.01
30	187009	250699	778	7.52%	<0.01	new_order	9757829	2061	<0.01
						payment	9757823	732	<0.01
						order_status	975782	80.4	<0.01
						delivery	975783	297	<0.01
						stock_level	975782	279	<0.01
31	193057	250699	665	7.88%	<0.01	new_order	10073413	2128	<0.01
						payment	10073390	756	<0.01
						order_status	1007336	84.0	<0.01
						delivery	1007337	306	<0.01
						stock_level	1007340	291	<0.01
32	199225	250699	825	8.23%	<0.01	new_order	10395227	2203	<0.01
						payment	10395210	779	<0.01
						order_status	1039524	86.1	<0.01
						delivery	1039515	316	<0.01
						stock_level	1039515	297	<0.01
33	205330	250699	707	9.34%	<0.01	new_order	10713743	2270	<0.01
						payment	10713733	802	<0.01
						order_status	1071377	88.8	<0.01
						delivery	1071371	326	<0.01
						stock_level	1071370	307	<0.01
34	211280	250699	881	8.56%	<0.01	new_order	11023775	2349	<0.01
						payment	11023756	823	<0.01
						order_status	1102379	89.6	<0.01
						delivery	1102377	336	<0.01
						stock_level	1102379	314	<0.01
35	217367	250699	749	6.50%	<0.01	new_order	11341382	2411	<0.01
						payment	11341394	852	<0.01
						order_status	1134133	94.8	<0.01

						delivery	1134140	345	<0.01
						stock_level	1134135	323	<0.01
36	223655	250699	932	7.96%	<0.01	new_order	11669262	2470	<0.01
						payment	11669263	881	<0.01
						order_status	1166925	96.8	<0.01
						delivery	1166931	358	<0.01
						stock_level	1166931	335	<0.01
37	230620	250699	791	6.60%	.010	new_order	12033570	2539	<0.01
						payment	12033543	905	<0.01
						order_status	1203360	99.9	<0.01
						delivery	1203354	368	<0.01
						stock_level	1203356	345	<0.01
38	236290	250699	983	7.39%	<0.01	new_order	12329209	2610	<0.01
						payment	12329211	930	<0.01
						order_status	1232923	102	<0.01
						delivery	1232924	377	<0.01
						stock_level	1232918	354	<0.01
39	242523	250699	834	6.14%	<0.01	new_order	12653989	2679	<0.01
						payment	12654022	951	<0.01
						order_status	1265406	105	<0.01
						delivery	1265405	387	<0.01
						stock_level	1265398	365	<0.01
40	248485	250699	1032	6.25%	.010	new_order	12965711	2752	<0.01
						payment	12965748	975	<0.01
						order_status	1296565	107	<0.01
						delivery	1296575	397	<0.01
						stock_level	1296574	371	<0.01
41	254863	250699	879	6.20%	<0.01	new_order	13298206	2813	<0.01
						payment	13298211	1003	<0.01

						order_status	1329822	110	<0.01
						delivery	1329820	410	<0.01
						stock_level	1329821	382	<0.01
42	261020	250699	1085	6.23%	<0.01	new_order	13619369	2888	<0.01
						payment	13619347	1025	<0.01
						order_status	1361937	112	<0.01
						delivery	1361936	417	<0.01
						stock_level	1361939	391	<0.01
43	268037	250699	921	6.41%	<0.01	new_order	13984892	2957	<0.01
						payment	13984884	1051	<0.01
						order_status	1398488	115	<0.01
						delivery	1398483	426	<0.01
						stock_level	1398489	400	<0.01
44	274362	250699	1143	5.97%	<0.01	new_order	14314897	3021	<0.01
						payment	14314903	1075	<0.01
						order_status	1431490	118	<0.01
						delivery	1431484	438	<0.01
						stock_level	1431499	411	<0.01
45	279701	250699	960	7.29%	<0.01	new_order	14594456	3098	<0.01
						payment	14594447	1097	<0.01
						order_status	1459441	121	<0.01
						delivery	1459447	447	<0.01
						stock_level	1459445	415	<0.01
46	285690	250699	1194	5.94%	<0.01	new_order	14906907	3159	<0.01
						payment	14906905	1125	<0.01
						order_status	1490692	124	<0.01
						delivery	1490690	458	.380
						stock_level	1490698	428	<0.01
47	291568	250699	1006	6.80%	<0.01	new_order	15212593	3230	<0.01

						payment	15212608	1147	<0.01
						order_status	1521262	126	<0.01
						delivery	1521255	468	<0.01
						stock_level	1521261	438	<0.01
48	298333	250699	1241	6.78%	.010	new_order	15566737	3295	.018
						payment	15566769	1171	.018
						order_status	1556677	128	<0.01
						delivery	1556674	480	.015
						stock_level	1556673	451	<0.01
49	304486	250699	1048	5.97%	.010	new_order	15887793	3362	<0.01
						payment	15887804	1196	<0.01
						order_status	1588781	131	<0.01
						delivery	1588780	492	<0.01
						stock_level	1588775	457	<0.01
50	310423	250699	1294	7.25%	<0.01	new_order	16197458	3431	<0.01
						payment	16197457	1222	<0.01
						order_status	1619744	133	<0.01
						delivery	1619747	499	<0.01
						stock_level	1619753	470	<0.01
51	316176	250699	1084	5.93%	<0.01	new_order	16497655	3509	<0.01
						payment	16497607	1243	<0.01
						order_status	1649757	136	<0.01
						delivery	1649770	508	<0.01
						stock_level	1649765	474	<0.01
52	322823	250699	1339	5.41%	<0.01	new_order	16843929	3571	<0.01
						payment	16843901	1270	<0.01
						order_status	1684387	140	<0.01
						delivery	1684402	520	<0.01
						stock_level	1684390	485	<0.01

53	328259	250699	1133	[illegible]5%	<0.01	new_order	17127282	3646	<0.01
						payment	17127297	1291	<0.01
						order_status	1712732	142	<0.01
						delivery	1712731	530	<0.01
						stock_level	1712736	492	<0.01
54	334740	250699	1403	6.09%	.010	new_order	17466420	3706	<0.01
						payment	17466431	1318	<0.01
						order_status	1746634	145	<0.01
						delivery	1746648	540	<0.01
						stock_level	1746644	507	<0.01
55	341364	250699	1175	5.37%	<0.01	new_order	17811910	3773	<0.01
						payment	17811911	1344	<0.01
						order_status	1781183	148	<0.01
						delivery	1781184	550	<0.01
						stock_level	1781194	514	<0.01
56	346317	250699	1446	6.16%	.010	new_order	18070511	3851	<0.01
						payment	18070512	1367	<0.01
						order_status	1807052	149	<0.01
						delivery	1807050	560	<0.01
						stock_level	1807053	521	<0.01
57	353857	250699	1212	6.14%	.010	new_order	18463947	3911	<0.01
						payment	18463928	1393	<0.01
						order_status	1846393	153	<0.01
						delivery	1846383	572	<0.01
						stock_level	1846395	533	<0.01
58	359057	250699	1493	7.69%	<0.01	new_order	18734019	3985	<0.01
						payment	18733997	1414	<0.01
						order_status	1873409	155	<0.01
						delivery	1873402	581	<0.01

						stock_level	1873404	540	<0.01
59	365598	250699	1260	7.60%	<0.01	new_order	19075294	4057	<0.01
						payment	19075295	1437	<0.01
						order_status	1907532	158	<0.01
						delivery	1907533	590	<0.01
						stock_level	1907526	551	<0.01
60	371215	250699	1548	6.41%	<0.01	new_order	19368850	4118	<0.01
						payment	19368839	1465	<0.01
						order_status	1936882	160	<0.01
						delivery	1936889	602	<0.01
						stock_level	1936879	560	<0.01
61	377941	250699	1304	5.03%	<0.01	new_order	19720151	4185	<0.01
						payment	19720158	1488	<0.01
						order_status	1972013	163	<0.01
						delivery	1972018	612	<0.01
						stock_level	1972008	572	<0.01
62	382899	250699	1596	6.43%	.010	new_order	19979356	4261	<0.01
						payment	19979348	1512	<0.01
						order_status	1997931	166	<0.01
						delivery	1997935	624	<0.01
						stock_level	1997941	575	<0.01
63	389591	250699	1343	6.62%	<0.01	new_order	20328192	4325	<0.01
						payment	20328167	1537	<0.01
						order_status	2032821	168	<0.01
						delivery	2032818	633	.380
						stock_level	2032817	589	<0.01
64	395399	250699	1653	7.02%	<0.01	new_order	20630883	4395	<0.01
						payment	20630883	1560	<0.01
						order_status	2063090	171	<0.01

						delivery	2063077	642	<0.01
						stock_level	2063089	599	<0.01
65	400890	250699	1387	6.67%	<0.01	new_order	20917043	4476	<0.01
						payment	20917065	1581	<0.01
						order_status	2091708	173	<0.01
						delivery	2091701	650	<0.01
						stock_level	2091709	606	<0.01
66	407336	250699	1715	6.97%	<0.01	new_order	21253929	4533	.040
						payment	21253944	1612	.010
						order_status	2125388	176	<0.01
						delivery	2125385	662	.389
						stock_level	2125392	614	<0.01
67	412030	250699	1430	9.66%	<0.01	new_order	21497961	4612	.381
						payment	21497954	1631	.370
						order_status	2149796	179	<0.01
						delivery	2149798	669	.400
						stock_level	2149794	623	.361
68	417047	250699	1758	8.58%	<0.01	new_order	21760961	4685	.400
						payment	21760978	1653	.390
						order_status	2176090	179	.254
						delivery	2176092	682	.396
						stock_level	2176104	631	.341
69	423860	250699	1465	8.71%	<0.01	new_order	22116088	4753	.090
						payment	22116104	1680	.310
						order_status	2211612	182	<0.01
						delivery	2211598	691	.340
						stock_level	2211611	639	<0.01
70	428707	250699	1803	10.7%	<0.01	new_order	22368984	4826	.390
						payment	22368978	1702	.371

						der_status	2236890	185	<0.01
						delivery	2236893	700	.391
						stock_level	2236894	648	.351
71	433599	250699	1511	9.56%	<0.01	new_order	22624039	4894	.401
						payment	22624068	1727	.380
						order_status	2262410	189	.401
						delivery	2262411	710	.399
						stock_level	2262409	656	.371
72	436717	250699	1855	11.6%	<0.01	new_order	22786942	4964	.401
						payment	22786907	1745	.400
						order_status	2278694	190	.400
						delivery	2278691	724	.399
						stock_level	2278696	669	.401
73	436428	250699	1556	9.76%	<0.01	new_order	22771860	5021	.655
						payment	22771904	1774	.800
						order_status	2277187	194	.400
						delivery	2277182	745	.401
						stock_level	2277194	674	.400
74	437534	250699	1905	9.57%	<0.01	new_order	22828606	5098	.401
						payment	22828617	1793	.401
						order_status	2282859	196	.401
						delivery	2282856	757	.441
						stock_level	2282865	679	.401
75	436143	250699	1594	8.90%	<0.01	new_order	22755860	5160	.521
						payment	22755859	1807	.476
						order_status	2275596	195	.390
						delivery	2275581	787	.490
						stock_level	2275582	690	.401
76	437219	250699	1946	9.73%	<0.01	new_order	22812199	5208	.401

						payment	22812213	1838	.550
						order_status	2281224	198	.401
						delivery	2281214	814	.401
						stock_level	2281221	698	.402
77	437089	250699	1637	9.07%	<0.01	new_order	22805760	5269	.401
						payment	22805785	1859	.737
						order_status	2280577	203	.400
						delivery	2280578	837	.408
						stock_level	2280573	704	.401
78	436712	250699	1999	11.3%	<0.01	new_order	22786709	5340	.691
						payment	22786692	1885	.635
						order_status	2278666	204	.400
						delivery	2278670	845	.401
						stock_level	2278674	712	.401
79	437185	250699	1667	10.2%	<0.01	new_order	22811169	5385	.401
						payment	22811211	1905	.545
						order_status	2281130	205	.400
						delivery	2281111	870	.723
						stock_level	2281125	734	.401
80	436265	250699	2031	9.87%	<0.01	new_order	22763538	5466	.458
						payment	22763561	1915	.686
						order_status	2276360	208	.401
						delivery	2276350	903	.411
						stock_level	2276356	728	.401
81	437064	250699	1709	12.0%	<0.01	new_order	22804091	5508	.489
						payment	22804107	1940	.708
						order_status	2280399	219	.401
						delivery	2280406	930	.800
						stock_level	2280409	737	.401

82	436071	250699	2074	0.0%	<0.01	new_order	22753631	5585	.659
						payment	22753621	1948	.642
						order_status	2275368	215	.401
						delivery	2275360	952	.702
						stock_level	2275368	748	.401
83	436479	250699	1751	9.81%	<0.01	new_order	22774329	5594	.401
						payment	22774307	1957	.791
						order_status	2277430	215	.551
						delivery	2277429	1049	.799
						stock_level	2277435	747	.401
84	436144	250699	2125	11.6%	<0.01	new_order	22757050	5698	.795
						payment	22757078	2005	.687
						order_status	2275706	217	.400
						delivery	2275695	1005	.800
						stock_level	2275702	756	.401
85	435393	250699	1796	10.5%	<0.01	new_order	22717099	5744	.800
						payment	22717134	2043	.660
						order_status	2271711	224	.401
						delivery	2271722	1026	.801
						stock_level	2271720	766	.401
86	435699	250699	2176	14.2%	<0.01	new_order	22733460	5810	.424
						payment	22733447	2051	.591
						order_status	2273339	215	.401
						delivery	2273346	1068	1.20
						stock_level	2273343	779	.401
87	435007	250699	1828	11.2%	<0.01	new_order	22697869	5854	.524
						payment	22697924	2046	.694
						order_status	2269790	223	.401
						delivery	2269791	1124	.799

						stock_level	2269789	778	.402
88	435357	250699	2218	12.3%	<0.01	new_order	22715782	5958	.409
						payment	22715812	2077	.675
						order_status	2271584	222	.401
						delivery	2271584	1106	1.02
						stock_level	2271574	781	.401
89	434565	250699	1865	12.4%	<0.01	new_order	22674879	5991	.666
						payment	22674859	2143	.798
						order_status	2267479	224	.400
						delivery	2267492	1120	.803
						stock_level	2267482	793	.401
90	434448	250699	2246	15.6%	<0.01	new_order	22668712	6056	.692
						payment	22668727	2131	.701
						order_status	2266874	229	.411
						delivery	2266879	1153	.799
						stock_level	2266869	809	.401
91	435112	250699	1906	11.5%	<0.01	new_order	22703178	6117	.617
						payment	22703212	2147	.606
						order_status	2270310	237	.401
						delivery	2270312	1201	.929
						stock_level	2270318	797	.801
92	434269	250699	2299	12.7%	<0.01	new_order	22658276	6111	.650
						payment	22658258	2167	.599
						order_status	2265820	236	.782
						delivery	2265829	1282	.860
						stock_level	2265834	819	.401
93	434172	250699	1943	14.2%	<0.01	new_order	22653180	6232	.642
						payment	22653196	2184	.800
						order_status	2265324	232	.401

						delivery	2265324	1257	.801
						stock_level	2265324	825	.401
94	434100	250699	2332	16.7%	.010	new_order	22650980	6291	.615
						payment	22650973	2211	.699
						order_status	2265094	233	.401
						delivery	2265093	1290	1.08
						stock_level	2265087	822	.401
95	433548	250699	1978	13.9%	<0.01	new_order	22621785	6331	.800
						payment	22621791	2222	.802
						order_status	2262181	244	.440
						delivery	2262189	1340	.801
						stock_level	2262183	825	.401
96	433530	250699	2374	15.0%	<0.01	new_order	22620652	6382	.409
						payment	22620601	2266	.681
						order_status	2262063	242	.401
						delivery	2262063	1334	.801
						stock_level	2262066	850	.401
97	432968	250699	2018	16.0%	<0.01	new_order	22591305	6444	.800
						payment	22591315	2271	.749
						order_status	2259127	245	.401
						delivery	2259129	1378	1.20
						stock_level	2259136	856	.401
98	432906	250699	2428	16.1%	<0.01	new_order	22588509	6438	.500
						payment	22588478	2243	.799
						order_status	2258846	244	.400
						delivery	2258844	1539	1.17
						stock_level	2258856	847	.401
99	433169	250699	2057	17.2%	<0.01	new_order	22601421	6540	.476
						payment	22601449	2302	.799

						rder_status	2260144	255	.401
						delivery	2260154	1459	1.57
						stock_level	2260140	867	.401
100	433431	250699	2461	13.8%	<0.01	new_order	22615125	6610	.521
						payment	22615125	2343	.642
						order_status	2261520	254	.521
						delivery	2261504	1446	.801
						stock_level	2261524	876	.402
101	432476	250699	2089	15.1%	<0.01	new_order	22565285	6645	.791
						payment	22565284	2341	.797
						order_status	2256534	248	.401
						delivery	2256518	1549	1.20
						stock_level	2256546	872	.401
102	433058	250699	2502	15.3%	<0.01	new_order	22596232	6687	.405
						payment	22596202	2369	.748
						order_status	2259624	254	.401
						delivery	2259621	1593	1.04
						stock_level	2259612	884	.401
103	432999	250699	2136	13.0%	<0.01	new_order	22592958	6781	.800
						payment	22592963	2376	.793
						order_status	2259291	254	.401
						delivery	2259309	1561	1.20
						stock_level	2259301	910	.402
104	433053	250699	2562	18.5%	<0.01	new_order	22595989	6859	.751
						payment	22595961	2392	.634
						order_status	2259596	272	.401
						delivery	2259603	1557	1.60
						stock_level	2259594	914	.401
105	432648	250699	2168	17.0%	<0.01	new_order	22574436	6879	.800

						payment	22574424	2415	.794
						order_status	2257444	262	.401
						delivery	2257440	1653	1.24
						stock_level	2257440	911	.401
106	432910	250699	2587	18.1%	<0.01	new_order	22588133	6930	.611
						payment	22588149	2443	.642
						order_status	2258806	275	.401
						delivery	2258813	1678	1.20
						stock_level	2258805	912	.491
107	432423	250699	2207	15.3%	<0.01	new_order	22562125	6973	.431
						payment	22562109	2488	.648
						order_status	2256220	273	.450
						delivery	2256216	1700	1.20
						stock_level	2256209	927	.402
108	431838	250699	2642	17.6%	<0.01	new_order	22531069	7064	.429
						payment	22531037	2481	.675
						order_status	2253115	265	.401
						delivery	2253098	1701	1.20
						stock_level	2253106	949	.411
109	432335	250699	2243	18.7%	<0.01	new_order	22557163	7124	.800
						payment	22557160	2495	.799
						order_status	2255719	272	.401
						delivery	2255712	1752	1.20
						stock_level	2255715	943	.402
110	432470	250699	2676	22.6%	.010	new_order	22565911	7083	.706
						payment	22565919	2502	.797
						order_status	2256592	281	.401
						delivery	2256595	1902	1.59
						stock_level	2256590	929	.402

111	431956	250699	2282	9.9%	<0.01	new_order	22538175	7032	.634
						payment	22538146	2507	.800
						order_status	2253819	278	.401
						delivery	2253819	2079	1.20
						stock_level	2253809	929	.402
112	432266	250699	2710	14.4%	<0.01	new_order	22555114	7231	.801
						payment	22555078	2558	.795
						order_status	2255511	284	.421
						delivery	2255498	1912	1.60
						stock_level	2255493	961	.401
113	432379	250699	2324	15.1%	<0.01	new_order	22561014	7253	2.52
						payment	22560976	2584	.790
						order_status	2256086	273	.411
						delivery	2256102	1991	1.60
						stock_level	2256079	963	2.00
114	432567	250699	2747	16.1%	<0.01	new_order	22570791	7349	.793
						payment	22570785	2599	.667
						order_status	2257085	280	.646
						delivery	2257071	1977	1.20
						stock_level	2257084	974	.411
115	432758	250699	2357	16.4%	<0.01	new_order	22580579	7373	2.53
						payment	22580544	2586	2.00
						order_status	2258052	294	.403
						delivery	2258028	2044	1.60
						stock_level	2258058	987	.402
116	432084	250699	2789	15.7%	<0.01	new_order	22544995	7428	2.45
						payment	22545009	2627	2.00
						order_status	2254498	289	.401
						delivery	2254498	2055	1.59

						stock_level	2254497	992	.411
117	432650	250699	2397	17.6%	<0.01	new_order	22574348	7448	2.23
						payment	22574370	2639	.807
						order_status	2257444	285	.794
						delivery	2257444	2138	2.00
						stock_level	2257435	1001	.401
118	431677	250699	2831	13.1%	<0.01	new_order	22523204	7470	.550
						payment	22523193	2668	.807
						order_status	2252336	289	.401
						delivery	2252320	2203	1.83
						stock_level	2252329	1001	.411
119	432194	250699	2437	14.8%	<0.01	new_order	22550931	7642	2.00
						payment	22550913	2695	.998
						order_status	2255094	292	1.78
						delivery	2255098	2105	1.59
						stock_level	2255092	1009	2.00
120	432111	250699	2853	12.3%	<0.01	new_order	22546415	7617	.796
						payment	22546400	2689	.804
						order_status	2254652	304	.401
						delivery	2254639	2259	1.69
						stock_level	2254633	1011	.401
121	431944	250699	2479	14.0%	<0.01	new_order	22537536	7685	.800
						payment	22537514	2714	.799
						order_status	2253750	290	.578
						delivery	2253753	2295	1.60
						stock_level	2253763	1003	.521
122	432075	250699	2888	16.8%	<0.01	new_order	22543817	7681	2.58
						payment	22543766	2698	1.82
						order_status	2254375	293	.401

						delivery	2254381	2417	1.55
						stock_level	2254377	1020	.401
123	431878	250699	2515	13.4%	<0.01	new_order	22534293	7815	2.39
						payment	22534273	2748	.795
						order_status	2253439	307	.403
						delivery	2253422	2309	1.68
						stock_level	2253441	1030	2.19
124	432317	250699	2933	15.2%	<0.01	new_order	22557172	7796	2.50
						payment	22557173	2744	.799
						order_status	2255719	299	.401
						delivery	2255712	2480	1.60
						stock_level	2255721	1037	.410
125	432337	250699	2551	18.2%	<0.01	new_order	22557110	7816	2.36
						payment	22557073	2757	2.30
						order_status	2255698	294	.677
						delivery	2255709	2555	1.60
						stock_level	2255714	1036	2.21
126	431955	250699	2969	13.5%	<0.01	new_order	22538691	7885	2.55
						payment	22538682	2781	2.00
						order_status	2253859	302	.797
						delivery	2253876	2554	2.39
						stock_level	2253869	1038	2.00
127	432242	250699	2588	16.1%	<0.01	new_order	22553068	7906	2.26
						payment	22553079	2816	.860
						order_status	2255302	312	.404
						delivery	2255299	2592	2.59
						stock_level	2255306	1047	.401
128	431665	250699	3020	17.4%	<0.01	new_order	22522415	7819	2.43
						payment	22522425	2795	2.52

						rder_status	2252242	299	.401
						delivery	2252246	2873	2.00
						stock_level	2252240	1025	2.00
129	432037	250699	2629	14.8%	<0.01	new_order	22542025	8031	.787
						payment	22542003	2881	2.00
						order_status	2254192	312	.531
						delivery	2254200	2628	2.00
						stock_level	2254196	1060	.402
130	431422	250699	3056	16.2%	<0.01	new_order	22509911	8018	2.51
						payment	22509937	2854	.968
						order_status	2250992	309	.411
						delivery	2250986	2773	1.76
						stock_level	2251003	1073	2.00
131	431697	250699	2664	14.7%	<0.01	new_order	22523501	8171	2.19
						payment	22523551	2906	2.00
						order_status	2252346	322	.796
						delivery	2252363	2668	1.60
						stock_level	2252358	1088	.402
132	431588	250699	3087	18.4%	<0.01	new_order	22519542	8175	2.00
						payment	22519519	2873	2.37
						order_status	2251951	330	2.00
						delivery	2251948	2828	2.30
						stock_level	2251951	1080	2.43
133	431672	250699	2704	16.0%	<0.01	new_order	22522943	8224	2.28
						payment	22522969	2898	2.40
						order_status	2252292	321	.401
						delivery	2252289	2853	2.40
						stock_level	2252287	1100	2.00
134	431721	250699	3131	16.7%	<0.01	new_order	22525346	8155	2.44

						payment	22525284	2890	2.41
						order_status	2252526	323	2.54
						delivery	2252534	3102	2.00
						stock_level	2252539	1049	2.00
135	431147	250699	2745	15.3%	<0.01	new_order	22495939	8138	2.49
						payment	22495918	2892	2.48
						order_status	2249586	322	.401
						delivery	2249612	3224	2.52
						stock_level	2249601	1080	1.82
136	431341	250699	3161	16.9%	<0.01	new_order	22506079	8327	2.59
						payment	22506080	2950	2.48
						order_status	2250601	321	.797
						delivery	2250606	3030	2.36
						stock_level	2250617	1104	2.29
137	432043	250699	2788	15.4%	<0.01	new_order	22542654	8396	2.59
						payment	22542667	2923	2.09
						order_status	2254267	315	1.69
						delivery	2254261	3114	2.37
						stock_level	2254280	1099	2.56
138	431690	250699	3205	15.1%	<0.01	new_order	22524499	8420	2.57
						payment	22524470	3033	2.32
						order_status	2252437	319	.643
						delivery	2252444	3069	2.57
						stock_level	2252440	1127	2.46
139	431814	250699	2817	15.7%	<0.01	new_order	22530001	8455	2.59
						payment	22529987	2999	2.54
						order_status	2253006	323	.978
						delivery	2252982	3191	2.28
						stock_level	2252989	1106	2.00

						stock_level	2249963	1110	2.00
146	431136	250699	3348	17.6%	<0.01	new_order	22494609	8796	2.53
						payment	22494623	3101	2.91
						order_status	2249476	357	.797
						delivery	2249456	3465	2.91
						stock_level	2249461	1158	2.44
147	431605	250699	2965	16.4%	<0.01	new_order	22520376	8869	2.72
						payment	22520386	3160	2.85
						order_status	2252031	332	1.20
						delivery	2252040	3478	2.59
						stock_level	2252036	1174	2.80
148	431383	250699	3400	18.1%	<0.01	new_order	22508992	8901	2.85
						payment	22508998	3120	2.53
						order_status	2250899	341	2.23
						delivery	2250905	3594	2.52
						stock_level	2250890	1190	2.52
149	430903	250699	3004	19.1%	<0.01	new_order	22483029	8827	3.14
						payment	22482994	3145	2.75
						order_status	2248299	352	2.00
						delivery	2248293	3776	2.81
						stock_level	2248302	1160	2.31
150	431436	250699	3431	22.9%	<0.01	new_order	22510840	8896	2.95
						payment	22510776	3139	2.92
						order_status	2251084	342	2.42
						delivery	2251097	3811	2.84
						stock_level	2251079	1173	2.99
[illegible]	431243	250699	3050	18.9%	<0.01	new_order	22500583	8984	3.00
						payment	22500592	3193	2.96
						order_status	2250060	352	2.41

3530

140	431771	250699	3242	.4%	<0.01	new_order	22528315	8354	2.28
						payment	22528325	3000	2.32
						order_status	2252834	323	2.32
						delivery	2252838	3457	2.10
						stock_level	2252835	1088	2.55
141	431299	250699	2857	17.1%	<0.01	new_order	22502913	8507	2.58
						payment	22502941	3036	2.34
						order_status	2250298	332	.401
						delivery	2250287	3339	2.07
						stock_level	2250291	1121	.741
142	431284	250699	3276	19.1%	<0.01	new_order	22503499	8396	2.55
						payment	22503478	2985	2.26
						order_status	2250339	315	2.00
						delivery	2250354	3687	2.11
						stock_level	2250348	1084	2.42
143	431111	250699	2889	18.5%	<0.01	new_order	22494260	8663	2.57
						payment	22494248	3054	2.24
						order_status	2249433	338	.630
						delivery	2249423	3381	2.40
						stock_level	2249419	1146	2.54
144	431606	250699	3315	16.6%	<0.01	new_order	22518962	8635	2.61
						payment	22518953	3061	2.48
						order_status	2251881	340	2.00
						delivery	2251905	3516	2.40
						stock_level	2251888	1118	1.84
145	431205	250699	2934	14.9%	<0.01	new_order	22499684	8592	2.58
						payment	22499700	3020	2.59
						order_status	2249968	330	2.23
						delivery	2249980	3751	2.25

[Return to Non Printer Friendly Page]

Sun Fire[tm] 12K / 15K Server: Hardware Specifications

Processor	
Number	**Sun Fire 12K:** 4 to 52 **Sun Fire 15K:** 16 to 106
Architecture	900 MHz, 1050MHz or 1200MHz UltraSPARC[tm] III CPU, ECC protected
Cache per processor Level 1 Level 2	 ECC protected 32 KB instruction and 64 KB data on chip ECC protected 8 MB external cache
System Interconnect	150 MHz Sun[tm] Fireplane redundant 18X18 data, address, and response crossbar interconnect
System Boards	
CPU/Memory Boards	**Sun Fire 12K:** Up to 9 CPU/Memory boards, each holding 4 processors and up to 32GB memory (32 DIMMs per board, 8 banks of 4 DIMMS), providing up to 288GB memory per system, and common design across the entire Sun Fire 3800 - 15K server line. **Sun Fire 15K:** Up to 18 CPU/Memory boards, each holding 4 processors and up to 32GB memory (32 DIMMs per board, 8 banks of 4 DIMMS), providing up to 576GB memory per system, and common design across the entire Sun Fire 3800 - 15K server line.
I/O	**Sun Fire 12K:** 9 I/O hubs support up to 36 I/O hot-swappable PCI slots. 18 slots are 66MHz, 18 slots are 33MHz. **Sun Fire 15K:** 18 I/O hubs support up to 72 I/O hot-swappable PCI slots. 36 slots are 66MHz, 36 slots are 33MHz.
System Controller (SC)	2 redundant system controllers. Automatic system failover of system controllers, automatic failover of SC clock and management functions, with no service interruption to users.
Main Memory	
Sun Fire 12K: 8GB to 288GB memory capacity per system, up to 288 DIMMs total per system **Sun Fire 15K:** 16GB to 576GB memory capacity per system, up to 576 DIMMs total per system 1GB, 2GB, and 4GB memory expansion options (each a group of 4 DIMMs) Up to eight memory expansion options per CPU/Memory board	
Standard Interfaces	
Ethernet	One ethernet/fast ethernet (10BASE-T/100BASE-TX) standard twisted-pair port (RJ-45) per system controller board.

PCI	Four slots per hsPCI assembly supporting up to two 33-MHz and two 33/66-MHz industry standard PCI boards.
Serial	One RS-232 serial TTYA port (mini-DIN8) per system controller board.
Internal Mass Storage	
Disks (Internal - System Controller Peripheral Board)	2 mirrored 18.2GB - 10000 RPM Disk Drives (system controller boot disks)
Disk Arrays (External - Peripheral Cabinet)	Sun StorEdge[tm] S1 *
DVD-ROM (Internal - System Controller Peripheral Board)	10X DVD-ROM Drive
Tape (Internal - System Controller Peripheral Board)	20-40 GB 4 mm DDS-4 Tape Drive
Primary boot device for Sun Fire 12K / 15K.	
Power Supplies	
N+1 redundant 6 dual-input AC-to-48 volt DC power supplies Two power cables go to each supply, so they can connect to separate power grids (12 power cords)	
Environment	
AC power	200 - 240 VAC, single phase, 47 - 63 Hz; requires 12 - 30 A circuits
Input power	**Sun Fire 12K:** 12,965 W **Sun Fire 15K:** 23,927 W
Heat output	44,081 BTU /hr (up to 9 slots occupied) 81,352 BTU/hr (up to 18 slots occupied)
mperature [1]	**Optimal:** 21° C to 23° C (70° F to 74° F) **Operating:** 10° C to 35° C (50° F to 95° F) **Nonoperating:** -20° C to 60° C (-4° F to 140° F)
Humidity	**Optimal:** 45% to 50% relative humidity, noncondensing **Operating:** 20% to 80% relative humidity, noncondensing **Nonoperating:** up to 93% relative humidity, noncondensing
Altitude	**Operating:** 3000 m (10,000 ft.) **Nonoperating:** 12,000 m (40,000 ft.)
Plug type - U.S. & Japan	NEMA L6-30P
Plug type - International	IEC 309, single phase, 32 A
1 - derate 2° C for every 1 km up to 3 km	
Regulations **Meets or exceeds the following requirements:**	
Safety	UL 1950, CUL CAN/CSA 22:2 M950, TUV EN60950

RFI/EMI FCC Immunity	Class A, EN50021-1 Class A, EN50082-1
Dimensions and Weights	
Height	191.8 cm (75.5 in.) 203.2 cm (80.0 in.) shipping
Width	84.6 cm (33.3 in.) 121.9 cm (48.0 in.) shipping
Depth	163.8 cm (64.5 in.) 191.8 cm (75.5 in.) shipping
Weight	**Sun Fire 12K:** 996.1 kg (2191.5 lb.); 1198.4 kg (2636.5 lb.) shipping **Sun Fire 15K:** 1142.6 kg (2513.7 lb.); 1344.9 kg (2958.7 lb.) shipping
Power cord	457 cm (15.0 ft.)
Clearance and Service Access	
Front	111.8 cm (44.0 in.) service access
Rear	111.8 cm (44.0 in.) service access
Please see the Sun Fire 15K System Site Planning Guide (806-3510) for information about proper cooling clearances and installation.	

Sun Fire 15K

System Detailed View

Product Home

- » Features & Benefits
- » Specifications
- ☐ Detailed View

Price & Buy »

Table of Contents

Overview

With 106 UltraSPARC[tm] III Cu 1.2 GHz processors, more than half a terabyte of memory in a single domain, and fifth-generation Dynamic System Domains, the Sun Fire[tm] 15K server helps redefine total cost of ownership (TCO) in data center environments. In order to further reduce TCO, the Sun Fire 15K server is now enhanced with the Capacity on Demand 2.0 "pay when used" option and the high performance Memory Placement Optimization Functionality.

Back to top

Evaluate

- » Product Home
- » Product Photo
- » System Performance
- » Customer Testimonia
- » Interactive Tour
- » Dynamic Reconfiguration
- » System Management Services
- » Server Comparisons
- » White Papers
- » Awards & Reviews

Get

- » Price & Buy
- » Consulting Services

Use

- » Documentation
- » Sun Blueprints Program

Maintain

- » System Upgrades
- » Sun Spare Parts

Low Total Cost of Ownership

Reducing total cost of ownership (TCO) and increase return on investment (ROI) are crucial today. Sun is the only vendor to offer address horizontal, vertical AND cross-generational scalability - from single processor workstations to large SMP systems. By committing to a seamless, smooth upgrade path, Sun helps keep your total cost of ownership low. With a common UltraSPARC(r) architecture, common Solaris Operating Environment, binary compatibility (from a single-CPU to hundreds of CPU systems, spanning generations and common components) -- Sun delivers unparalleled protection of your applications and hardware investments.

The Sun Fire servers are an extension of Sun's award-winning Sun Enterprise[tm] family of servers. Sun will continue to enhance and support the Enterprise family for years to come, allowing you to adopt the

Sun Fire servers according to your schedule.

Back to top

» Support Services
» Warranties

See Also
» All Sun High-End Servers

Dynamic Resource Management

Sun provides mainframe-class resource management tools to users of both high-end and midrange servers. Today, it's more vital than ever to have complete control over your system resources. With the Sun Fire 15K server, this aspect of IT management is easier than ever, thanks to Dynamic System Domains, Solaris Resource Manager[tm] software, Solaris[tm] Bandwidth Manager software and Solaris Processor Sets.

Sun has a long history of providing the tools and capabilities you need to reduce administrative costs, increase the flexibility of your IT resources and dynamically match your systems to your business requirements. While many organizations are just beginning to talk about partitioning and maximizing technological resources in an open systems environment, Sun has been delivering these capabilities for more than six years.

Dynamic System Domains

Sun's proven Dynamic System Domain technology allows you to run multiple mission-critical applications on a single server. Each domain is fully isolated from hardware and software faults that may occur in another domain. With Dynamic Reconfiguration (DR), you can easily move system resources from one domain to another to support fluctuations in business workloads. Also, you can flexibly customize I/O and CPU/memory to your requirements by independently associating any I/O board with any domain. Ideal for server consolidation projects, Dynamic System Domains provide flexible, mainframe-like resource management enabling you to optimize your IT resources.

With the Sun Fire 15K server, Sun introduces the 5th-generation Dynamics System Domains which provides advanced domain resource management capabilities, including:

- InterDomain Networking (IDN): Construct a very high-speed virtual TCP/IP network connection between two domains across the Sun Fireplane Interconnect the fastest domain-to-domain communications.
- Shared Resource Domains: Prevent errors in one IDN domain from affecting the other, helping to ensure availability and uptime.
- Automated Dynamic Reconfiguration: Allows you to script threshold- or time-based DR operations, enabling you to automatically match your IT resources to your business requirements.

Processor Sets

Processor sets enable a Sun Fire 15K server's UltraSPARC III processors to be divided into dedicated groups for enhanced management of your CPU resources. Through Solaris Operating Environment commands, processes may be bound to a particular set of processors, preventing CPU contention and eliminating processor starvation. Because multiple applications can run within their own processor sets on dedicated CPUs, processor sets also help to facilitate server consolidation.

Back to top

Mainframe Rehosting

All businesses must drive down operational costs to sustain long-term competitive advantage in the market. For IT organizations with large investments in mainframes, this is an increasing challenge. With no real competitors left in the mainframe server business, the cost of the associated hardware and software licenses continue their rapid rate of increase.

The challenge for mainframe-based businesses today is how to keep the value of proven CICS and batch applications, while dramatically reducing the costs associated with mainframes.

Through the Mainframe Affinity Program, Sun offers products, tools, partnerships and services that help enable you to interoperate with, rehost or replace mainframe applications on more cost-efficient, open platforms - often at equal or greater levels of performance, flexibility and scalability.

Sun mainframe rehosting solutions help enable you to reuse your mainframe applications and data files on high performance, high availability Sun servers and to redefine total cost of ownership across your IT organization, resulting in up to 70% cost savings.

Back to top

Availability

Sun takes a broad, integrated approach to providing high availability. The Sun Fire 15K server delivers mainframe-class features such as full hardware redundancy, Dynamic System Domains and Hot Swap Components. These features, combined with the Solaris 8 Operating Environment, Sun[tm] Cluster software and Sun StorEdge[tm] storage solutions is designed to bring you the high availability your enterprise demands.

The rock-solid, mainframe-class availability offered by the Sun Fire 15K server creates an ideal platform for your organization's most mission-critical applications. Extensive availability features include:

- 5th-generation Dynamic System Domains
- Automated System Controller failover
- Full Hardware Redundancy
- Dynamic Reconfiguration
- Hot CPU Upgrades
- Memory Scrubbing
- ECC-Protected E-cache
- End-to-End Data Integrity, including ECC Protection
- Concurrent CPU, Memory and I/O Maintenance
- Online Hardware Upgrades
- Hardened Operating System Kernel
- Live Operating System Upgrades
- Redundant I/O Channels
- Automatic System Recovery
- Parity Protected L1 Cache
- Redundant Power
- Redundant Cooling

For virtually continuous application access and built-in load balancing, Cluster Platforms provide factory-integrated combinations of software, servers, and storage arrays designed to help you simplify deployment of IT infrastructures. These application-ready hardware and software stacks have been pre-tested for interoperability and reliability, so you can get all the benefits of Sun technology while reducing the time, cost, and risk of deployment.

Sun's Service organization will guide you in designing, implementing and managing solutions that help ensure every aspect of your environment supports your uptime goals. Sun's innovative programs, proven methodologies and proactive services -- such as SunReady[sm] Lifecycle Advantage and Sun Remote Services -- help you to minimize downtime and maximize availability and ease of management.

Separate Admin/Error Busses

Advancements in the Sun Fire 15K server include separate uptime (error) and console (administration) busses to enhance reliability, availability, and serviceability. Within the UltraSPARC III processor, the uptime bus runs independent of the main system bus, allowing the CPU to be powered-on, configured and tested without requiring that the majority of the system be operational. For example, if a fatal error is detected on the system bus, each processor can boot and run diagnostics over the uptime bus to identify and isolate any problems. Additionally, key portions of internal state can be sampled in real-time -- even while the machine continues to run a normal workload. This enables visibility into the CPU for both detection and proactive prevention of errors.

A separate console bus communicates with each of up to 18 Dynamic System Domains if data and address busses are inaccessible. The console bus is also used for system component configuration as well as low-level diagnostic execution.

System Controller Failover

The internally-packaged System Controller (SC), running a separate instance of the highly reliable Solaris Operating Environment, expertly monitors, administers and manages all resources for the Sun Fire system. The Sun Fire 15K server is uniquely configured with redundant, failover System Controllers, to provide uninterrupted access to system administration. Failover assists in ensuring no single point of failure in the management of the system. At any time during SC failover, the failover process does not affect any configured or running Dynamic System Domains, except for temporary loss of services from the SC. In the event of hardware or software failures, the SC will failover to the active spare SC. All System Management Services data, configuration, and log files are replicated on the spare SC, while active domains continue to operate.

There are two private Ethernets for communications between the two System Controllers. This private network is used as a heartbeat function between each System Controller, as well as data replication of platform/domain configuration files.

Traffic Manager

Traffic Manager I/O is designed to deliver automatic fail-over to alternate paths in the event of a path failure. It also helps to provide manual path switch-over for Dynamic Reconfiguration (DR), ideal for high data-transfer environments. Additionally, Traffic Manager's tunable, policy-driven load balancing enhances I/O performance for devices with multiple paths by providing a native N-Way multipathing solution for SCSI-3 FC storage devices in Solaris Operating Environment.

Back to top

Data Integrity

Error correcting code and parity protection throughout system, including error protection on UltraSPARC(r) III processors, data cache, system interface, Sun Fireplane Interconnect, and console bus.

Back to top

Scalability

With today's heightened focus on total cost of ownership (TCO) and return on investment (ROI), maintaining flexibility is vital to extracting the most from your investments. The ability to easily add capacity, performance and bandwidth -- with the minimum amount of complexity -- is key to being able to provision resources where needed.

Sun delivers the architecture on which you can build a massively scalable and redeployable application environment. The Sun Fire servers have been designed from the ground up to scale easily to grow at a pace and redeploys to match your business needs. When combined with the scalability of the Solaris Operating Environment, UltraSPARC III processors, Sun[tm] Cluster software and StorEdge[tm] disk arrays, Sun delivers the scalability you need to be ready for whatever tomorrow brings.

Sun systems are architected with scalability as a key design focus, both for changes in hardware capacities within a server as well as for mid-life product enhancements. As your capacity demands increase, Sun Fire servers support a simple and non-disruptive process for adding CPU, Memory and I/O resources.

The Solaris Operating Environment has the added advantage of more than eight years of effort that enables near linear utilization of multiple processors. Today, Solaris scales efficiently and robustly to 106 UltraSPARC III processors in a single physical chassis.

Sun's ability to pack such a high density of processors within a single physical chassis is a direct outcome of our sophisticated interconnect technology, the Sun Fireplane Interconnect. This crossbar-based interconnect enables a point-to-point connection for all addresses and data transmissions, resulting in low latency and high bandwidth for superior application performance.

Back to top

Big Memory

For memory-intensive computation and processes, databases as large as half a terabyte in a single domain can be performed in-memory, reducing data retrievals from external disk or tape.

Back to top

Scalable Operating System

The Solaris 9 Operating Environment has the added advantage of more than eight years of effort that enables near linear utilization of multiple processors. Today, Solaris scales efficiently and robustly to 106 UltraSPARC III processors in a single physical chassis.

Solaris 9 also provides the Memory Placement Optimization (MPO) feature which enables the servers to put memory closer to the CPU that needs it, therefore increasing performance.

Back to top

High Performance

In any computing system, the key to performance goes beyond individual metrics such as CPU speed or I/O transfer rates. The best performing computing environments deliver balanced performance. The Sun Fire servers deliver a level of performance that is sustainable, real and useful.

The SPARC[tm] architecture, the Solaris Operating Environment and the Sun Fireplane Interconnect have been designed to work together seamlessly. The natural synergies that flow from having the system elements developed using a single design vision results in systems that deliver exceptional real-world performance.

Sun Fireplane Interconnect

In order to provide the bandwidth required to optimize performance in today's computing environments, system interconnects are required to be faster and have lower latencies than ever before. The Sun Fireplane Interconnect is built to provide very high system bandwidth -- up to 172.8 GB/sec peak bandwidth in the Sun Fire 15K server. The Sun Fireplane Interconnect results in deterministic latencies, which translate into more predictable performance across a broad set of applications. What's more, big memory -- over 1/2 TB -- makes Sun Fire systems an excellent platform for in-memory applications and memory-intensive computation.

UltraSPARC III Cu Processors

The UltraSPARC III Cu microprocessor, Sun's third-generation 64-bit processor, incorporates architectural features designed to optimize SMP multiprocessor environments. It scales the clock rates and delivers high memory bandwidth, with a system interface bandwidth of 2.4 GB/sec. The memory subsystems, as well as E-cache, are protected with Error Correcting Code (ECC).

The UltraSPARC architecture is specifically crafted to support workload-intensive environments such as e-commerce, large corporate networks, high-capacity web servers and online transaction processing -- or any demanding commercial or technical computing environment. Key features such as an on-chip memory controller, Uptime bus, and high memory bandwidth all contribute to increased application performance.

Back to top

Memory Placement Optimization (MPO)

A feature of the Solaris Operating Environment, MPO improves the placement of memory pages across the across the physical memory of a server, resulting in increased performance.

Back to top

Investment Protection

Sun systems adhere to a consistent, binary-compatible system design based on the SPARC/Solaris/SMP combination. This design consistency, from generation to generation, helps ensure that Sun systems offer a degree of compatibility not available from any other platform vendor.

Back to top

Secure Management

The Sun Fire 15K server is designed to provide strong security for both single and multiple domain configurations. The highly secure system management environment includes an internal network with dedicated links to each domain and utilizes encryption for system controller-to-domain communications. In addition, multi-level access control capability provides heightened protection by guarding against unauthorized administrator access.

Back to top

System Management

Sun Management Center software offers a single point of management for Sun systems and storage components, the Solaris Operating Environment, and applications running on the Solaris platform. Sun Management Center software integrates into heterogeneous IT environments and scales to allow management from one system to thousands of servers and desktop systems, from anywhere on the network.

Back to top

Remote Administration

Sun's suite of remote management and monitoring services enables proactive, early problem detection and prompt resolution of system events. This contributes to high service levels by delivering faster problem resolution and direct access to Sun experts and design engineers. This also helps protect your invesments in staff by reducing their monitoring workload and enhancing their expertise.

Back to top

Manageability

The Capacity on Demand 2.0 (COD) purchasing option is designed to offer instant access to additional system capacity with no disruption to operations. Customers can configure Sun Fire servers with additional "capacity on demand" resources and pay for those resources only when they are needed.

Back to top

Processor

UltraSPARC III Processors

The UltraSPARC III microprocessor, Sun's third-generation 64-bit processor, incorporates architectural features designed to optimize SMP multiprocessor environments. It scales the clock rates and delivers high memory bandwidth, with a system interface bandwidth of 2.4 GB/sec. The memory subsystems, as well as E-cache, are protected with Error Correcting Code (ECC).

The UltraSPARC architecture is specifically crafted to support workload-intensive environments such as e-commerce, large corporate networks, high-capacity web servers and online transaction processing -- or any

demanding commercial or technical computing environment. Key features such as an on-chip memory controller, Uptime bus, and high memory bandwidth all contribute to increased application performance.

Back to top

Capacity

- Up to 106 UltraSPARC(r) III Cu 1.2-GHz Processors
- More than 1/2 TB Memory in a single domain
- Up to 18 fifth-generation Dynamic System Domains
- Hot-swappable Uniboard CPU/Memory Boards, I/O, MaxCPU boards, power, fans
- Redundant, high-performance Sun[tm] Fireplane Interconnect with up to 172.8 GBps peak bandwidth
- Full hardware redundancy including power and cooling systems

Back to top

System

Uniboard CPU/Memory Boards Common across all Sun Fire 3800-15K servers, the Uniboard CPU/memory board design allows customers to provision resources between Sun servers to meet specific application needs, providing investment protection and resource flexibility. The Sun Fire 15K server supports up to eighteen Uniboard CPU/memory boards, providing a total memory capacity of 576 GB for the domain. Each Uniboard in the Sun Fire 15K server is configured with four UltraSPARC III Cu 1.2-GHz processors and up to 32 GB of memory. Memory is arranged in eight banks of four DIMM modules each, with two banks associated with each processor. Customers can also opt to use a smaller Uniboard CPU/memory board with two processors and 4 GB of memory, enabling the creation of physical domains as small as two processors.

Back to top

Performance

Overall System Bandwidth Up to 172.8 GBps peak, up to 43.2 GBps sustained.

Overall I/O Bandwidth: up to 21.6 GBps sustained.

Back to top

Availability

Full hardware redundancy, Hot Swap CPU, Memory, I/O, Power and Fans, Upgrades, Online upgrades, Journaling file system, Concurrent maintenance, Full data integrity, Redundant network connections, Redundant storage connections, Hardened operating system kernel, Hardened I/O drivers,

Back to top

RAS Features

Sun's proven Dynamic System Domain technology allows you to run multiple mission-critical applications on a single server. Each domain is fully isolated from hardware and software faults that may occur in another domain. With Dynamic Reconfiguration (DR), you can easily move system resources from one domain to another to support fluctuations in business workloads. Also, you can flexibly customize I/O and CPU/memory to your requirements by independently associating any I/O board with any domain. Ideal for server consolidation projects, Dynamic System Domains provide flexible, mainframe-like resource management enabling you to optimize your IT resources.

Back to top

Security

The Sun Fire 15K server is designed to provide strong security for both single and multiple domain configurations. The highly secure system management environment includes an internal network with dedicated links to each domain and utilizes encryption for system controller-to-domain communications. In addition, multi-level access control capability provides heightened protection by guarding against unauthorized administrator access.

Back to top

Resource Management

Fifth-generation Dynamic System Domains, Solaris Resource Manager [tm] software, Solaris Bandwidth Manager software

Back to top

Software

Solstice Site Manager[tm] and Solstice Domain Manager[tm], Solstice Backup[tm], Solstice DiskSuite[tm], Sun StorEdge[tm]

Volume Manager, VERITAS Volume Manager 3.1.1, VERITAS File System 3.4, Sun Cluster 3.0 software

Back to top

Mass Storage

Netra[tm] S1 Thin Storage (Boot Device); 250+ terabytes direct connect storage available; Fibre Channel, Low Voltage Differential and Differential SCSI supported; Sun StorEdge[tm] A5200; Sun StorEdge array products supported, Sun StorEdge 9900 products supported.

Back to top

Power/Fan

Fully redundant power and cooling are standard with this system.

Back to top

Environment

AC Power:
200-240 single phase VAC, 47-63 Hz, with six 30 Amp circuits redundant with another six on 2 separate power grids

Operating:
10° C to 35° C; 50° F to 90° F; 20% to 80% relative humidity; altitude up to 3,048 m (10,000 ft.)

Back to top

Regulations

Safety:
UL 1950, CUL CAN/CSA 22:2 M950, TUV EN60950

RFI/EMI FCC Immunity:
Class A, EN50021-1 Class A, EN50082-1

Back to top

Dimensions and Weight

Height:
109 cm (74.75 in.)

Width:
85 cm (33.25 in.)

Depth:
166 cm (65 in.)

Weidth:
1,000 kg (2,200 lb.) fully configured

Back to top

Upgrades

Full system upgrades are available for Sun Enterprise[tm] 4x00, 5x00, 6x00 and 10000 systems, along with the Sun Fire 6800 server. Older Sun servers are eligible under Sun's Server Consolidation Program, and trade-in programs for other vendors' servers are also available. For more information, contact your local sales representative.

Back to top

Key Applications and Markets

Product	Overview	Applications
Sun Enterprise 10000	For large-scale mission-critical applications, Sun's 64-way Enterprise [tm] 10000 Server provides	• Business Financial • Customer Management

	mainframe-like Dynamic System Domains that allow multiple applications to run in isolated environments on a single server.	Solutions ▪ Decision Support Data Warehouse ▪ Electronic Commerce
Sun Fire 12K	With up to 52 UltraSPARC(r) III Cu 1.2-GHz processors and 288 GB of memory per domain with end-to-end data integrity, the Sun Fire[tm] 12K server is an integral building block in a business-ready infrastructure primed to Make the Net Work.	▪ Business Financial ▪ Customer Management Solutions ▪ Decision Support Data Warehouse ▪ Electronic Commerce ▪ Enterprise Resource Planning ▪ ISV Solutions ▪ Software Development ▪ Technical Applications
Sun Fire 15K	With 106 UltraSPARC9(r) III Cu 1.2-GHz processors, more than half a terabyte of memory, and fifth-generation Dynamic System Domains, the Sun Fire[tm] 15K server helps redefine total cost of ownership in data center environments.	▪ Business Financial ▪ Customer Management Solutions ▪ Decision Support Data Warehouse ▪ Electronic Commerce ▪ Enterprise Resource Planning ▪ ISV Solutions ▪ Software Development ▪ Technical Applications

Back to top

1. This page meets my need. disagree ○ ○ ○ ○ ○ ○ agree

2. This page was easy to find. disagree ○ ○ ○ ○ ○ ○ agree

13.564

Sun Fire™ 15K Server

Making the Net work with a massively scalable server ideal for mainframe rehosting, server consolidation, technical computing, and business intelligence.

Key feature highlights

Protect investments with binary compatibility across the entire Sun Fire server family, and hot-swappable, interchangeable Uniboard CPU/Memory boards, common across Sun Fire 4800-15K servers.

Maximize uptime with up to 18 Dynamic System Domains, reconfigurable while applications are running.

Exceptional availability via automatic system failover of two redundant System Controllers and system clock with no service interruption to users.

Scales up to 106 high-performance, award-winning UltraSPARC® III Cu processors in a symmetric multiprocessing architecture.

Fully redundant, reconfigurable Sun™ Fireplane interconnect delivers outstanding real-world performance.

Capacity on Demand (COD) purchasing option helps enhance and simplify system scalability, reduce hardware acquisition costs, and increase system availability.

High Availability with Investment Protection

Running the robust Solaris™ 9 Operating Environment, the Sun Fire™ 15K server features built-in hardware redundancy for maximum uptime and availability, scales up to 106 UltraSPARC® III Cu processors and supports big memory—over 1/2 TB per domain—to handle large workloads or to support server consolidation. The Sun Fire 15K server delivers exceptional performance with up to 172.8 GB/sec aggregate bandwidth via the redundant Sun Fireplane interconnect and through the Memory Placement Optimization (MPO) functionality. Extremely flexible resource management is provided by Dynamic Reconfiguration and Capacity on Demand.

Sun Fire™ 15K Server

Specifications

Processor	
Number	Up to 106
Architecture	UltraSPARC® III Cu Superscalar SPARC® V9, ECC Protected
Cache per processor	Level 1: Parity protected 32 KB instruction and 64 KB data on chip (single-bit errors are corrected) Level 2: ECC protected 8 MB external cache
System interconnect	150 MHz Sun Fireplane redundant 18X18 data, address, and response crossbar interconnect

System	
CPU/Memory boards	Up to 18 Uniboard CPU/Memory Boards, with four processors each and up to 32 GB memory per board; maximum 576 GB memory per domain. (Also, Uniboards with 2 CPUs and 4 GB memory) Up to 17 MaxCPU boards with two processors each. Allows system to expand to 106 processors
I/O	Up to 72 I/O hot-swappable PCI slots; 36 slots are 66 MHz; 36 slots are 33 MHz; supports 10/100BaseT ethernet, gigabit ethernet, UltraSCSI (LVD and HVD), ATM, FC-AL, and HiPPI

Performance	
Overall system bandwidth	Up to 172.8 GB/sec. aggregate, up to 115.2 GB/sec. peak, up to 43.2 GB/sec. sustained
Overall I/O bandwidth	Up to 21.6 GB/sec. sustained

Availability	
Standard	Hot swap CPU, memory, I/O, power, fans Online upgrades Journaling file system Redundant network connections Redundant storage connections Hardened operating system kernel Hardened I/O drivers

RAS Features	
Standard	Dynamic Reconfiguration, Concurrent DR, Initiate DR from domain as well as from System Controller (SC)
Dynamic System Domains	Up to 18 Domains allow secure, fault-isolated, dynamic partitioning of resources within a single server

Security	
Domain management	Dedicated network connections (SC to 18 domains) inside Sun Fireplane interconnect

Resource Management	
Standard	Sun's fifth-generation Dynamic System Domains, Solaris™ Resource Manager, and Bandwidth Manager

Software	
Operating System	Solaris™ 8 or later Operating Environment (10/01 or later)
Languages	C, C++, Pascal, FORTRAN, Java™
Networking	ONC™/NFS™, TCP/IP, SunNet™ OSI, X.25 Start, DCE, Netware
System management	Sun MC 3.0; SMS 1.1 (or later)
Network management	VERITAS Volume Manager 3.1.1, VERITAS File System 3.4, Sun Cluster 3.0

Storage	
Standard	250+ terabytes direct connect storage—Fibre Channel (1 GB and 2 GB) and UltraSCSI; Sun StorEdge™ 9900, 6900, 3900, T3, A5200, S1, D1000, and tape devices

Environment	
AC power	200–240 single phase VAC, 47–63 Hz. Two N+1 power grids, each using six 30-Amp circuits. Second power grid provided for redundancy.
Optimum	22° (72° F) at 45% noncondensing humidity
Range	10° C to 35° C (50° F to 90° F) at 20% to 80% noncondensing humidity
Altitude	Up to 3048 meters /10,000 feet

Regulations	
Meets or exceeds the following requirements:	
Safety	UL/CSA-60950, EN60950, IEC950 CB Scheme with all country deviations, IEC825-1, 2, and CFR21 part 1040
Ergonomics	EK1-ITB-2000
RFI/EMI	ENC55022/CISPR22 Class A, FCC CFR47 Part 15 Class A, EN61000-3-2, EN61000-3-3 FCC
Immunity	EN55024
Regulatory markings	CE, FCC A, ICES-003 A, C-tick, VCCI A, GOST-R, BSMI, EK, UL/cUL, TUV-GS

Dimensions and Weight	
Height	191 cm (74.75 in.)
Width	85 cm (33.25 in.)
Depth	166 cm (65 in.)
Weight	1122 kg (2468 lb.) fully configured

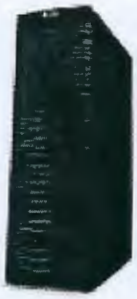
Upgrades

The Upgrade Advantage Program is available to customers trading in older Enterprise™ 4x00, 5x00, 6x00, and 10000 systems. Trade-in allowances are available towards the purchase of new Sun Fire™ 4800, 6800, 12K, and 15K servers. Customers trading in multiple Sun or competitive servers can utilize Sun's Server Consolidation Program.

Purchase these products from the Sun℠ Store, sun.com/store, or contact your Sun Sales Rep, or an authorized Sun reseller near you.

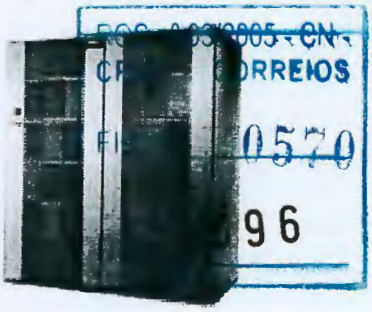
For related server choices refer to:

Sun Fire 12K



Sun Fire 6800

For complementary storage refer to:



Sun StorEdge 9980

Sun Microsystems, Inc. 4150 Network Circle, Santa Clara, CA 95054 USA **Phone** +1-800-555-9SUN or +1-650-960-1300 **Web** sun.com

Sun microsystems
We make the net work.

Doc 6

13.512

Rack-optimized 1U storage with faster data access and increased scalability and versatility—at no extra cost.

Sun StorEdge™ S1 Array

HIGHLIGHTS

- **Delivers a variety of key enhancements to the Netra™ st D130 array, including:**
  - **160-MB/sec. Ultra3 SCSI low voltage differential**
  - **Daisy chain up to four devices**
  - **12-meter cabling**
- 1U form factor and variety of rack-mounting options enable system to fit 19-inch, 23-inch, 24-inch, and 600-mm racks
- System takes in air from the front and exhausts to the back, for quicker, more efficient cooling
- Increased manageability with Lights-Out Management and Storage Subsystem Manager software, which allows remote monitoring of enclosure, drives, and temperature
- Front and back LEDs and front-accessible hot-swap disks enhance serviceability
- AC and DC power options and ruggedized, NEBS Level-3 packaging are ideal for deployment in a variety of powering environments and under less than ideal environmental conditions
- Compatible with a wide variety of Sun servers including Sun Netra; backward compatible with the Netra st D130 array
- Ideal incremental storage solution for all three tiers of an Internet architecture

Purchase this product from the Sun™ Store, sun.com/store, or contact an authorized Sun reseller near you.

The Sun StorEdge™ S1 array is an ideal solution for rack-intensive environments where fast data transfers, efficient space utilization, and compatibility with a wide range of Sun™ servers are critical concerns. The device delivers excellent performance—up to 160-MB/sec. throughput—while its 1U form factor, compact footprint, and variety of rack options allow it to fit neatly into standard rack environments. The Sun StorEdge S1 array works with a variety of Sun Netra™ and general-purpose workgroup and enterprise servers. And together with Sun's other rack-optimized 1U servers and PCI system expander, the Sun StorEdge S1 array supports modular computing, helping companies to balance performance, storage capacity, and PCI connectivity—affordably.

A rack-optimized 1U storage array with exceptional versatility.

SUN STOREDGE S1 ARRAY SPECIFICATIONS

WORKGROUP AND ENTERPRISE STORAGE SOLUTIONS

ARCHITECTURE

Carrier features	Supports 19-in., 23-in., 24-in., and 600-mm rack configurations, with fixed-rail options Flame-resistant, fireproof metal enclosure NEBS Level-3 Certified
Status and sensors	Device and drive status information accessible from host server Front and rear LEDs for system and drive status
LVD/SE (160/40 MB/s) SCSI	Standard ANSI (X3.131-1994, X3.277-1996, SPI-3X3.252) Maximum cable length 12 meters for LVD and 3 meters for SE SCSI Direct connect to host on-board SCSI port with no host adapter

DISK DRIVES

Form factor	3.5-inch low-profile, LVD
Supported drives	18.2 GB or 36.4 GB, 10,000 rpm

SOFTWARE

Operating system	Solaris™ 2.6 Operating Environment and higher Sun™ Cluster 3.0 (with Netra T1 AC200/DC200, Netra E1 PCI System Extender, and Sun StorEdge S1 array) Remote monitoring through Storage Subsystem Manager software

SUPPORTED PLATFORMS

Servers	Netra T1 AC200/DC200 Netra t 1120/1125 Netra t 1400/1405 Netra ct 400/800 Sun Enterprise™ 220R/420R Sun Fire™ 280R Sun Fire 15K

ENVIRONMENT

Power	AC or DC
AC power	100–240 V AC, single-phase (47–63 Hz)
DC power	-48/-60 V DC
Input current	Less than 2 A at 100 V AC (150 W) Less than 4 A at -40 V DC (150 W)
Operating temperature	5° C to 40° C (41° F to 104° F), 5% to 85% relative humidity, noncondensing (not to exceed 0.024 kg water/kg of dry air)
Short-term operating temperature	-5° C to 55° C (23° F to 131° F), 5% to 90% relative humidity, noncondensing (not to exceed 0.024 kg water/kg of dry air)
Nonoperating temperature	-40° C to 70° C (-40° F to 158° F), 90% maximum relative humidity, noncondensing
Acoustic noise	Less than 60 dBa (GR-63-CORE Test Method)
Seismic	Meets GR-63-CORE requirements for earthquake risk zone 4
Heat output	150 W, 512 BTUs/hr

REGULATIONS

Meets or exceeds the following requirements:

Safety	UL/CSA-60950, EN60950, IEC950 CB Scheme with all country deviations
RFI/EMC	EN55022/CISPR22 Class B, FCC CFR47 Part 15 Class B, EN61000-3-2, EN61000-3-3, EN 300 386 V1.2.1 (2000-03)—Telecom Center Only
Immunity	EN55024, EN 300 386 V1.2.1 (2000-03)—Telecom Center Only
Telcordia NEBS	GR-63-CORE, GR-1089-CORE, SR-3580 Level-3
Regulatory markings	CE, FCC, ICES-003, C-tick, VCCI, GOST-R, BSMI, EK, UL/cUL, TUV-GS,
Telcordia	NEBS Level-3

KEY APPLICATIONS

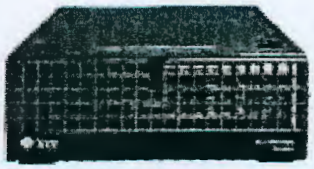
Tier 1	Web caching Video streaming Domain name service Incremental storage for horizontal scaling Firewall Web hosting Authentication
Tier 2	Simple boot device Incremental storage for application servers Mail/messaging Network management Softswitch Billing
Tier 3	Simple redundant boot device

DIMENSIONS AND WEIGHT

Height	44 mm (1.73 in.)
Width	436 mm (17.16 in.)
Length	450 mm (17.71 in.)
Weight (with drives)	8.8 kg (19.4 lb.)

Sun StorEdge MultiPack-FC Array

Sun StorEdge D240 Media Tray



Sun StorEdge D1000 Array

Sun StorEdge A1000 Array

Sun StorEdge T3 Array

Certified Excellence

Telcordia Technologies Certified servers
NEBS LEVEL 3 GR-2064, ISSUE 1
www.telcordia.com

Certified Excellence (and Design) is a certification mark of Telcordia Technologies (formerly Bellcore)

For additional information on this product go to:

www.sun.com/storage/workgroup/S1

HEADQUARTERS SUN MICROSYSTEMS, INC., 901 SAN ANTONIO ROAD, PALO ALTO, CA 94303-4900 USA
PHONE: 650 960-1300 OR 800 555-9SUN INTERNET: www.sun.com

Sun microsystems

take it to the n[th]

SALES OFFICES

AFRICA (NORTH, WEST, AND CENTRAL): +9714-3366333 • ARGENTINA: +5411-4317-5600 • AUSTRALIA: +61-2-9844-5000 • AUSTRIA: +43-1-60563-0 • BELGIUM: +32-2-704-8000 • BRAZIL: +55-11-5187-2100 • CANADA: +905-477-6745 • CHILE: +56-2-3724500 • COLOMBIA: +571-629-2323 • COMMONWEALTH OF INDEPENDENT STATES: +7-502-935-8411 • CZECH REPUBLIC: +420-2-3300-9311 • DENMARK: +45 4556 5000 • EGYPT: +202-570-9442 • ESTONIA: +372-6-308-900 • FINLAND: +358-9-525-561 • FRANCE: +33-01-30-67-50-00 • GERMANY: +49-89-46008-0 • GREECE: +30-1-618-8111 • HUNGARY: +36-1-202-4415 • ICELAND: +354-563-3010 • INDIA: +91-80-5599595 • IRELAND: +353-1-8055-666 • ISRAEL: +972-9-9710500 • ITALY: +39-039-60551 • JAPAN: +81-3-5717-5000 • KAZAKHSTAN: +7-3272-466774 • KOREA: +822-2193-5114 • LATVIA: +371-750-3700 • LITHUANIA: +370-729-8468 • LUXEMBOURG: +352-49 11 33 1 • MALAYSIA: +603-264-9988 • MEXICO: +52-5-258-6100 • THE NETHERLANDS: +00-31-33-45-15-000 • NEW ZEALAND: +64-4-499-2344 • NORWAY: +47 23 36 96 00 PEOPLE'S REPUBLIC OF CHINA: BEIJING: +86-10-6803-5588; CHENGDU: +86-28-619-9333; GUANGZHOU: +86-20-8755-5900; SHANGHAI: +86-21-6466-1228; HONG KONG: +852-2202-6688 • POLAND: +48-22-8747800 • PORTUGAL: +351-21-4134000 • RUSSIA: +7-502-935-8411 SINGAPORE: +65-438-1888 • SLOVAK REPUBLIC: +421-7-4342 94 85 • SOUTH AFRICA: +2711-805-4305 • SPAIN: +34-91-596-9900 • SWEDEN: +46-8-631-10-00 • SWITZERLAND: GERMAN: 41-1-908-90-00; FRENCH: 41-22-999-0444 • TAIWAN: +886-2-2514-0567 • THAILAND: +662-636-1555 TURKEY: +90-212-335-22-00 • UNITED ARAB EMIRATES: +9714-3366333 • UNITED KINGDOM: +44-1-276-20444 • UNITED STATES: +1-800-555-9SUN OR +1-650-960-1300 • VENEZUELA: +58-2-905-3800 • WORLDWIDE HEADQUARTERS: +1-800-555-9SUN OR +1-650-960-1300

LFC1.8 Printed in USA 9/01 DE1506-0/15K

[Return to Non Printer Friendly Page]

Sun StorEdge[tm] S1 Array: Hardware Specifications

Disks	
18GB	Fujitsu MAN3184MC (18.2GB - 10000 RPM) Seagate ST318305LC (18.2GB - 10000 RPM)
36GB	Seagate ST336605LC (36.4GB - 10000 RPM) Fujitsu MAN3367MC (36.4GB - 10000 RPM)
73B	Seagate ST373307LC (73.4GB - 10000 RPM)
Racking	
Supports 19-in., 23-in., 24-in., and 600-mm rack configurations, with fixed-rail options	
Standard Interfaces	
LVD/SE SCSI	Two ports, 160/40 MB/s Standard ANSI (X3.131-1994, X3.277-1996, SPI-3X3.252) Maximum cable length 12 meters for LVD and 4 meters for SE SCSI Direct connect to host on-board SCSI port with no host adapter
Environment	
AC input voltage	100-240 VAC, 47-63 Hz
DC input voltage	-48 TO -60 VDC
Input power	150 W
Input current	Less than 2A at 100VAC (150W) Less than 4A at -40 VDC (150W)
Heat output	512 BTU/hr
Temperature [1]	**Operating:** 5° C to 40° C (41° F to 104° F) **Operating(short term):** -5° C to 55° C (23° F to 131° F) **Nonoperating:** -25° C to 65° C (-13° F to 149° F)
Humidity [1]	**Operating:** 5% to 85% relative humidity, non-condensing **Operating(short term):** 5% to 95% relative humidity, non-condensing **Nonoperating:** 5% to 95% relative humidity, non-condensing
Altitude	**Operating:** 0 m to 3000 m (0 ft. to 10,000 ft.) **Nonoperating:** 0 m to 12,000 m (0 ft. to 40,000 ft.)
Acoustic noise	**Operating:** 6.0 Bels

	Idling: 6.0 Bels
Seismic	Meets GR-63-CORE requirements for earthquake risk zone 4
Number of cords	1
Plug type - U.S.	NEMA 5-15P
1 - short term is defined as operating 96 consecurtive hours	
Regulations **Meets or exceeds the following requirements:**	
Safety	UL/CSA-60950, EN60950, IEC950 CB Scheme with all country deviations
RFI/EMI	EN55022/CISPR22 Class B, FCC CFR47 Part 15 Class B, EN61000-3-2, EN61000-3-3, EN 300 386 V1.2.1 (2000-03) - Telecom Center Only
Immunity	EN55024, EN 300 386 V1.2.1 (2000-03) - Telecom Center Only
Telcordia NEBS	GR-63-CORE, GR-1089-CORE, SR-3580 Level-3
Regulatory Markings	CE, FCC, ICES-003, C-tick, VCCI, GOST-R, BSMI, EK, UL/cUL, TUV-GS
Telcordia	NEBS Level-3
Dimensions and Weights	
Height	44 mm (1.73 in.)
Width	436 mm (17.16 in.)
Depth	450 mm (17.71 in.)
Weight	5.9 kg (13 lb.) without drives 8.8 kg (19.4 lb.) with drives

Sun Documentation on the Web

The docs.sun.com[sm] web site enables you to access Sun technical documentation on the Web. You can browse the docs.sun.com archive or search for a specific book title or subject at:

http://docs.sun.com

Sun Welcomes Your Comments

We are interested in improving our documentation and welcome your comments and suggestions. You can email your comments to us at:

docfeedback@sun.com

Please include the part number of the document in the subject line of your email.

Please Recycle

Sun Microsystems, Inc. • 901 San Antonio Road • Palo Alto, CA 94303-4900
USA • 650 960-1300 • Fax 650 969-9131

Adobe PostScript

Part Number: 816-1112-10
Revision A, April 2001

36 Gbyte, 1 –Inch, 10K rpm Disk Drive Specifications

SCSI Interface

Sun microsystems

Disk Drive Installation

For information on how to install your disk drive, refer to your system or drive enclosure documentation.

See "Sun Documentation on the Web" on the back page if you need to order any documentation.

Drive Specifications

Power Requirements

Activity	+5 VDC (±5%)	+12 VDC (±7%)
Motor start	1.0A	2.5A
Max Operating (Random IOs)	1.3A	1.6A
Idle	1.0A	0.8A

Physical Characteristics

Height	Width	Depth	Weight
1.00 in	4 in	5.75 in	1.3 lb
25.4 mm	101.6 mm	146 mm	0.6 kg

Performance

Attribute	Value
Capacity, formatted	36,420,074,496 bytes minimum 71,132,958 blocks (512 bytes per sector)
Seek times (read/write)	
Single track seek	0.7msec / 0.9 msec
Average seek	5.6 msec / 6.0 msec
Maximum seek	10.0 msec / 10.5 msec
Rotational latency	
Maximum	5.99 msec (10,025 rpm)
Average	2.99 msec
HDA data transfer rate	
Disk to read buffer	35.0 Mbytes per sec minimum
Interface transfer rate	narrow / wide / ultra/ LVD
Synchronous	10 to 160 Mbytes per sec
Asynchronous	5 to 20 Mbytes per sec
Start/stop	
Power up to ready	30 sec typical
Spin down	30 sec typical

Dcc (3

Sun microsystems

The versatile, high-speed adapter for reliable LAN and storage connectivity.

Sun™ Dual Fast Ethernet + Dual SCSI PCI Adapter

HIGHLIGHTS

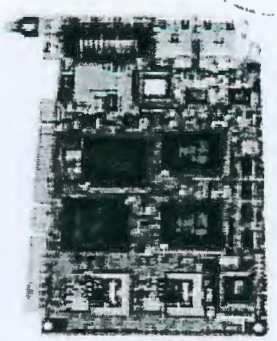
- Provides two independent FastEthernet ports (dual RJ-45) and two independent 80-MB/sec. Ultra SCSI-2 ports (dual VHDCI) on a single 32/64-bit, 33/66-MHz PCI card
- Supports single-ended and low-voltage differential signaling for use of longer cables
- Auto-negotiation capability allows immediate connection to existing 10-Mb/sec. Ethernet or migration to 100-Mb/sec. FastEthernet
- Supports load balancing for RX packets among multiple CPUs
- Features dynamic reconfiguration, redundancy, and failover support for high availability
- Provides built-in bootable drivers (Solaris™ 8 Operating Environment, update 7 only)
- Supports 3.3-V or 5-V PCI slots (universal)
- Features low CPU utilization for efficient use of server resources and bandwidth
- Compliant with IEEE 802.3u for interoperability
- Supports infinite burst capabilities (on UltraSPARC™ III processor-based servers only)

Today's enterprise and Internet data center environments demand high-speed, high-density, affordable solutions for attaching to both LAN environments and storage devices. And Sun meets that demand with the Sun™ Dual Fast Ethernet + Dual SCSI PCI adapter. The adapter features four ports on a single, full-size PCI card—two FastEthernet ports for LAN connectivity and two Ultra SCSI-2 ports for attaching to SCSI-2 compliant peripherals—which saves valuable slots and lowers cost of ownership by simplifying service and support. Plus, the Sun Dual Fast Ethernet + Dual SCSI PCI adapter supports universal PCI powering environments, features 64-bit ASICs for improved bus operation, and accommodates single-ended and low-voltage differential signaling—for an extremely versatile solution. And its auto-negotiation capabilities provide backward compatibility with 10-BaseT Ethernet environments, for outstanding investment protection.

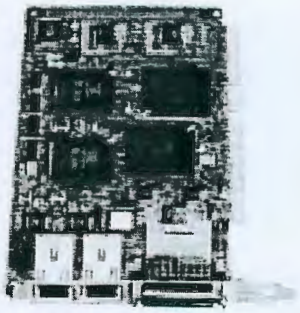
Purchase these products from the Sun™ Store, sun.com/store or contact an authorized Sun reseller near you.

SUN DUAL FAST ETHERNET + DUAL SCSI PCI ADAPTER

Enterprises and Internet data centers alike look to Sun to provide high-performance, versatile, highly reliable networking solutions. The Sun Dual Fast Ethernet + Dual SCSI PCI adapter delivers two FastEthernet ports and two SCSI ports on a single PCI card—for reliable performance with minimal downtime and lower total cost of ownership.



Back



Front

SUN DUAL FAST ETHERNET + DUAL SCSI PCI ADAPTER SPECIFICATIONS

PERFORMANCE

PCI clock	Maximum 33/66 MHz
PCI data burst transfer rate	Up to 64-byte bursts
SCSI synchronous transfer rate	80 MB/sec.
SCSI asynchronous transfer rate	Maximum 12 MB/sec. (16-bit) Maximum 6 MB/sec. (8-bit)
Transfer size	Maximum 4 GB
PCI data/address lines	AD31-0 or AD63-0
PCI modes	Master/slave
SCSI interface	Single-ended (SE) Low Voltage Differential (LVD)
SCSI bus parity	Yes
SCSI 8-bit bus devices	Yes
SCSI 16-bit bus devices	Yes
10-BaseT transfer rate	Up to 10 Mb/sec.
100-BaseT transfer rate	Up to 100 Mb/sec.

HARDWARE SUPPORTED

Servers	
Sun Ultra™	30, 60, 80
Sun Enterprise™	220R, 420R, 250, 450, 280R, 480R, 880R, E10K, E15K
Sun Blade™	100, 1000
Sun Fire™	4800, 4810, 6800
StorEdge™	S1
Peripherals	All Sun-supported SCSI-2 devices

SOFTWARE SUPPORTED

Operating environment	Solaris Operating Environment 8, update 7 and higher
Firmware	OpenBoot™ PROM 3.0 and higher
Diagnostic	SunVTS™ 4.4 and higher

POWER REQUIREMENTS

Power consumption	Maximum 10 W
Voltage	3.3 V and 5 V

DIMENSIONS AND WEIGHT

Length	175 mm (6.8 in.)
Width	107 mm (4.2 in.)

HEADQUARTERS SUN MICROSYSTEMS, INC., 901 SAN ANTONIO ROAD, PALO ALTO, CA 94303-4900 USA
PHONE: 650 960-1300 OR 800 555-9SUN INTERNET: www.sun.com

Sun microsystems

take it to the nth

SALES OFFICES

AFRICA (NORTH, WEST AND CENTRAL): +9714-3366333 • ARGENTINA: +5411-4317-5600 • AUSTRALIA: +61-2-9844-5000 • AUSTRIA: +43-1-60563-0 • BELGIUM: +32-2-704-8000 • BRAZIL: +55-11-5187-2100 • CANADA: +905-477-6745 • CHILE: +56-2-3724500 • COLOMBIA: +571-629-2323 • COMMONWEALTH OF INDEPENDENT STATES: +7-502-935-8411 • CZECH REPUBLIC: +420-2-3300-9311 • DENMARK: +45 4556 5000 • EGYPT: +202-570-9442 • ESTONIA: +372-6-308-900 • FINLAND: +358-9-525-561 • FRANCE: +33-01-30-67-50-00 • GERMANY: +49-89-46008-0 • GREECE: +30-1-618-8111 • HUNGARY: +36-1-202-4415 • ICELAND: +354-563-3010 • INDIA: +91-80-5599595 • IRELAND: +353-1-8055-666 • ISRAEL: +972-9-9710500 • ITALY: +39-039-60551 • JAPAN: +81-3-5717-5000 • KAZAKHSTAN: +7-3272-466774 • KOREA: +822-2193-5114 • LATVIA: +371-750-3700 • LITHUANIA: +370-729-8468 • LUXEMBOURG: +352-49 11 33 1 • MALAYSIA: +603-264-9988 • MEXICO: +52-5-258-6100 • THE NETHERLANDS: +00-31-33-45-15-000 • NEW ZEALAND: +64-4-499-2344 • NORWAY: +47 23 36 96 00 PEOPLE'S REPUBLIC OF CHINA: BEIJING: +86-10-6803-5588; CHENGDU: +86-28-619-9333; GUANGZHOU: +86-20-8755-5900; SHANGHAI: +86-21-6466-1228; HONG KONG: +852-2202-6688 • POLAND: +48-22-8747800 • PORTUGAL: +351-21-4134000 • RUSSIA: +7-502-935-8411 SINGAPORE: +65-438-1888 • SLOVAK REPUBLIC: +421-7-4342 94 85 • SOUTH AFRICA: +2711-805-4305 • SPAIN: +34-91-596-9900 • SWEDEN: +46-8-631-10-00 • SWITZERLAND: GERMAN: 41-1-908-90-00; FRENCH: 41-22-999-0444 • TAIWAN: +886-2-2514-0567 • THAILAND: +662-636-1555 TURKEY: +90-212-335-22-00 • UNITED ARAB EMIRATES: +9714-3366333 • UNITED KINGDOM: +44-1-276-20444 • UNITED STATES: +1-800-555-9SUN OR +1-650-960-1300 • VENEZUELA: +58-2-905-3800 • WORLDWIDE HEADQUARTERS: +1-800-555-9SUN OR +1-650-960-1300

SUN™

10/01

Tel (8)

Sun StorEdge™
Complete Storage Solutions

On the Web | www.sun.com/storage

Sun StorEdge™ 2 Gb PCI Single and Dual Fibre Channel Network Host Bus Adapter (HBA)

Product Brief

The Sun StorEdge™ 2 Gb PCI Single and Dual Fibre Channel Network Host Bus Adapter (HBA) has been optimized for peak performance and real-world scalability in storage area networks (SANs). Engineered for maximum bandwidth, our HBA eliminates host bus bottlenecks that may impede the high-performance of 2 Gb Fibre Channel and creates a balanced solution. With support for multiple protocols—SCSI, IP, and FC-Tape—our HBA is optimized for high-speed data movement and system management, providing the flexibility needed to run complex storage networks. Sun StorEdge™ Traffic Manager software helps dramatically simplify administration by providing superior SAN-wide failover and load balancing between HBAs to improve availability and address storage growth without adding complexity.

Sun StorEdge Complete Storage Solutions—providing you with comprehensive hardware, software, and services to solve your business challenges enterprise-wide.

High data transfer rate
Supports up to 400 MB/sec Fibre Channel data transfer rates in Full Duplex mode.

Choice of models
Single- and Multi-channel models.

Hands-off management
Automatically negotiates Fibre Channel bit rate (1 or 2 Gb).

Complete compatibility
Backwards compatible with standard 33- and 66-MHz PCI.

Specifications

Fibre Channel chip	QLogic ISP2312A (single-port card) QLogic ISP2342A (dual-port card)
RAM (per Fibre Channel port)	256 KB
Onboard intelligence	Single chip engine includes enhanced RISC processor, Fibre Channel Protocol manager, PCI DMA controller, 2 Gb transceivers, and on-chip frame buffers.
Topology	FC-AL, Point-to-Point, Fabric
Fabric support	F-Port
Class of service	Class 3
Transfers	Full Duplex in point-to-point and fabric topologies.
Protocols	SCSI, FCP2 (FC-Tape), IP
Host bus	Conforms to PCI-X Specification 1.0 and PCI Local Bus Specification 2.2.
FC data transfers	Up to 400 MB/sec per channel with Full Duplex.

Power Consumption	
Single-channel PCI	< 6 Watts
Dual-channel PCI	< 12 Watts
Form Factor	
Standard half card PCI	6.875" x 4.200"
3U compact PCI	6.600" x 2.536"
Environment	
Operating	0° C to 55° C (32° F to 131° F) 5% to 90% relative humidity, noncondensing
Nonoperating	-20° C to 65° C (-40° F to 149° F) 0% to 95% relative humidity, noncondensing
Host Software	
Software drivers	PCI: Sun StorEdge Network Foundation Software 6.0

Document ID: ID41665
Synopsis: Sun[TM] GigaSwift Gigabit Ethernet Adapters - Further Information

Description Top

Document Body Top

GigaSwift Gigabit Ethernet Further Information

- Gigabit Ethernet is the IEEE standard for Ethernet with 1000 Mbit/s.
- Full Duplex operation allows simultaneous traffic in each direction, so the aggregate bandwidth is 2GBit/s.
- GigaSwift is the third generation of Sun gigabit ethernet products.
- It operates on both, fiber and copper cable.
- GigaSwift supports VLANs, it can decode VLAN tagged packets
- Older products are Gigabit Ethernet 1.x (vge) and Gigabit Ethernet 2.x/3.x (ge).
- Purpose
  - provide a "big pipe" for server connections to many clients or to backup systems.
  - provide services to different VLANS over one interface. GigaSwift can decode VLAN tagged packets.
  - Hardware TCP/UDP checksum generation, packet parsing and interrupt coalescing reduce CPU processing for increased server efficiency
  - Additionally, the SunSwitch is available.
- Common Standards
  - IP Versions 4 and 6
  - IEEE 802.1d - Quality of Service
  - IEEE 802.1p - Priority Tagging
  - IEEE 802.1q - VLAN Tagging
  - IEEE 802.3ab - 1000Base-TX over Category 5 UTP copper cable.
  - IEEE 802.3u - Fast Ethernet including Autonegotiation (100Mbit/s)
  - IEEE 802.3z - 1000Base-SX overFiber
  - IEEE 802.3x - Ethernet Flow Control (sender and receiver side)
  - Hardware Details

- UTP NIC
  - Dynamic Reconfiguration and redundancy/failover support
  - 6.8inch x 4.2 inch short card
  - Load balancing for received packets among multiple CPUs
  - Does not support 1000 Mbit/s half duplex support (normally not needed)
  - Hardware TCP/UDP checksum generation, packet parsing and interrupt coalescing reduce CPU processing for increased server efficiency
  - Sun developed ASIC and Adapter
  - Standards our NIC applies to
    - IEEE 802.3ab (UTP NIC), 802.3z (Fiber NIC), 802.3u, 802.3x, 802.1q, 802.1p, 802.1d
    - special SNMP MIB
    - IPv4 and IPv6 support
    - PCI 2.2 33/66 MHz, 32 or 64 bit bus master

- Abbreviations/Acronyms
  - IEEE - Institute of Electrical and Electronics Engineers, Inc., standardizes Ethernet
  - Jumbo Frame - An Ethernet frame which is larger than 1518 bytes (9K bytes).
  - NIC - Network Interface Card
  - VLAN - Virtual LAN, the ability to have several independent net segments within one hardware.
  - LAN - Local Area Network, network which is geographically limited (typically to a 1 km radius, e.g. within a building)

Versions

- Hardware
  - Available Hardware Versions

Table 1. Hardware

Version	Mkt Part#	Part#	Comment
1.0	X1150A	501-5902	PCI copper UTP Adapter
1.0	X1151A		PCI Multimode Fiber Adapter
1.0	X1261A	501-5523	cPCI 3U Multimode Fiber Adapter

1.0	X2222A	501-5727	100 Mbit/s dual UTP/SCSI PCI Combo
1.0	A37	501-5819	SunFire V480 On-board 1000 Mbit/s

- How to Determine Hardware Version prtconf -pv | grep SUNW,pci-ce

- Software
  - Packages
    - SUNWced - Sun GigaSwift Ethernet Adapter (32-bit Driver)
    - SUNWcedx - Sun GigaSwift Ethernet Adapter (64-bit Driver)
    - SUNWce - Sun GigaSwift Ethernet Adapter Driver Headers
    - SUNWcem - Sun GigaSwift Ethernet Adapter Driver Man Pages
    - SUNWcea - Sun GigaSwift Ethernet Adapter Driver 32 bit adb Macros
    - SUNWceax - Sun GigaSwift Ethernet Adapter Driver 64 bit adb Macros
    - SUNWvld - VLAN utility routines (32-bit, for 5.8)
    - SUNWvldx - VLAN utility routines (64-bit, for 5.8)
    - SUNWvldx - VLAN utility headers (for 5.8)
  - How to Determine Product Version Number: pkginfo -l SUNWced | grep VERSION
  - How to Determine Driver Version Number: modinfo | grep CE or strings /kernel/drv/ce | grep CE or strings /platform/sun4u/kernel/drv/ce | grep CE

- Driver Versions Table

Table 2. Driver Versions

Version	Comment/Availability
1.87	GigaSwift 1.0 CD Part# 704-7117-10 (Jan.01)
1.105	Solaris 8 4/01
1.109	Solaris 8 10/01, GigaSwift 1.0u1 CD (Nov.01)
1.115	Solaris 9 FCS

Compatibility

- Hardware Compatibility

Table 3. Hardware Compatibility

supported Architecture	max # of cards	Comment			
	UTP	Fiber	cPCI	Combo	

Ultra 5,10	1	1		systems without graphic card
Ultra 60, E250	1	1		
Ultra 80	1	2		
E 220R	2	1		
E280R, E420, E450	2	2		
3x00-6x00	2	4		Use shielded UTP cable
E10K	TBD	X		
Netra 20	X			
Netra t1		X		
Netra t 112x	1	1		
Netra t 140x, AC/DC200	1			
Blade 100	1	1		
Blade 1000	2	2		
V480	X	X		
V880	4	4		
F 3800			4	cPCI X1261A, only
F 48x0,6800	X	X	4	
F12k,15k	6	X		

Key:
X - supported, max Number of cards not yet defined.
recommended CPU power:
500MHz per adapter, with a minimum of one 167MHz to handle interrupts. For max throughpı

- Software Compatibility Matrix A complete list of patches can be found on sunsolve.sun.com

Table 4. Software Compatibility

	Product Version
O/S	1.0
4.x	N/S
2.4	N/S
2.5	N/S
2.5.1	N/S
2.6	112327-NN
7*32	112327-NN
7*64	112327-NN
8	111883-NN
9	xxxxxx-NN

Key:
N/S - Product not supported on this OS
N/P - No patch applicable for this OS
N/A - Not Available
7*32 - Solaris 7 - 32 bit kernel

```
7*64 - Solaris 7 - 64 bit kernel
xxxxxx-NN means there is no patch for this version yet
```

Installation/Configuration Details

- Cabling
  - Fiber cable: Multimode Fiber 62.5um (max 260m) or 50um (max 550m), SC connector Part numbers: 2m - 537-1004, 5m - 537-1020, 15m 537-1006
  - Copper cable: Category 5, tested for Gigabit connections, max 100m, RJ45 connector
- Configuration Files Location
  - /etc/hostname.ce<instance number> - IPv4 address and interface config
  - /etc/hostname6.ce<instance number> - IPv6 address and interface config, Solaris 8
  - /etc/hostname.ce<vlan-tag><instance number> - VLAN interface config, IPv4 (for 5.8)
  - /etc/hostname6.ce<vlan-tag><instance number> - VLAN interface config, IPv6 (for 5.8)
  - /kernel/drv/ce.conf - can be used for Operational Mode parameter settings
  - /etc/system - can be used for Operational Mode parameter settings
  - /etc/path_to_inst - automatically generated to map hardware and driver
- Important configuration commands (short overview)
  - ifconfig - configure IP interface online
  - eeprom local-mac-address?=true - use unique onboard ethernet address
  - /usr/sbin/ndd -set /dev/ce - change Operational Mode parameters online
- More config tips
  - Use S68net-tune script to change Operational Mode parameters.
- Config file examples
  - /etc/system can NOT be used
  - /etc/path_to_inst is generated on boot -r to map hardware and driver

    path

    ```
    # grep ce /etc/path_to_inst
    "/pci@1f,2000/pci@1/network@0" 0 "ce"
    ```

  - /etc/hostname.ce<vlan-tag><instance number> - VLAN interface config

- VLAN packages are available for SunOS 5.8, only
- The hostname in this file should be found in /etc/hosts
- The VLAN tag must be the same on the link partner side (switch, other system)

```
                    instance # (last 3 digits, value=0 -> uses ce0 interface)
                    |||
/etc/hostname.ce123000
                      |||
                      VLAN tag (digit 4 and higher, value=123)
```

VLAN

```
# cat /etc/hostname.ce1000
lab058-enet11
# grep lab058-enet11 /etc/hosts
172.16.24.58    lab058-enet11
lab058# ifconfig ce1000
```

- Configure Ethernet Flow Control (802.3x)
  - Check out User's Guide Chapter 4, Configuring Driver Parameter - Flow Control Parameters.
  - use ndd command to enable sending and receiving of pause frames

NDD

```
# ndd -set /dev/ce adv_pause_cap 1
# ndd -set /dev/ce adv_autoneg_cap 0
```

  - enable sending and receiving of pause frames on the other side (switch)

Pause Frames

```
cat5500> (enable) set port flowcontrol 8/5 send on     (Example for a Cisco Catalys
Port 8/5 flow control send administration status set to on
(port will send flowcontrol to far end)
cat5500> (enable) set port flowcontrol 8/5 receive on
Port 8/5 flow control receive administration status set to on
(port will require far end to send flowcontrol)
```


  - check (on both sides) if setting was successful and is used

Setting

```
# kstat -p ce | grep link | grep pause
ce:0:ce0:link_asmpause  0
ce:0:ce0:link_pause     1
```

  - if setting was not successful, try to unplug/replug the cable or to disable/enable autonegotiation.
  - Use boot script to set parameters while booting.

FAQ

1. What can I do when the link does not come up?
   - Check Operational Mode settings (see below) and Hardware, see Troubleshooting)
2. How do I see the actual Operational Mode settings ?
   - Check link_ parameters of netstat -k ce[your_interface.number]
     - link_up - 0 down, 1 up
     - link_speed - speed in Mbit/s
     - link_duplex - 1 half duplex, 2 full duplex, 0 down

     This parameters must show the same values on both sides. If not, Autonegotiation does not work.

What can I do when Autonegotiation does not work ?

   - You can disable Autonegotiation and set the correct Operational Mode values yourself on both sides. This is called "Forced Mode".

4. How do I disable Autonegotiation ?
   - Use S68net-tune script to change Operational Mode parameters or ndd -set /dev/ce, see Troubleshooting
5. Is it OK if all MAC addresses are the same ?
   - In most modern networks, this will cause problems. (packet loss, low performance) To avoid this set eeprom local-mac-address\?=true and reboot.
6. The Link does not come up or has problems when connected to Cisco switch
   - Some Cisco switches (e.g. Catalyst 6500) have Autonegotiation disabled by default. This is not according to the IEEE 802.3z standard. To get the connection running, set both sides either to forced 1000 Mbit/s Full Duplex or enable Autonegotiation on the switch.
7. Does ce support Jumbo Frames ?
   - This feature can be implemented in the ce driver on request within a Sun Professional Services project. Such a driver will not be supported through the usual support channels.
8. Can I boot over gigabit ethernet?
   - Yes. Use the ce device path to boot. Autonegotiation to the link partner (switch) must be enabled and working, since you can not play with operational modes of the NIC in boot prom. To boot correctly, the SUNWce* packages must be installed on the boot server. That means, the boot image as well as the install base directory must contain the ge driver.

Driver

```
{0} ok show-nets
```

```
a) /pci@1f,4000/pci@2/network@0
...
q) NO SELECTION
Enter Selection, q to quit: a
a) /pci@1f,4000/pci@2/network@0 has been selected.
Type ^Y ( Control-Y ) to insert it in the command line...
{0} ok boot /pci@1f,4000/pci@2/network@0
.......
```

1. How do I see the Operational Mode settings ?

   - The driver distinguishes between 4 types of settings :

     - **"advertized"** - configurable Operational Mode parameters, will be used on next negotiation. Use show_ce.sh or ndd /dev/ce to read this driver parameters. To select the interface you want to check, use ndd -set /dev/ce instance [your_interface.number] The parameter names begin with adv_
     - **"capabilities"** - the hardware capabilities. The settings can be read with netstat -k ce [your_interface.number]. The parameter names begin with cap_.
     - **"link partner capabilities"** - the settings as the link partner reported them. Invalid when Autonegotiation was off on one side. The settings can be read with netstat -k ce [your_interface.number] The parameter names begin with lp_cap_.
     - **"actual mode"** - the actual used parameters. link_ parameters of netstat -k ce [your_interface.number]

2. How can I find out the current PCI bus speed ?

   - Type /usr/platform/[platform]/sbin and locate SUNW,pci-ce

Bus Speed

```
...
========================= IO Cards =========================
     Bus   Freq
Brd  Type  MHz   Slot  Name                        Model
---  ----  ----  ----  ----------------------  -----------
SYS   PCI    66     2   pciclass,020000  SUNW,pci-ce
```


Information Gathering

Things to get:	Comment:
Do you suspect a problem concerning Gigabit Ethernet or IP ?	If IP, the GBE part may not k
network topology plan	What is connected to what? (c
The other side: link partner	e.g. Sun, repeater, switch (t
Sun System (*)	machine type
card version ? (*)	try prtconf -pv | grep SUNW,p
Software Version (*)	pkginfo -l SUNWced | grep VER

Are recommended patches installed ? (*)

connection completely down or is some traffic possible ?

Did it work once ?	YES - Are there changes in SW NO - Is it an installation/cc
Are there error messages ? (*)	/var/adm/messages, /var/log/syslog
Does netstat -k ce[if#] show any errors ? (*)	ierrors oerrors late_coll
Config Files:	/etc/hostname.ce*(*), /kernel/drv/ce.conf, /etc/system
IP config (*)	ifconfig -a; netstat -rvpn

Things to try:

Unique MAC addresses? (*)	in most cases eeprom local-m
Operational Mode configuration (*)	See FAQ
Operational Mode config of the link partner	See FAQ
Snoop suspected interface	e.g. snoop -d ce[if#] -o ce.
What do the LEDs on the Board show ?	
hardware test	See Troubleshooting

- information needed to assign to the next level of support:
  - Short failure description including error or warning messages
  - Short customer situation including timeframes and business impact
  - Platform, part# and revision of NIC, used SBUSor PCI slot (if obtainable)
  - Special commands (see above, if no explorer is available)
  - Special commands (see above, information is not collected by explorer)
  - Explorer output (or path to location)
  - Product gather output (or path to location)
  - Network overview (detailed sketch, cable lengths

- Where is a test machine connected (e.g. a "slow" client) ?
- Short description of your measures to find and solve the problem before the handover
- Use handover template to assign to next level

Installation/De-installation

- Installation
  - Hardware
    - Cabling:
      - Copper: max. 100m Category 5 (or better) Unshielded Twisted Pair (UTP), RJ-45 Plug.
      - Fiber: Multimode Fiber: max 260 62.5u or max 500m 50u, SC-Plug
  - Software
    - sample install log
- De-Installation
  - remove the packets, delete the config files, remove entries from /etc/hosts, etc., remove the card(s)

Troubleshooting

- Troubleshooting Info
  - Check LED state
    - PCI cards:

Table 5. PCI cards

Label	Colour	Meaning	Source
LINK QUALITY	Purple	Gigabit link quality good	PHY
1000X	Green	Link 1Gbit/s up	PHY
100X	Green	Link 100Mbit/s up	PHY
10X	Green	Link 10Mbit/s up	PHY
FDX	Green	Full Duplex Mode	PHY
FDX	Off	Half Duplex Mode	PHY
TX	Green	PHY Transmitting Data	PHY
RX	Green	PHY Receiving Data	PHY
TXM	Green	MAC Transmitting Data	MAC
RXM	Green	MAC Receiving Data	MAC

- compact PCI cards:

Table 6. PCI Cards

Label	Colour	Meaning	Source
HOT SWAP	Blue	Hot swap possible	

- Check Hardware on BootProm (if the Cable is connected properly)

BootProm

```
{0} ok setenv auto-boot? false necessary, if it was set to true
{0} ok reset all
{0} ok show-nets
a) /pci@1f,4000/pf@5
b) /pci@1f,4000/network@1,1
c) /pci@1f,4000/pci@2/network@0
q) NO SELECTION
Enter Selection, q to quit: c
/pci@1f,4000/pci@2/network@0 has been selected.
Type ^Y ( Control-Y ) to insert it in the command line.
e.g. ok nvalias mydev ^Y
         for creating devalias mydev for
/pci@1f,4000/pci@2/network@0
{0} ok test /pci@1f,4000/pci@2/network@0 (you can use ^Y for the path)
Testing /pci@1f,4000/pci@2/network@0
Internal loopback test -- succeeded.
Link is  -- up
{0} ok watch-net /pci@1f,4000/pci@2/network@0
Internal loopback test -- succeeded.
Transceiver check  -- passed
Looking for Ethernet Packets.
'.' is a Good Packet.  'X' is a Bad Packet.
Type any key to stop.
.......^C
{0} ok setenv auto-boot? true necessary, if it was set to true before
{0} ok
```

- Error Messages
  - /var/adm/messages : WARNING: ce0: xcvr addr:0x01 - link down - physical connection cut, link partner down or Autonegotiation failed

- Traces/Commands
  - netstat -k ge0 shows error statistics counters. Check the most important ones:
    - ierrors - should be smaller than 1% of ipackets
    - oerrors - should be smaller than 1% of opackets
    - late_collisions - Wrong Operational Mode settings or illegal network diameter
    - crc_err, code_violations - Corrupted incomig packets, should be smaller than 1% of ipackets
    - code_violations - Corrupted incomig packets, should be smaller than 1% of ipackets
  - Force Operational Mode when Autonegotiation fails: To select the interface you want to change,

use ndd -set /dev/ce instance [your_interface.number]. Then ndd -set /dev/ce to set the "advertized" (adv_) values. link_master must be 0 on one side and 1 on the other. Switches use 1, default for our card is 0.

Interface number

```
example: forced 1000 Mbit/s on an UTP
# ndd -set /dev/ce instance 0  <-- settings for ce0
# ndd -set /dev/ce link_master 0  <-- for switch connection
# ndd -set /dev/ce adv_1000fdx_cap 1
# ndd -set /dev/ce adv_1000hdx_cap 0
# ndd -set /dev/ce adv_100fdx_cap 0
# ndd -set /dev/ce adv_100hdx_cap 0
# ndd -set /dev/ce adv_10fdx_cap 0
# ndd -set /dev/ce adv_10hdx_cap 0
# ndd -set /dev/ce adv_autoneg_cap 0
```

Sometimes you must unplug and replug the connector to initialize Autonegotiation.

rmance

- Performance Tuning Hints
  - use a 66MHz, 64 bit PCI slot.
  - Select a slot that does not share bus bandwidth with other slots.
  - 4x 300 MHz CPUs needed for maximum performance.
  - For PCI performance, use Solaris 2.6 5/98 or later.
- Test Results
  - Tolly Group Test on a e6.5k/400MHz stated:
    - 940 Mbit/s unidirectional traffic, download (Solaris 8)
    - 925 Mbit/s unidirectional traffic, download (Solaris 7)
    - 848 Mbit/s bidirectional traffic (Solaris 7)
  - Performance should be measured with several ttcp streams.

References

- Manuals
  - Platform Notes: Sun GigaSwift Ethernet on docs.sun.com
- Other Important Links
  - GigaSwift on www.sun.com
  - Product Photos

CHAPTER 5

System Components

The sections in this chapter describes the major components used in the Sun Fire 15K/12K systems (FIGURE 5-1).

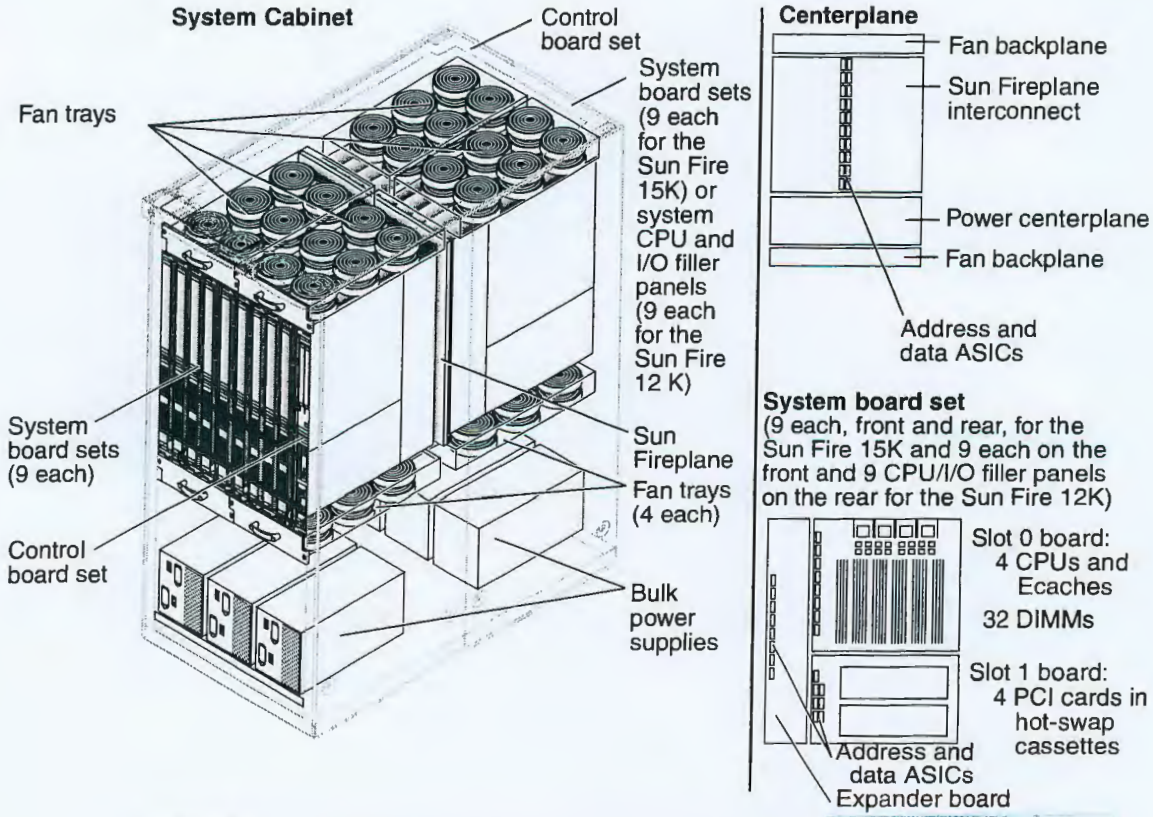


FIGURE 5-1 Sun Fire 15K/12K Systems Major Components

5.1 Cabinets

The Sun Fire 15K/12K systems can consist of two or more air-cooled cabinets: a system cabinet and one or more customer-selected I/O expansion racks (FIGURE 5-2). The system cabinet includes the CPU/Memory and system control peripherals, such as PCIs.

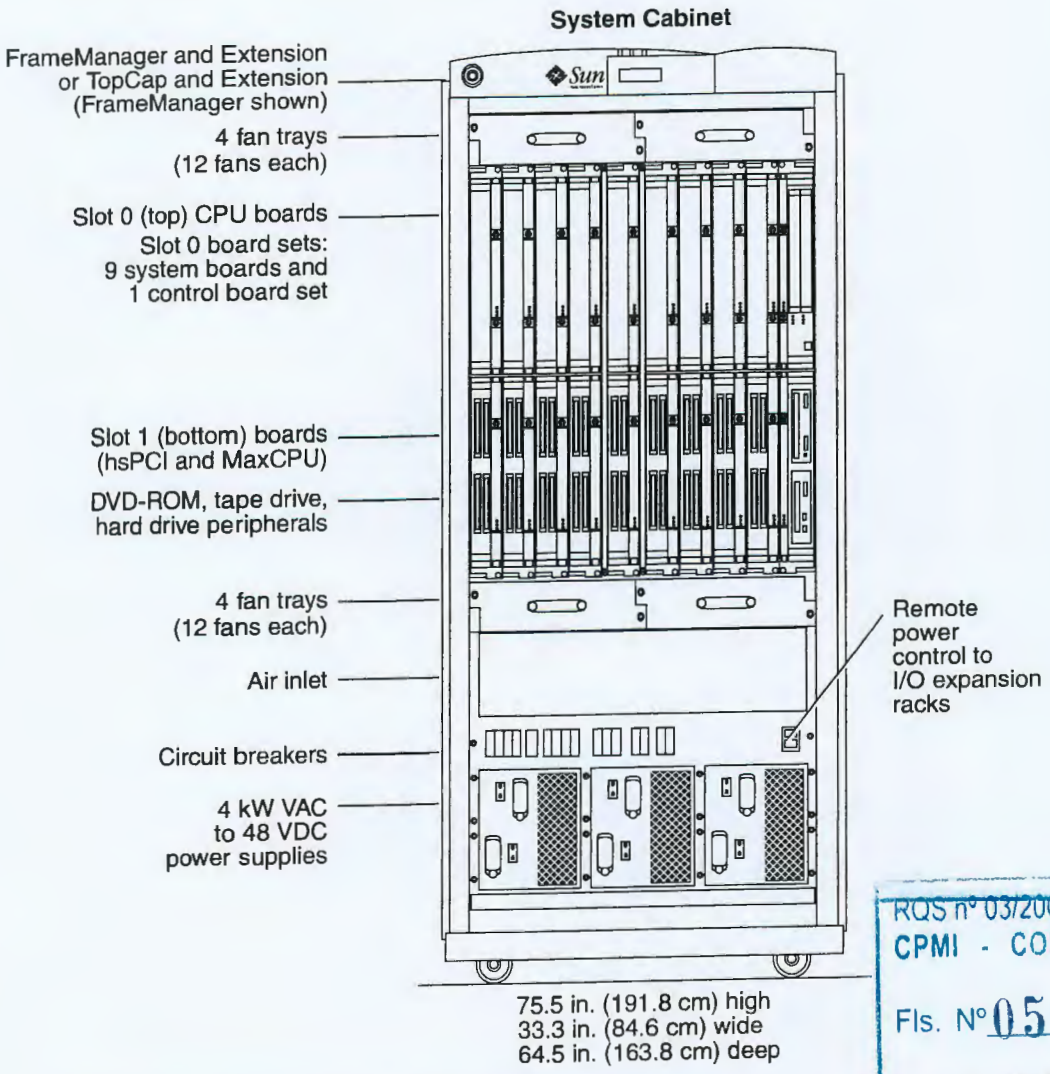


FIGURE 5-2 Sun Fire 15K/12K Systems Cabinet—Front View

The system cabinet is configured with a full complement of eight fan trays, six bulk power supplies, and two System Control board sets, which perform RAS services. (See Section 5.3.2 "Controller Board Set" on page 5-11.)

In the Sun Fire 15K system, up to 18 system board sets can be configured to determine the number of CPUs and the amount of memory per system. In the Sun Fire 12K system, up to 9 system board sets can be configured to determine the number of CPUs and the amount of memory per system. (See Section 5.3.1 "System Board Set" on page 5-7.)

A fully loaded Sun Fire 15K system cabinet weighs 2,467.8 lbs (1,121.7 kg). A fully loaded Sun Fire 12K system cabinet weighs 2141.0 lbs (987.0 kg).

5.1.1 System Power

The Sun Fire 15K systems run 200–240 VAC, single-phase power with a frequency of 47 to 63 Hz. The system cabinets require twelve 30-amp circuits, which are usually connected to two separate power sources. In North America and Japan, the site power receptacles are NEMA L6-30P; otherwise, they are IEC 309. The power cables that go between the system and the facility power receptacles are supplied with the system.

The system cabinets use six dual-input 4 kW dual AC–DC bulk power supplies. Two power cables go to each supply. These supplies convert the input power to 48 VDC. These systems can run with a failed bulk power supply, and the bulk power supplies can be replaced while the system is in operation.

Power is distributed to the individual boards through separate DC circuit breakers. Each board has its own on-board voltage converters, which transform 48 VDC to the levels required by the on-board logic components. Failure of a DC-to-DC converter affects only that particular system board.

5.1.2 System Cooling

The only operating environment limitations of the Sun Fire 15K/12K systems are:

- Temperature: 50–90 °F (10–35 °C)
- Humidity: 20%–80%
- Altitude: up to 10,000 ft (3,048 m)

The fully loaded systems draw 24 kW of power and have an air-conditioning load of approximately 77,860 BTU/hour for the Sun Fire 15K system and approximately 36,570 BTU/hrs for the Sun Fire 12K system. Smaller configurations draw less power.

For single Sun Fire 15K system or single Sun Fire 12K system heat dissipation, each system needs perforated tiles under the unit. Each tile needs to be capable of delivering 600 cubic feet per minute of cooling air. Rows of fully loaded system cabinets can be located adjacent to each other. Refer to the *Sun Fire 15K/12K Systems Site Planning Guide* for further details.

The air goes in through air inlets in the bottom, front, and back of the system cabinet and out through the top. Four fan trays are located above the system boards, and four are located below. The fans have three speeds that normally run at high speed. If any of the components get too hot, the fans are switched to super-high speed. The system is capable of running with a failed fan, and the fan trays can be hot-swapped while the system is running.

5.2 Centerplanes

FIGURE 5-3 shows how the boards and fan trays on one side of a Sun Fire 15K/12K systems connect into the fan backplane, the power centerplane, and the Sun Fireplane interconnect.

A slot 0 board and a slot 1 board connect into a system carrier plate with an expander board, which in turn connects into the Sun Fireplane interconnect. This unit is called a board set. (See Section 5.3 "System Boards" on page 5-6.)

Nine system board sets connect into each side of the Sun Fireplane interconnect with a system carrier plate and the expander, slot 0 through 8 (front side) and slot 9 through 17 (rear side) of the Sun Fire 15K system. Nine system board sets connect into the front side of the Sun Fireplane interconnect with a system carrier plate and an expander, slot 0 through 8 and nine CPU and I/O filler panels slide into slot 9 through 17 (rear side) of the Sun Fire 12K system. Two system controller board sets (System Control board and System Control peripheral board) connect into each side of the Sun Fireplane interconnect with the system control carrier plate and the centerplane support board, slot SC0 (front side) and slot SC1 (rear side). Power is distributed to all board sets through the power centerplane which is located beneath the Sun Fireplane interconnect.

The Sun Fireplane interconnect has two dedicated slots (both on the right side, front and rear) for the system controller board sets. These board sets contain power, clock, and JTAG support for the Sun Fireplane interconnect ASICs and hold the System Control boards and their associated peripherals (DVD-ROM, tape drive, and hard drive).

Four fan backplanes are mounted above the Sun Fireplane interconnect, and four are mounted below the power centerplane, distributing power to the eight fan trays.

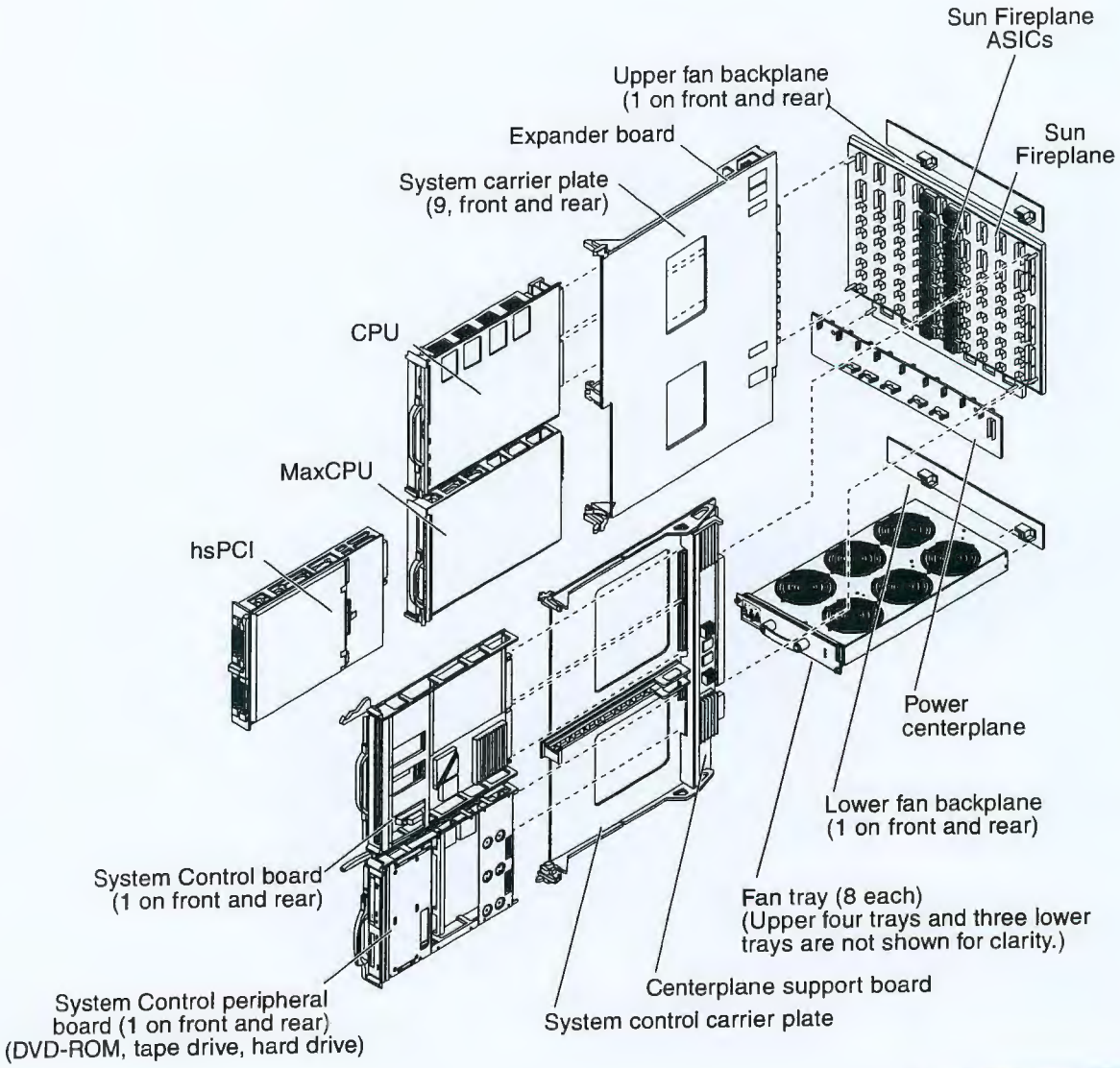


FIGURE 5-3 Sun Fireplane interconnect and Other Components

5.2.1 Sun Fireplane Interconnect

The Sun Fireplane interconnect is the heart of the Sun Fire 15K/12K systems and provides a peak data bandwidth of 43 Gbytes per second among the 18 board sets. The Sun Fireplane interconnect also delivers a console bus and an Ethernet connection to each board set.

The Sun Fireplane interconnect contains three 18x18 crossbars. The 18x18 address crossbar provides a path for address transactions between the address extender queue (AXQ) ASIC on each expander board. A pair of unidirectional paths goes to each expander board, one sending and one receiving. Each address transaction takes two system-interconnect cycles (13.3 ns) to be transmitted across the address crossbar.

The 18x18 response crossbar provides a reply path between the AXQ ASIC on each expander board. Each response message takes either one or two system-interconnect cycles (6.7 ns or 13.3 ns), depending on the type. The response path is half the width of the address path. A pair of unidirectional paths goes to each expander board, one sending and one receiving.

The 18x18 data crossbar moves cache-line (72-byte-wide) packets between the system data interface (SDI) ASICs on each expander board. Each connection is a bidirectional 36-byte-wide path. The bandwidth is 18 slots x 32-byte path x 150 MHz divided by two for bidirectional paths that are equal to 43.2 Gbytes per second. To maximize the use of these bidirectional paths, the data multiplexer (DMX) ASICs queues received data.

5.3 System Boards

A board set is a combination of three system boards that connect into the Sun Fireplane interconnect. It is also called an expander. There are two types of board sets:

- **System board set**. Boards with CPU/Memory, PCI bus controllers, and optical link controllers. (See Section 5.3.1 "System Board Set" on page 5-7.)
- **Controller board set**. Boards with power, clock, and JTAG support for the Sun Fireplane interconnect, system controller boards, and their associated peripherals. (See Section 5.3.2 "Controller Board Set" on page 5-11.)

5.3.1 System Board Set

A system board set is a combination of three boards, an expander board, a slot 0 board, and a slot 1 board. The board set, as a unit, *cannot be hot-swapped* from the Sun Fireplane interconnect. Due to the weight of the components, the slot 0 and slot 1 boards are individually removed first, and then the expander and its carrier plate can be hot-swapped. The individual slot 0 and slot 1 boards can be hot-swapped from the expander.

Slot 0 boards have a 4.8 Gbyte per second off-board data port. They are the primary locations of CPUs and are the only location of memory in a Sun Fire 15K/12K systems. Only one Slot 0 board type is used in the Sun Fire 15K/12K systems.

Slot 1 boards have a 2.4 Gbyte per second off-board data port. There are two slot 1 board types: hsPCI and MaxCPU, which are unique to the Sun Fire 15K/12K systems server.

5.3.1.1 Expander Board

An expander board acts as a 2:1 MUX to expand a Sun Fireplane interconnect slot so that it accommodates the slot 0 and slot 1 type boards. The expander board provides a level-2 address bus that can do 150 million snoops per second. The AXQ on the expander board recognizes addresses targeted at other board sets and transmits them across the Sun Fireplane interconnect.

The expander provides a three-port data switch to route data between the slot 0 board, the slot 1 board, and the Sun Fireplane interconnect. This three-port data switch is 36-bytes wide to the Sun Fireplane interconnect and to the slot 0 board, and 18 bytes wide to the slot 1 board. A board set can transfer a maximum rate of 4.8 Gbytes per second to other board sets.

It is possible to use an expander with only one system board (either slot 0 or slot 1). A system board can be hot-swapped into the expander, tested, and configured into a running system without disturbing the other board. The expander can be hot-swapped and inserted after its two system boards are removed.

5.3.1.2 CPU/Memory Board

The CPU/Memory board is a slot 0 board. It contains up to four CPUs and eight external cache DIMMs. Each CPU controls 0, 4, or 8 DIMMs. The maximum possible DIMM size is 2 Gbytes, which is 64 Gbytes of memory per board. DIMMs must be the same size and must not have sizes intermixed on a board. All CPUs on the board must be the same speed.

Two CPU/Memory pairs are connected to the rest of the system through the level-0 dual CPU data switch. Each CPU/Memory can transfer data at a maximum rate of 2.4 Gbytes per second. The pair of CPU/Memory units share a 4.8 Gbyte per second port to the data switch. The level-1 data switch connects the two pairs of CPUs to the off-board data port that goes to the expander board. (See FIGURE 5-4.)

5.3.1.3 Example of System Board Set

FIGURE 5-4 and FIGURE 5-5 show an example board set diagram and board set layout composed of an expander board, a CPU/Memory board, and a PCI board.

5.3.1.4 PCI Assembly (hsPCI)

The PCI assembly is a slot 1 option board. It is also called the hsPCI assembly. It provides four standard PCI slots, two at 33 MHz and two at 33/66 MHz. The assembly has two PCI controllers, each of which provides a 33 MHz PCI bus and a 33/66 MHz PCI bus.

A cassette is used to provide hot-swap capabilities for industry-standard PCI assemblies. The cassette is a passive card carrier that adapts the standard PCI pins to a connector.

A PCI card is placed into a PCI hot-swap cassette, and then the cassette is hot-swapped onto the PCI assembly. The software recognizes this assembly as a standard PCI assembly with the system controller turning power on and off to each PCI slot. (See FIGURE 5-4.)

5.3.1.5 MaxCPU Board

The MaxCPU board is a slot 1 board. It has two CPUs but does not include any memory. This board enables CPUs to replace PCI cards in system configurations when more CPU power, instead of I/O connectivity, is necessary.

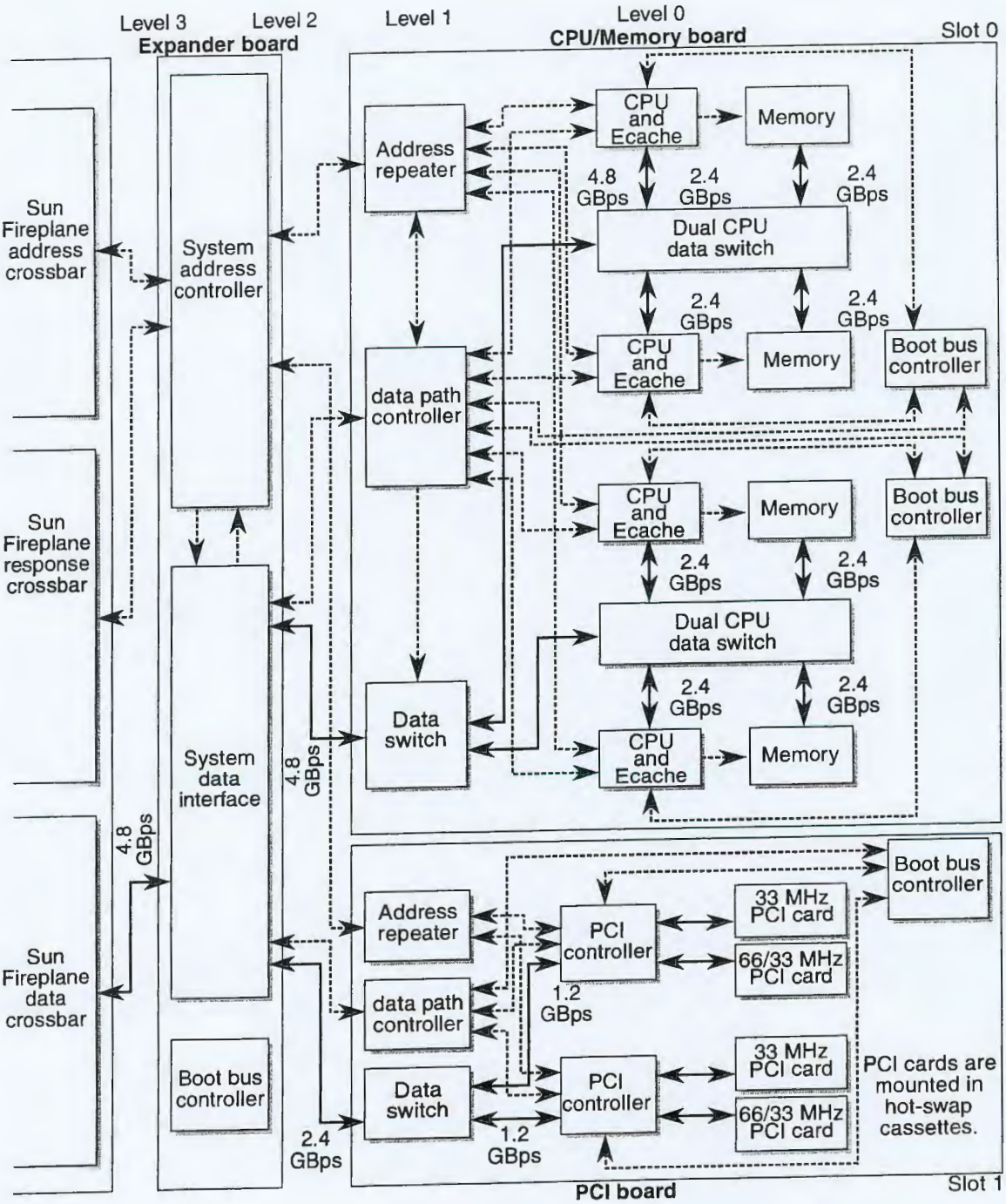


FIGURE 5-4 Board Set Block Diagram

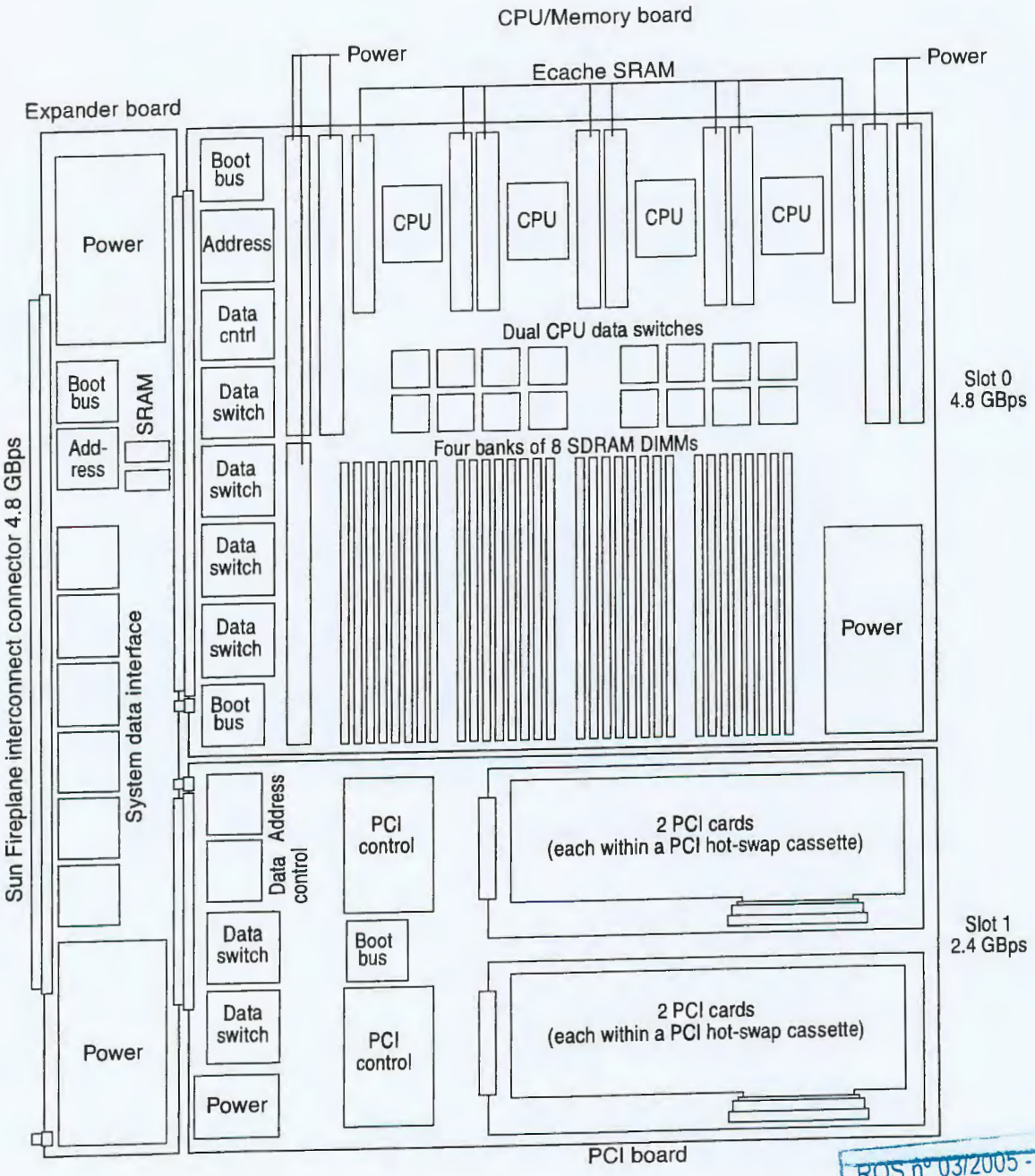


FIGURE 5-5 System Board Set Layout

5.3.2 Controller Board Set

The controller board set provides critical services and resources required for operation and control of the Sun Fire 15K/12K systems (FIGURE 5-6).

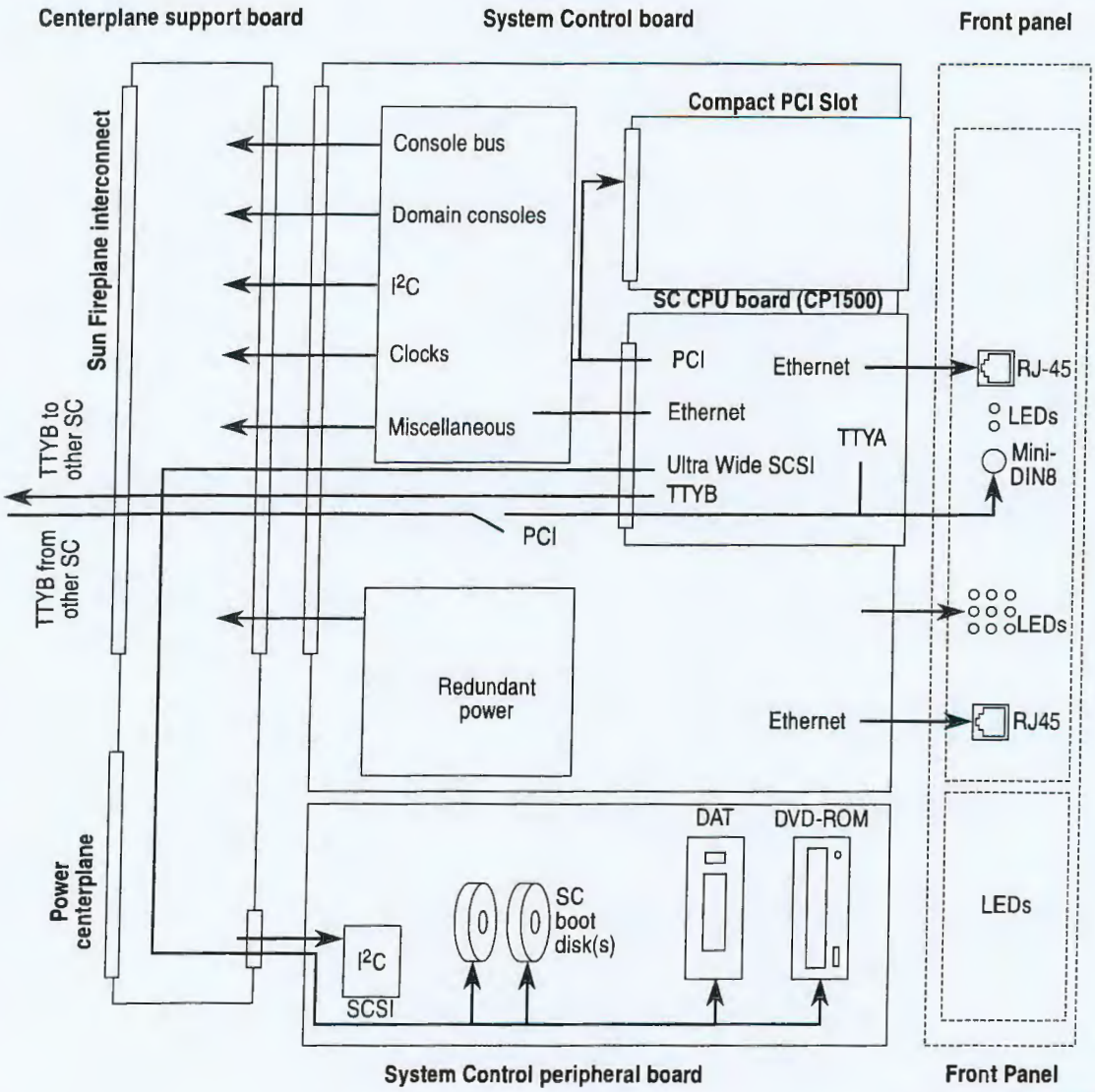


FIGURE 5-6 System Controller Board Layout

This board set consists of three boards:

- **Centerplane support board**: Connects into a dedicated Sun Fireplane interconnect slot and is the same size as an expander board with power, clock, and JTAG support for the Sun Fireplane interconnect.
- **System Control board**: Connects into the centerplane support board and is the same size as a slot 0 system board.
- **System Control Peripheral board**: Connects into the centerplane support board and is the same size as a slot 1 system board. This peripheral board holds a DVD-ROM, disk drives, and a 4-mm format DAT (digital audio tape) drive.

The System Control board is a two-board combination:

- **SC CPU board**. The SC CPU board is an off-the-shelf SPARCengine CP1500 6U cPCI board with an UltraSPARC-IIi embedded system. This board runs Solaris Software, the System Management Software, and all associated applications required for startup, maintenance, and interrogation of the system.
- **System Control board**. The control board provides the Sun Fire 15K/12K systems with specific logic and connection to the centerplane support board.

The system controller board set provides the following critical services and resources required for operation and control of the Sun Fire 15K/12K systems:

- System clock
- I^2C bus to the entire system
- Console bus to the entire system
- Serial (TTY) port through the SC CPU board
- Serial (TTY) port between the two system controllers
- CP1500 (using the UltraSPARC IIi processor) to run Solaris Software, System Management Software, and all associated applications required for bringup, maintenance, and interrogation of the system
- Exclusive access to all dynamic system domain consoles
- SCSI to support DVD-ROM, DAT drives, and hard drives
- Support of high-availability features for failover of SC operations to the redundant SC
- Support of security features to provide a secure administrative environment up to and including certified B1 security
- Secure private Ethernet lines to all I/O boards on each expander Management Area Network (MAN)

The SPARCengine cPCI card is mounted flat and on top of the SC in the same manner that the PCI cards are mounted onto the I/O boards.

CHAPTER 1

Introduction to System Management Services

This manual describes the System Management Services (SMS) 1.3 software that is available with the Sun Fire 15K/12K server system.

This chapter includes the following sections:

- Sun Fire 15K/12K Server System
- SMS Features
- System Architecture
- SMS Administration Environment
- Sun Management Center

Sun Fire 15K/12K Server System

The Sun Fire 15K/12K server is a member of the next-generation Sun Fire server family.

The system controller (SC) in the Sun Fire 15K/12K is a multifunction, Nordica-based printed circuit board (PCB), which provides critical services and resources required for the operation and control of the Sun Fire system. In this book, the system controller is called the *SC*.

The Sun Fire 15K/12K system is often referred to as the *platform*. System boards within the platform can be logically grouped together into separately bootable systems called *dynamic system domains*, or simply *domains*.

Up to 18 domains on the Sun Fire 15K, and up to 9 domains on the Sun Fire 12K can exist simultaneously on a single platform. (Domains are introduced in this chapter, and are described in more detail in "SMS Configuration" on page 57.) The system management services (SMS) software lets you control and monitor domains, as well as the platform itself.

The following list is an overview of the many services the SC provides for the Sun Fire system:

- Manages the overall system configuration.
- Acts as a boot initiator for its domains.
- Serves as the syslog host for its domains; note that an SC can still be a syslog client of a LAN-wide syslog host.
- Provides a synchronized hardware clock source.
- Sets up and configures dynamic domains.
- Monitors system environmental information, such as power supply, fan, and temperature status.
- Hosts field-replaceable unit (FRU) logging data.
- Provides redundancy and automated SC failover in dual SC configurations.
- Provides a default name service for the domains based on virtual hostids, and MAC addresses for the domains.
- Provides administrative roles for platform management.

Redundant SCs

There are two SCs within Sun Fire platform. The SC that controls the platform is referred to as the main SC, while the other SC acts as a backup and is called the spare SC. The software running on the SC monitors the SCs to determine when an automatic failover should be performed.

We strongly recommend that the two SCs have the same configuration. This duplication includes the Solaris operating environment, SMS software, security modifications, patch installations, and all other system configurations

The failover functionality between the SCs is controlled by the daemons running on the main and spare SCs. These daemons communicate across private communication paths built into the Sun Fire platform. Other than the communication of these daemons, there is no special trust relationship between the two SCs.

SMS software packages are installed on the SC. In addition, SMS communicates with the Sun Fire 15K/12K system over an Ethernet connection, see "Management Network Services" on page 141.

SMS Features

SMS 1.3 supports Sun Fire 15K/12K servers running the Solaris 8 and Solaris 9 operating environments.

Note – SMS 1.3 is available for Solaris 8 02/02 software. That version will *not* run on Solaris 9 software without replacing specific driver packages. Conversely, the Solaris 9 version of SMS 1.3 will not run on Solaris 8 02/02 software without replacing specific driver packages. For more information contact your Sun service representative.

SMS 1.3 is compatible with Sun Fire 15K/12K domains that are running the Solaris 8 02/02 through Solaris 9 operating environment. The commands provided with the SMS software can be used remotely.

Note – Graphical user interfaces for many of the commands in SMS are provided by Sun Management Center. For more information, see "Sun Management Center" on page 11.

SMS enables the platform administrator to perform the following tasks:

- Administrate domains by logically grouping domain configurable units (DCU) together. DCUs are system boards such as CPU and I/O boards. Domains are able to run their own operating systems and handle their own workloads. See "SMS Configuration" on page 57.
- Dynamically reconfigure a domain so that currently installed system boards can be *logically* attached to or detached from the operating system while the domain continues running in multiuser mode. This feature is known as *dynamic reconfiguration* and is described in the *System Management Services (SMS) 1.3 Dynamic Reconfiguration User Guide* (A system board can be *physically* swapped in and out when it is not attached to a domain, while the system continues running in multiuser mode.)
- Perform automatic dynamic reconfiguration of domains using a script. Refer to the *System Management Services (SMS) 1.3 Dynamic Reconfiguration User Guide.*
- Monitor and display the temperatures, currents, and voltage levels of one or more system boards or domains.
- Monitor and control power to the components within a platform.
- Execute diagnostic programs such as power-on self-test (POST).

In addition, SMS:

- Warns you of impending problems, such as high temperatures or malfunctioning power supplies.
- Notifies you when a software error or failure has occurred.
- Monitors a dual SC configuration for single points of failure and performs an automatic failover from the main SC to the spare depending on the failure condition detected.
- Automatically reboots a domain after a system software failure (such as a panic).
- Keeps logs of interactions between the SC environment and the domains.
- Provides support for the Sun Fire 15K/12K system dual grid power option.

SMS enables the domain administrator to perform the following tasks:

- Administrate domains by logically grouping *domain configurable units* (DCU) together. DCUs are system boards such as: CPU and I/O boards. Domains are able to run their own operating systems and handle their own workloads. See "SMS Configuration" on page 57.
- Boot domains for which the administrator has privileges.
- Dynamically reconfigure a domain for which the administrator has privileges, so that currently installed system boards can be *logically* attached to or detached from the operating system while the domain continues running in multiuser mode. This feature is known as *dynamic reconfiguration* and is described in the *System Management Services (SMS) 1.3 Dynamic Reconfiguration User Guide.* (A system board can be *physically* swapped in and out when it is not attached to a domain, while the system continues running in multiuser mode.)
- Perform automatic dynamic reconfiguration of domains using a script for which the administrator has privileges. Refer to the *System Management Services (SMS) 1.3 Dynamic Reconfiguration User Guide.*
- Monitor and display the temperatures, currents, and voltage levels of one or more system boards or domains for which the administrator has privileges.
- Execute diagnostic programs such as power-on self-test (POST) for which the administrator has privileges.

The following features are provided in this release of SMS:

- Dynamic system domain (DSD) configuration
- Configured domain services
- Domain control capabilities
- Capacity on demand (COD)
- Domain status reporting
- Hardware control capabilities
- Hardware status monitoring, reporting, and handling
- Hardware error monitoring, reporting, and handling
- System controller (SC) failover
- Configurable administrative privileges
- Dynamic FRUID

System Architecture

SMS architecture is best described as distributed client-server. `init`(1M) starts (and restarts as necessary) one process: `ssd`(1M). `ssd` is responsible for monitoring all other SMS processes and restarting them as necessary. See FIGURE 3-1.

The Sun Fire 15K/12K platform, the SC, and other workstations communicate over Ethernet. You perform SMS operations by entering commands on the SC console after remotely logging in to the SC from another workstation on the local area network. You must log in as a user with the appropriate platform or domain privileges if you want to perform SMS operations (such as monitoring and controlling the platform).

Note – If SMS is stopped on the main SC and the other SC is powered off, the domains gracefully shutdown and the platform is powered down. If the remaining SC is simply powered off without a shutdown of SMS, SMS won't have time to power off the platform and the domains will crash.

Dual system controllers are supported within the Sun Fire 15K/12K platform. One SC is designated as the primary or main system controller, and the other is designated as the spare system controller. If the main SC fails, the failover capability automatically switches to the spare SC as described in "SC Failover" on page 155.

Most domain configurable units are active components and you need to check the system state before powering off any DCU.

Note – Circuit breakers must be on whenever a board is present, including expander boards, whether or not the board is powered on.

For details, see "Power Control" on page 128.

SMS Administration Environment

Administration tasks on the Sun Fire 15K/12K system are secured by group privilege requirements. Upon installation, SMS installs the following 39 UNIX groups to the `/etc/group` file.

- `platadmn` - Platform administrator
- `platoper` - Platform operator

- `platsvc` - Platform service
- `dmn[`*A...R*`]admn` - domain [*domain_id*|*domain_tag*] administrator (18)
- `dmn[`*A...R*`] rcfg` - domain [*domain_id*|*domain_tag*] configurator (18)

`smsconfig`(1M) allows an administrator to add, remove, and list members of platform and domain groups as well as set platform and domain directory privileges using the `-a`, `-r`, and `-l` options.

`smsconfig` also can configure SMS to use alternate group names including NIS managed groups using the `-g` option. Group information entries can come from any of the sources for groups specified in the `/etc/nsswitch.conf` file (refer to `nsswitch.conf`(4)). For instance, if domain A was known by its domain tag as the "Production Domain," an administrator could create a NIS group with the same name and configure SMS to use this group as the domain A administrator group instead of the default, `dmnaadmn`. For more information, refer to the *System Management Services (SMS) 1.3 Installation Guide*, "Administration Privileges" on page 15, and refer to the `smsconfig` man page.

Network Connections for Administrators

The nature of the Sun Fire 15K/12K physical architecture, with an embedded system controller, as well as the supported administrative model (with multiple administrative privileges, and hence multiple administrators) dictates that an administrator utilize a remote network connection from a workstation to access SMS command interfaces to manage the Sun Fire 15K/12K system.

Caution – Shutting down a remote workstation while a tip session is active into a Sun Fire 15K/12K SC will bring both SCs down to the OpenBoot OK prompt. This will not affect the domains and after powering the remote system back on you can restore the SCs by typing go at the OK prompt; however, you should end all tip sessions before shutting down a remote workstation.

Since the administrators provide information to verify their identity (passwords) and might possibly need to display sensitive data, it is important that the remote network connection be secure. Physical separation of the administrative networks provides some security on the Sun Fire 15K/12K system. Multiple external physical network connections are available on each SC. SMS software supports up to two external network communities.

For more information on Sun Fire 15K/12K networks, see "Management Network Services" on page 141. For more information on securing the Sun Fire 15K/12K system see "Security Options" on page 14.

SMS Operating Environment

You can interact with the SC and the domains on the Sun Fire 15K/12K system by using SMS commands.

SMS provides a command-line interface to the various functions and features it contains.

▼ To Begin Using the SC

1. **Boot the SC.**

   For the examples in this guide, the *sc_name* is `sc0` and *sms-user* is the *user-name* of the administrator, operator, configurator, or service personnel logged onto the system.

   The privileges allotted to the user are determined by the platform or domain groups to which the user belongs. In these examples, the *sms-user* is assumed to have both platform and domain administrator privileges, unless otherwise noted.

   For more information on the function and creation of SMS user groups, refer to the *System Management Services (SMS) 1.3 Installation Guide* and see "Administration Privileges" on page 15.

Note – This procedure assumes that `smsconfig -m` has already been run. If `smsconfig -m` has not been run, you will receive the following error when SMS attempts to start and SMS will exit.

```
sms: smsconfig(1M) has not been run. Unable to start sms services.
```

2. **Log in to the SC and verify that SMS software startup has completed. Type:**

```
sc0:sms-user:> showplatform
```

3. **Wait until `showplatform` finishes displaying platform status.**

   At this point you can begin using SMS programs.

SMS Console Window

An SMS console window provides a command-line interface from the SC to the Solaris operating environment on the domain(s).

▼ To Display a Console Window Locally

1. **Log in to the SC, if you have not already done so.**

Note – You must have domain privileges for the domain on which you wish to run `console`.

---

2. Type:

```
sc0:sms-user:> console -d domain_indicator option
```

where:

`-d` Specifies the domain using a *domain_indicator*:

domain_id - ID for a domain. Valid *domain_id*s are 'A'...'R' and are case insensitive.

domain_tag - Name assigned to a domain using `addtag`(1M).

`-f` Force
Opens a domain console window with "locked write" permission, terminates all other open sessions, and prevents new ones from being opened. This constitutes an "exclusive session." Use it only when you need exclusive use of the console (for example, for private debugging). To restore multiple-session mode, either release the lock (~^) or terminate the console session (~.).

`-g` Grab
Opens a console window with "unlocked write" permission. If another session has "unlocked write" permission, the new console window takes it away. If another session has "locked" permission, this request is denied and a read-only session is started.

`-l` Lock
Opens a console window with "locked write" permission. If another session has "unlocked write" permission, the new console window takes it away. If another session has "locked" permission, the request is denied and a read-only session is started.

`-r` Read Only
Opens a console window in read-only mode

`console` creates a remote connection to the domain's virtual `console` driver, making the window in which the command is executed a "console window" for the specified domain (*domain_id* or *domain_tag*).

If `console` is invoked without any options when no other console windows are running for that domain, it comes up in exclusive "locked write" mode session.

If `console` is invoked without any options when one or more non-exclusive console windows are running for that domain, it will come up in "read-only" mode.

Locked write permission is more secure. It can only be taken away if another console is opened using `console -f` or if ~*(tilde-asterisk) is entered from another running console window. In both cases, the new console session is an "exclusive

session", and all other sessions are forcibly detached from the domain virtual console.

`console` can utilize either Input Output Static Random Access Memory (IOSRAM) or the internal management network for domain console communication. You can manually toggle the communication path by using the `~=` (tilde-equal sign) command. Doing so is useful if the network becomes inoperable, in which case the console sessions appears to be hung.

Many console sessions can be attached simultaneously to a domain, but only one console will have write permissions; all others will have read-only permissions. Write permissions are in either "locked" or "unlocked" mode.

Tilde Usage

In a domain console window, a tilde (~) that appears as the first character of a line is interpreted as an escape signal that directs console to perform some special action, as follows:

Character	Description
~?	Status message
~.	Disconnects console session
~#	Breaks to OpenBoot™ PROM or `kadb`
~@	Acquires unlocked write permission. See option `-g`
~^	Releases write permission
~=	Toggles the communication path between the network and IOSRAM interfaces. You can use `~=` only in private mode (see `~*`).
~&	Acquires locked write permission; see option `-l` . You may issue this signal during a read-only or unlocked write session.
~*	Acquires locked write permission, terminates all other open sessions, and prevent new sessions from being opened; see option `-f` . To restore multiple-session mode, either release the lock or terminate this session.

`rlogin` also processes tilde-escape sequences whenever a tilde is seen at the beginning of a new line. If you need to send a tilde sequence at the beginning of a line and you are connected using `rlogin`, use two tildes (the first escapes the second for `rlogin`). Alternatively, do not enter a tilde at the beginning of a line when running inside of an `rlogin` window.

If you use a `kill -9` command to terminate a console session, the window or terminal in which the `console` command was executed goes into raw mode, and appears hung. Type `CTRL-j`, then `stty sane`, then `CTRL-j` to escape this condition,

In the domain console window, `vi`(1) runs properly and the escape sequences (tilde commands) work as intended only if the environment variable TERM has the same setting as that of the console window.

For example:

```
sc0:sms-user:> setenv TERM xterm
```

If you need to resize the window, type:

```
sc0:sms-user:> stty rows 20 cols 80
```

For more information on domain console, see "Domain Console" on page 141 and refer to the `console` man page.

Remote Console Session

In the event that a system controller hangs and that console cannot be reached directly, SMS provides the `smsconnectsc` command to remotely connect to the hung SC. This command works from either the main or spare SC. For more information and examples, refer to the `smsconnectsc` man page.

Your other option is to connect to the hung SC using an external console connection but you cannot run `smsconnectsc` and use an external console at the same time.

Sun Management Center

Sun Management Center for the Sun Fire 15K/12K is an extensible monitoring and management tool that provides a system administrator with the ability to manage the Sun Fire 15K/12K system. Sun Management Center integrates standard SNMP based management structures with new intelligent and autonomous agent and management technology based on the client/ server paradigm.

Sun Management Center is used as the GUI and SNMP manager/agent infrastructure for the Sun Fire system. The features and functions of Sun Management Center are not covered in this manual. For more information, refer to the latest Sun Management Center documentation available at `www.docs.sun.com`.

oc 12 - item 3 VxFS é um JFS

fls. 166

STORAGE MANAGEMENT SOFTWARE

VERITAS File System

VERITAS File System

» In the Spotlight

Storage Related:

» White Papers
» Success Stories
» Press Releases

Print

VERITAS File System software is a powerful, quick-recovery journaling file system that is designed to provide high performance and easy management for mission-critical applications. The software augments UNIX® file management with high availability, data throughput, and up-to-date structural integrity.

Contact Me | Get the Software

VERITAS File System is a high-performance, quick-recovery, journaling file system. It helps provide the performance and manageability mission-critical applications require. VxFS provides scalable performance and capacity to meet the demands of increased user loads and client/server environments.

Highlights

Key Applications:
VERITAS File System 3.2 (VxFS) software augments UNIX® file management and provides scalable performance and capacity to meet the demands of increased user loads and client/server environments.

Key Specifications:
VERITAS File System has online management capabilities, such as defragmentation and flexible file system sizes. The software helps enable online backups and fast recovery times: The journaling file system means no file system checks are required.

Key Benefits:
Is designed to provide fast recoverability, high availability, high performance and scalability. Centralized management in heterogeneous environments.

Key Related Hardware:
- Sun StorEdge A5200
- Sun StorEdge T3 Array for the Enterprise
- Sun StorEdge T3 Array for the Workgroup

Key Industries:
VxFS is suitable for virtually any mission-critical site that needs high availability, robust data access, and fast recovery.

Requirements:

- Solaris 2.6, 7, or 8 Operating Environments.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0617
Doc: 3696

1. This page meets my need. disagree ○ ○ ○ ○ ○ ○ ○ agree

2. This page was easy to find. disagree ○ ○ ○ ○ ○ ○ ○ agree

UFS Feature	Description
State flags	Show the state of the file system: clean, stable, active, logging, or unknown. These flags eliminate unnecessary file system checks. If the file system is "clean," "stable," or "logging," file system checks are not run.
Extended fundamental types (EFT)	Provides 32-bit user ID (UID), group ID (GID), and device numbers.
Large file systems	Allows files of approximately 1 terabyte in size in a file system that can be up to 16 terabytes in size. You can create a multiterabyte UFS file system on a disk with an EFI disk label.

For detailed information about the UFS file system structure, see Chapter 44.

UFS Logging

UFS logging is the process of storing transactions (changes that make up a complete UFS operation) in a log before the transactions are applied to the UFS file system. Once a transaction is stored, the transaction can be applied to the file system later.

At reboot, the system discards incomplete transactions, but applies the transactions for completed operations. The file system remains consistent because only completed transactions are ever applied. This consistency remains even when a system crashes, which normally interrupts system calls and introduces inconsistencies into a UFS file system.

UFS logging provides two advantages:

- Prevents file systems from becoming inconsistent, therefore eliminating the need to run the `fsck` command. And, because `fsck` checking can be bypassed, UFS logging reduces the time required to reboot a system if it crashes, or after an unclean halt (see "What the `fsck` Command Checks and Tries to Repair" on page 602 for details on unclean halts).
- UFS logging can significantly reduce the boot time on systems with large file systems, which usually take a long time to read and verify with the `fsck` command.

The log created by UFS logging is continually flushed as it fills up. The log is flushed when the file system is unmounted or as a result of the `lockfs -f` command.

UFS logging is not enabled by default.

If you need to enable UFS logging, specify the `-o logging` option with the `mount` command in the `/etc/vfstab` file or when you mount the file system manually. The log is allocated from free blocks on the file system, and it is sized at approximately 1

Mbyte per 1 Gbyte of file system, up to a maximum of 64 Mbytes. Logging can be enabled on any UFS file system, including the root (/) file system. Also, the `fsdb` command now has new debugging commands to support UFS logging.

In some operating systems, a file system with logging enabled is known as a *journaling* file system.

Planning UFS File Systems

When laying out file systems, you need to consider possible conflicting demands. Here are some suggestions:

- Distribute the work load as evenly as possible among different I/O systems and disk drives. Distribute the `/export/home` file system and swap space evenly across disks.
- Keep pieces of projects or members of groups within the same file system.
- Use as few file systems per disk as possible. On the system (or boot) disk, you should have three file systems: root (/), `/usr`, and swap space. On other disks, create one or, at most, two file systems; one being additional swap space, preferably. Fewer, roomier file systems cause less file fragmentation than many small, over-crowded file systems. Higher-capacity tape drives and the ability of the `ufsdump` command to handle multiple volumes make it easier to back up larger file systems.
- If you have some users who consistently create very small files, consider creating a separate file system with more inodes. However, most sites do not need to keep similar types of user files in the same file system.

For information on default file system parameters as well as procedures for creating new UFS file systems, see Chapter 39.

UFS Direct Input/Output (I/O)

Direct I/O is intended to boost bulk I/O operations. Bulk I/O operations use large buffer sizes to transfer large files (larger than 256 Kbytes).

Using UFS direct I/O might benefit applications, such as database engines, that do their own internal buffering. Starting with the Solaris 8 1/01 release, UFS direct I/O has been enhanced to allow the same kind of I/O concurrency seen when accessing raw devices. Now you can get the benefit of file system naming and flexibility with very little performance penalty. Check with your database vendor to see if they can enable UFS direct I/O in their product configuration options.

Direct I/O can also be enabled on a file system by using the `forcedirectio` option to the `mount` command. Enabling direct I/O is a performance benefit only when a file system is transferring large amounts of sequential data.

Doc 12 item 4


```
#to mount          to fsck            point        type pass at boot options
#
fd                 -                  /dev/fd      fd   -    no      -
/proc              -                  /proc        proc -    no      -
/dev/dsk/c0t0d0s1  -                  -            swap -    no      -
/dev/dsk/c0t0d0s0  /dev/rdsk/c0t0d0s0 /            ufs  1    no      -
/dev/dsk/c0t0d0s6  /dev/rdsk/c0t0d0s6 /usr         ufs  1    no      -
/dev/dsk/c0t0d0s5  /dev/rdsk/c0t0d0s5 /datab       ufs  2    yes     -
/dev/dsk/c0t0d0s7  /dev/rdsk/c0t0d0s7 /export/home ufs  2    yes     -
swap               -                  /tmp         tmpfs -    yes     -
```

▼ How to Determine the Number of Tapes Needed for a Full Backup

1. **Become superuser or assume an equivalent role.**
2. **Estimate the size of the backup in bytes.**

   `# ufsdump S` *file-system*

   The `S` displays the estimated number of bytes that are needed to do the backup.
3. **Divide the estimated size by the capacity of the tape to see how many tapes you need.**

   For a list of tape capacities, see Table 46–5.

Example—Determining Number of Tapes

In this example, the file system of 489,472 bytes easily fits on a 150-Mbyte tape.

```
# ufsdump S /export/home
489472
```

Backing Up a File System

The following are general guidelines for performing backups:

- Use single-user mode or unmount the file system, unless you are creating a snapshot of a file system. For information about UFS snapshots, see Chapter 48.
- Be aware that the backing up of file systems when there are directory-level operations (such as creating, removing, and renaming files) and file-level activity occurring means that some data will not be included in the backup.
- You can run the `ufsdump` command from a single system and remotely back up groups of systems across the network through remote shell or remote login, and direct the output to the system on which the tape drive is located. (Typically, the

tape drive is located on the system from which you run the `ufsdump` command, but it does not have to be.)

Another way to back up files to a remote drive is to pipe the output from the `ufsdump` command to the `dd` command. For information about using the `dd` command, see Chapter 51.

- If you are doing remote backups across the network, the system with the tape drive must have entries in its `/.rhosts` file for each client that will be using the drive. Also, the system that initiates the backup must be included in the `/.rhosts` file on each system that it will back up.
- To specify a remote tape device on a system, use the naming convention that matches the OS release of the system with the remote tape drive. For example, use the `/dev/rst0` device for a remote drive on a system that is running the SunOS 4.1.1 release or compatible versions. Use the `/dev/rmt/0` device for a system running the Solaris 9 release or compatible versions.

Note – Use the `nisbackup` command to back up a NIS+ master server. For information on using this command, see *System Administration Guide: Naming and Directory Services (FNS and NIS+).*

▼ How to Backup a File System to Tape

The following steps provide the general steps for backing up file systems using the `ufsdump` command. The examples show specific uses of options and arguments.

1. **Become superuser or assume an equivalent role.**
2. **Bring the system to run level S (single-user mode).**

   ```
   # shutdown -g30 -y
   ```

3. **(Optional) Check the file system for consistency.**

   ```
   # fsck -m /dev/rdsk/device-name
   ```

   The `fsck -m` command checks for the consistency of file systems. For example, power failures can leave files in an inconsistent state. For more information on the `fsck` command, see Chapter 43.

4. **If you need to back up file systems to a remote tape drive:**

   a. **On the system to which the tape drive is attached (the tape server), add the following entry to its `/.rhosts` file.**

      host `root`

      The *host* entry specifies the name of the system on which you will run the `ufsdump` command to perform the backup.

Task	Description	Instructions
	Restore files interactively - Use this method when you are unsure of the file names because you can browse the media contents and select individual files and directories.	"How to Restore Files Interactively" on page 677
	Restore files non-interactively - Using this method is probably faster if you already know the few file names to be restored.	"How to Restore Specific Files Non-Interactively" on page 679
	Restore a file system – Use this method when you get a new disk drive or as part of a recovery procedure.	"How to Restore a Complete File System" on page 681
Restore the root (/) or /usr file systems	Restoring the root (/) or /usr file systems involves booting the system from a local CD or the network.	"How to Restore the root (/) and /usr File Systems" on page 684

Preparing to Restore Files and File Systems

The `ufsrestore` command copies files to disk, relative to the current working directory, from backups that were created by using the `ufsdump` command. You can use the `ufsrestore` command to reload an entire file system hierarchy from a level 0 dump and incremental dumps that follow it or to restore one or more single files from any backup tape. If the `ufsrestore` command is run as superuser, files are restored with their original owner, last modification time, and mode (permissions).

Before you start to restore files or file systems, you need to know the following:

- The tapes (or diskettes) you need
- The raw device name on which you want to restore the file system
- The type of tape device you will use
- The device name (local or remote) for the tape drive

Determining the File System Name

If you have properly labeled your backup tapes, you should be able to use the file system name (`/dev/rdsk/`*device-name*) from the tape label. For more information, see "How to Find File System Names" on page 656.

Solaris 9 Operating System

Product Home

- » Family Comparison
- » General FAQ
- » System Requirements

Get the Software »

SOLARIS™

The Solaris 9 Operating System redefines the operating system to a services platform by combining traditional OS functionality, application services, and identity management. The Solaris 9 OS delivers the security, manageability and performance that IT professionals need to increase service levels and decrease costs and risks; it's the rock-solid foundation for solutions based on the Sun ONE software architecture. Customers can take full advantage of UltraSPARC or x86 processor-based systems, from smaller departmental servers to massive SunPlex clusters with hundreds of CPUs.

→ **Sun Fire 15K Server Sets World Record**

→ **Delivering Choice, Innovation and Value**

At a Glance

Product	Purpose
Solaris Operating System for SPARC Platforms	Designed for multiprocessing and 64-bit computing using UltraSPARC processor-based systems - from small departmental servers to massive SunPlex clusters with hundreds of CPUs.
Solaris Operating System for x86 Platforms	Delivers superior scalability across platforms, providing plenty of room for your growing enterprise along with the performance you need to handle the most complex tasks in record times.
Trusted Solaris Operating System for both SPARC and x86 platforms	Provides superior safeguards against internal and external threats far beyond the protection commonly found in standard operating systems.

» **Contact Me**

Evaluate

- □ Product Home
- » Data Sheets
- » Tours
- » Case Studies
- » White Papers
- » News & Events

Get

- » Get the Software
- » Licensing Information
- » Programs & Promotions
- » Support & Services
- » Training

Use

- » Documentation
- » Product Registration
- » Community & Resources
- » Developer Resources

Maintain

- » Upgrades & Add-Ons
- » Patches & Support
- » Newsletters & Alerts
- » Previous Versions

Doc 14

Sun™ ONE Studio 7, Compiler Collection

(formerly Forte™ Compiler Collection 7)

For the Solaris™ Operating Environment

Key feature highlights

Provides ISO/IEC C, C++, and Fortran 95 standards support

Accepts common de facto C and C++ language extensions

Supports 64-bit application development

Includes two C++ standard libraries: the Sun binary-compatible version and STLport

Provides expanded support for the OpenMP API

Supports mixed-language linking with C, C++, and Fortran objects

Compatible with Sun Performance Library ware

Delivers significant improvements in both compile-time and run-time performance

Offers enhanced, global program checking across multiple source files for Fortran 95 to check OpenMP directives

Provides stack overflow detection in Fortran

Delivers interval arithmetic support, available in C++ and Fortran 95

Provides the ability to debug Java™ code as well as C, C++, and Fortran

Includes new serial number license number for entitlement

The Sun™ ONE Studio 7, Compiler Collection (formerly Forte™ Compiler Collection 7) is a key component of the Sun Open Net Environment (Sun ONE) — Sun's vision, architecture, platform, and expertise for delivering Services on Demand. It provides a comprehensive, productive environment for developing reliable, scalable, high-performance applications in C, C++, and Fortran for the Solaris™ Operating Environment.

The Sun ONE Studio 7, Compiler Collection includes the following command-line interface-based (CLI-based) components:

- Complete C, C++, and Fortran 95 language systems for building high-performance 32-bit and 64-bit applications
- Compatible software components to compile, build, and debug applications easily
- Multithreading development tools for developing multithreaded/multiprocessing applications
- Compatibility with Sun Performance Library™ software, providing maximum performance for matrix algebra and signal processing
- A new serial number licensing model for entitlement to ease installation and administration

64-Bit Application Development

Sun's developer products support development of both 32-bit and 64-bit applications. The 64-bit technology offers a variety of benefits to developers, including:

- 64-bit address space: Increase the capacity of problems you can solve, or run existing problems entirely in RAM for a huge performance boost.
- 64-bit integer arithmetic: Increase the calculation speed for mathematical operations.
- Large files (>4 GB): Store and manipulate large quantities of data without splitting them into multiple files.

With 64-bit technology, your applications can solve larger, more complex problems than ever before.

High-Performance Compilers

The Sun ONE Studio 7, Compiler Collection offers significant boosts in both compilation and execution speed over previous versions:

- The C++ compiler supports ISO/IEC C++, including features such as namespaces, bool, and covariant returns.
- The C compiler supports both ANSI and K&R C, plus some features from C99.
- The Fortran 95 compiler fully supports ISO/IEC Fortran 95, as well as new language constructs from the emerging Fortran 2000 standard.
- All of Sun's compilers enable optimized run time for SPARC® systems, enabling your applications to run as fast as possible.

The Sun ONE Studio 7, Compiler Collection helps you achieve higher performance, throughput, and responsiveness with multithreaded applications.

Turbocharge Applications With Multithreading Technology

The Sun ONE Studio 7, Compiler Collection helps you achieve higher performance, throughput, and responsiveness with multithreaded applications. You can build these powerful applications with our comprehensive multithreading solution using capabilities such as OpenMP API support for C, C++, and Fortran code and improved performance analysis tools.

Boost Programming Productivity and Application Quality

The Sun ONE Studio 7, Compiler Collection provides a command-line interface-based (CLI-based) debugger, which can provide significant productivity boosts from basic to advanced features. Set breakpoints, examine variables, and navigate the call stack. You can even compile with optimization and parallelization flags along with debugging.

To improve application quality, advanced features such as Runtime Error Checking can help you catch hard-to-find bugs like memory access violations and memory leaks — before putting the application into production.

The Compiler Collection also includes an incremental linker to significantly reduce the link time of changes to your large applications during the debug cycle.

Language Development Systems

C compiler offers:

- ANSI C X3.159-1989 and K&R C support
- Mixed-mode capabilities to ease K&R to ANSI C transition

Native C++ compiler offers:

- Support for the ISO/IEC 14882:1998 C++ language standard
- Compatibility mode for easy migration from prestandard (ARM-style) ISO/IEC C++
- Class support for interval data types, enabling development of applications that guarantee answer correctness and solve nonlinear problems that are otherwise impossible to solve numerically
- Choice of the Sun binary-compatible default or STLport standard library
- OpenMP C++ v1.0 API support
- Native Connector support, allowing Java™ applications easy access to native C++ functions and classes

Libraries offer:

- IEEE 754 floating-point arithmetic
- Single-, double-, and quadruple-precision floating-point numerical formats
- Algebraic, transcendental, financial, rounding, conversion, and random number functions
- Multithreading support throughout the C++ libraries — not just limited to libC or iostreams
- Garbage collection to eliminate memory leaks
- Tools.h++ Class Library Version 7.1
- File space management
- An exception facility
- Multithreading compatibility with both UNIX® and POSIX threads

Fortran 95 compiler offers:

- Automatic loop parallelization
- Sun and Cray-style parallelization directives in Fortran
- Global Program Checking across multiple source files, now extended to perform static verification of OpenMP directives
- Full implementation of the following standards:
  - ANSI X3.198-1992 Fortran 90
  - ISO 1539:1991 Fortran 90
  - ISO/IEC 1539-1:1997 Fortran 95
- Improved support for the emerging Fortran 2000 standard; new keywords such as DECIMAL=, IOMSG=, ROUND=, and IEEE TR
- Interval arithmetic support, enabling development of applications that guarantee answer correctness and solve nonlinear problems that are otherwise impossible to numerically solve
- OpenMP Fortran v2.0 API support
- Cray extensions, such as Cray POINTER
- Compatibility with the discontinued Forte Compiler FORTRAN 77

Sun Performance Library component offers:

- Numerical routines optimized for maximum performance that are callable from C, C++, or Fortran, including:
  - LAPACK version 3.0
  - BLAS – 1,2,3
  - Fast Fourier transform (FFT) routines
  - Convolution and correlation routines
  - Sparse solver and BLAS routines
  - Interval BLAS routines
- Support for single-processor or multiprocessor systems
- Support for Fortran 95 language features
- Specially tuned version for UltraSPARC® processors (including UltraSPARC III chips)
- Support for 64-bit code on UltraSPARC platforms

Programming Environment

Building

- Executes build jobs in parallel on single or multiple machines distributed on a network

Debugging

- Command-line debugging of:
  - Multithreaded applications
  - Shared and dynamically linked libraries
  - Running processes
  - Debug optimized code
  - Assembly language programs
  - Java language support to seamless stepping through C, C++, Fortran, and Java programs
- Program control and data evaluation features:
  - Set conditional breakpoints, postbreak modifiers, and watchpoints
  - Trace program statements and variables
  - Navigate call stack
  - Evaluate expressions and functions
  - Monitor variables and expressions

Runtime Error Checking

- Detects memory access violations, run-time memory usage, and memory leaks:
  - Read/write from/to unallocated memory
  - Write to read-only memory
  - Read from uninitialized memory
  - Misaligned read/write
  - Bad/misaligned/duplicate free
  - Out of memory
- Integrated with debugger
  - Interactive or batch operation

Sun™ ONE Studio 7, Compiler Collection

Multithreading Development Tools

Multithreaded Debugging and Analysis

- Browse, select, and view active threads
- Control, evaluate, and modify specific threads
- Monitor thread entry point, current location status, pending event, and lightweight process

Multithreaded Locking Analysis (LockLint)

- Static source code analyzer for ANSI C code
- Captures locking design assertions
- Reports on potential synchronization errors, deadlock, and data race conditions

Multiprocessing (MP) Optimizations

- Automatic parallelization of C and Fortran code — detects loops that can be executed in parallel and generates code to distribute execution on SPARC MP systems
- Integrated in compiler optimization phases, avoiding source code preprocessing
- Support for the OpenMP Fortran v2.0 API, OpenMP C v1.1 API, and a subset of the OpenMP C++ v1.0 API

Licensing

- New product entitlement based on serial numbers eases license installation and administration
- Royalty-free run-time library (.so) distribution
- Attractive upgrade pricing available for existing licensed users

About Sun ONE

The Sun Open Net Environment (Sun ONE) is Sun's vision, architecture, platform, and expertise for delivering Services on Demand today and in the future. Based on open standards such as Java and XML technology, Sun ONE provides a highly scalable and robust framework for building and deploying a variety of Services on Demand — from traditional Web-based applications to future context-aware Web services. By simplifying the way Web services are created, assembled, and deployed, the Sun ONE platform can enhance productivity, speed time to market, and increase business opportunities for enterprises worldwide.

System Requirements

Software Recommendations

Solaris 9, 8, and 7 Operating Environments (SPARC Platform Edition) — Entire Distribution or Entire Distribution plus OEM Support
Netscape Navigator™ 4.0 or compatible JavaScript™ software-enabled browser
Compatible IDEs: Sun ONE Studio 4, Enterprise Edition or Forte Developer 6 update 2

Hardware Recommendations

Ultra™ 10 300-MHz system minimum; Ultra 60 360-MHz or Sun Blade™ 100 500-MHz system recommended
Memory: 256 MB minimum; 512 MB recommended
Swap Space: 512 MB minimum; 1024 MB recommended
Disk Space: 1.3 GB
CD-ROM for installation

For More Information

To learn more about Sun's complete and proven family of developer products, visit sun.com/developer-products.

For additional information on Sun ONE, visit sun.com/sunone.

Sun Microsystems, Inc. 901 San Antonio Road, Palo Alto, CA 94303-4900 USA **Phone** 800 786-7638 or +1 512 434-1577 **Web** sun.com

Sun ONE Studio 7, Compiler Collection

Licensing Information

Licensing for the Sun ONE Studio software has been greatly simplified through the implementation of a new serial number-based licensing model. This new licensing model:

- Makes it easier and faster for customers to install and run the software
- Simplifies the administration and management of licenses
- Standardizes the licensing model across the entire Sun ONE Studio product line so customers have a consistent experience

The Sun ONE Studio licensing model requires that the customer simply input a serial number license during installation. The customer is then able to begin using the software immediately. The serial number includes an RTU (right to use) that defines the number of users that can concurrently use the product.

The Sun ONE Studio licensing model does not enforce usage tracking, hence there is no service denial for the software. However, the customer is expected to abide by the terms and conditions of the RTU license and purchase the appropriate number of licenses to support the number of developers using the software.

This new licensing model will be used in all future releases of the Sun ONE Studio products - Sun ONE Studio 4 (formerly Forte for Java), and Sun ONE Studio 7 (formerly Forte Developer). Customers using Sun ONE Studio products will have a consistent user experience for licensing.

Differences from the Previous Licensing Model

The previous licensing model, which was implemented in the Sun Workshop and Forte Developer product lines, used the Globetrotter FLEXlm licensing software. The new Sun ONE Studio licensing model:

- Eliminates the need to call the License Center for a password to complete the installation process. The customer can simply install the serial number when prompted during the installation process, and he or she can then use the software immediately. Customers using the Try and Buy version of the software can also take advantage of this new feature. The customer can generate the trial serial number from the software product itself.
- Eliminates usage tracking and service denial. The new serial number licensing model does not track software usage, so there is no service denial based upon RTU usage. This new policy makes it easy for the developer's to use the Sun ONE Studio products. However the customer is bound by the legal terms and conditions of the RTU license so the customer must ensure that they have enough licenses to cover usage.

Benefits to the Developer Customer

The Sun ONE Studio licensing model eliminates the cost associated with license administration, and dramatically reduces the time and effort

required to install and maintain software licenses.

The developer customer will never experience service denial. Developers who are added to a project can use the software while waiting for the purchase and delivery of additional software licenses.

For more detailed information about the Sun ONE Studio licensing model please also see our Licensing FAQ and our Licensing technical white paper.

Maintain

- » Upgrades & Add-ons
- » Patches & Support
- » Newsletters
- » Previous Versions

NEC

13.453

Comprovação das Especificações Exigidas no Edital 050/2003

5. Unidade de backup

23/07/03

SUN STOREDGE L700 TAPE LIBRARY
Detailed View

Sun StorEdge L700
» Features, Functions & Benefits
» Specifications
□ Detailed View
» In the Spotlight

Storage Related:
» White Papers
» Success Stories
» Press Releases

See Also:
» Remote Management
» Professional Services
» Sun Servers
» PatchPro

Contact Me

Introduction

This library is available with either 9x40, (S)DLT, or LTO technologies. The Sun StorEdge L700 tape library and the Sun StorEdge L700 tape library with DLT 8000 are complementary products. A summary of these technologies in the Sun StorEdge L700 tape library is delineated in the following table:

Feature	9840	9840B	9940	DLT 8000	SDLT 320	LTO 1	LTO 2
Maximum Number of Drives	12	12	12	20	20	20	20
Maximum Native Throughput	120 MB/sec.	228 MB/sec.	360 MB/sec.	120 MB/sec.	320 MB/sec.	300 MB/sec.	600 MB/sec.
Maximum Number of Data Cartridge Slots	690	690	690	690	690	690	690
Number of Diagnostic and Cleaning Cartridge Slots	12	12	12	12	12	12	12
Maximum Native Capacity	13.5 TB	13.5 TB	129.6 TB	27.1 TB	108.4 TB	67.8 TB	129.6 TB

Back to Top

Features, Functions & Benefits

- HOT-SWAPPABLE COMPONENTS
- COMPACT FORM FACTOR

- ADVANCED TAPE TECHNOLOGY
- DIGITAL LINEAR TAPE TECHNOLOGY
- SERVER CONNECTIVITY
- FLEXIBLE ACCESS

HOT-SWAPPABLE COMPONENTS

Feature: Hot-plug drives and power supplies.

Function: Run-time exchange of drives and power supplies.

Benefit: Excellent performance, reliability, and availability.

COMPACT FORM FACTOR

Feature: Small footprint.

Function: 13 U of 19-inch rack space for integration of RAID, Fibre Channel hubs, switches, and other SAN components.

Benefit: Helps enable maintenance of resources and accessories in a single, secure enclosure.

ADVANCED TAPE TECHNOLOGY

Feature: Support for 9840B tape technology.

Function: The 9840B tape cartridge includes both the supply and takeup reels. This design allows for five-second load and 11 seconds average access time. Native capacity of each cartridge is 20 GB and archival life is estimated at 15 to 30 years.

Benefit: Helps decrease access times and increase data transfer rates.

DIGITAL LINEAR TAPE TECHNOLOGY

Feature: Support for digital linear tape SDLT 320 technology.

Function: Implements a simple tape path operating at a low constant tension.

Benefit: Helps increase data transfer rates, lowers tape wear-and-tear, and is backward compatible with DLT 7000/8000.

SERVER CONNECTIVITY

Feature: Support for Java technology.

Function: Java technology-based Web server for monitoring and diagnosis.

Benefit: The library remains competitive and protects your investment.

FLEXIBLE ACCESS

Feature: Cartridge access port can be accessed via the front panel in offline mode.

Function: The cartridge access port can be controlled via either software or front panel.

Benefit: Highly accessible and easy to use productivity tool.

Back to Top

Highlights

Typical Applications

- Backup for active-use databases ranging from 9.1 to 27.6 TB
  To enable capacity for multiple backups of data—daily, weekly, and monthly—tape capacity should be configured for at least three to five times the capacity of online storage.
- Archival
- Hierarchical storage management (HSM)
- Quick information retrieval

Software Compatibility

The Sun StorEdge L700 tape library is supported by VERITAS NetBackup software, Solstice Backup software, and many other storage management software applications including:

- Oracle (including Oracle on Microsoft Windows NT)
- Informix
- SAP
- Microsoft Exchange
- Microsoft SQL server
- Lotus Notes on Microsoft Windows NT and on SPARC systems
- Sybase

Ease of Management

Also available in the Sun StorEdge L700 library is library monitoring software. This monitoring software utilizes the Ethernet network port and Web server embedded in the Sun StorEdge L700 tape library. The monitoring software is out-of-band, in that it is fully independent of the library SCSI control path, the data SCSI path, and the server (s) to which the library is connected.

Back to Top

Enabling Technology

The Sun StorEdge L700 tape library includes a number of features that makes it especially well-suited to data center environments. They include:

- Hot-plug drives and power supplies for outstanding RAS features
- 13U of 19-inch rack space for custom integration of RAID or Fibre Channel hubs—enables maintenance of resources and accessories in a single, secure enclosure
- 9840B tape technology helps decrease access times and increase data transfer rates
- 9940, LTO 2, and SDLT technologies help enable the largest amount of capacity in this library
- Java technology-based Web server for monitoring and diagnosis helps enable the library to remain competitive in the long run, thus protecting customers' investments
- A highly accessible load port, via software or front panel
- Tapes drives (and their data cartridges) can be shared by multiple hosts

Highly Reliable Robotic Technology

The Sun StorEdge L700 tape library uses advanced rotational robotics, which uses a rotational mechanism for horizontal positioning. The unit needs no adjustments or

lubrication, and is designed for a cycle life of over one million cycles.

Digital Linear Tape Technology Overview

Digital linear tape (DLT) technology uses multichannel linear or serpentine recording. Linear or serpentine technology uses a multichannel tape. The tape carries data in parallel channels that run past a single stationary head. Each of the channels passes over its own write element within the head. The use of four channels with the DLT 8000 essentially doubles data transfer rates compared to the DLT 4000 (two channels).

Media and read/write head durability further distinguish digital linear tape technology from other offerings. Digital linear tape implements a simple tape path and operates at a low constant tension, with the tape head being stationary, helping to minimize wear-and-tear on both tape and heads. In contrast, helical scan technology utilizes a read/write head positioned on a rotating drum. The drum lays data down diagonally across a slow-moving tape. Because the tape is wrapped around the rotating drum, tape and head life are usually lower.

Future digital linear tape products will easily grow in capacity by increasing bit density. Performance improvements occur through the addition of new heads and channels, or by increasing the tape speed.

Digital linear tape offers several advanced features, such as full SCSI-2 command set implementation, built-in diagnostics, and a high (native) data transfer rate of 6 MB/sec. The current version of DLT 8000 tapes has a native capacity of 40 GB per cartridge. The digital linear tape cost per megabyte is comparable to 8-mm technology. As digital linear tape technology evolves to higher-capacity tapes and higher transfer rates, it is a suitable option for enterprise environments where storage needs are increasing rapidly.

Adaptive Cache Buffering Scheme

The DLT transfer rate could surpass that of many host computers. DLT overcomes this potential issue by using an adaptive cache buffering scheme. Host data rates are monitored and the drive automatically adjusts its transfer rate to match that of the system. This helps minimize the number of times the drive has to stop and reposition.

9840B Tape Technology Overview

The 9840B tape drive is a high-performance tape drive designed for the enterprise and multiplatform environments. Performance characteristics of the drive are as follows:

Tape load and initialize to ready	5 sec.
Search time	8 sec. (first search) and 11 sec. (average)
Maximum rewind time	16 sec.
Data buffer size	8 MB/drive
Maximum block size	256 KB

The 9840B tape cartridge is a 1/2-inch cartridge and includes both the supply and takeup reels. This design allows for five second load and 11 seconds average access time. When inserted in the drive, the cartridge and tape are pressed against the read/write path in the drive, and the drive servo mechanisms engage the supply and take-up reels in the cartridge. Each cartridge weighs 262 grams, or 9.17 ounces. The media itself is based on advanced media particle technology with polyethylene napthalate (PEN) substrate. Native capacity of each cartridge is 20 GB and archival life is estimated at 15 to 30 years.

The 9840B was designed to work in automated environments and specifically targets environments needing fast cartridge loads (that is, fast cartridge hand-offs from the library gripper to the drive). This allows for fast access to the first byte and frees the library to service other mount/dismount requests. With a load time of five seconds, the

9840B significantly outperforms any other tape drive. The following table lists the rates for several characteristics of the 9840B drive.

Data transfer rate (uncompressed)	19 MB/sec.
Load time	5 sec.
Unload time (includes rewind)	4 sec.
Average search time (excluding load)	8 sec.
Average rewind time	8 sec.
Time to backup 100 MB	21 sec.
Time to locate (load and search)	12 sec.

Vision System

The Sun StorEdge L700 tape library uses an advanced digital vision system for cartridge management, adaptive targeting, and self-calibration. Due to this advanced capability, there is no scheduled manual calibration or other maintenance of the Sun StorEdge L700 tape library. In addition, this system not only reads regular bar code labels but also marginal bar code labels that off the shelf scanning systems have difficulty reading. Another function of the vision system is the ability to read multiple types of bar codes, including the traditional StorageTek Tri-Optic bar code labels, CompacTape IV, and 9840 Tri-Optic labels.

Bar Code Label Support

Cartridge labels can be purchased through StorageTek by calling (800) 905-8502 (US).

Cartridge Access Port (CAP)

The cartridge access port (CAP) contains up to 20 cartridges in four five-cartridge, removable magazines. An additional CAP can be purchased to allow loading of up to 40 cartridges (total). (Note that utilizing the second CAP replaces the viewing window of the library.)

The cartridge access port(s) can be controlled via either software or the front panel. If using backup software, it is recommended that the software be used to transfer cartridges from the bins to the cartridge access ports (and vice versa), as this will keep the inventory correct within both the software and the hardware. In the offline mode, the cartridge access port(s) can be accessed via the front panel without problems.

Removable Magazines

The removable magazines boast a patented easy-loading feature that helps enable them to swing out for loading and unloading, or lift out for remote storage or vaulting.

Gripper Mechanism

The Sun StorEdge L700 tape library's wide-based gripper mechanism is designed to enhance cartridge stability and enable faster moves. The gripper and cartridge slot design allow efficient handling of both DLT 8000 and 9840 cartridges. In addition, the advanced cartridge-cell design provides pinpoint cartridge location, resulting in simpler mechanics. That means that the gripper mechanism need not reposition the cartridge, thus allowing faster, more accurate, and more reliable movements.

The library also features fast audit times. An audit of the library's cartridges and drives takes at most five minutes with a fully loaded library.

Operator Panel

13.447

The operator panel contains buttons, indicators, and a large graphic display. The panel shows cartridge access port information, tape library and drive status, tape library and drive configuration, test sequences, and error and event information. The panel is also capable of showing the current firmware for the robotics and the drives.

Architectural Design

The following figures depict the architectural design of the Sun StorEdge L700 tape library.

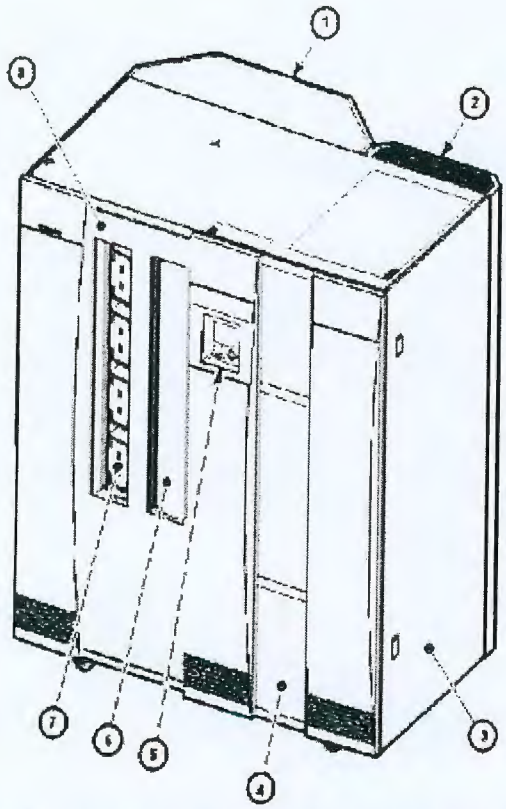
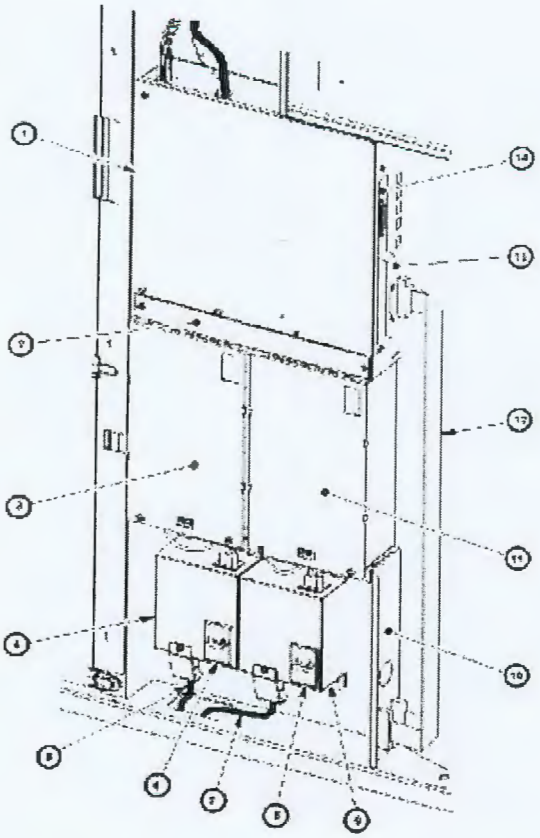


Figure 2. Sun StorEdge L700 tape library major external components

Major external components of the Sun StorEdge L700 tape library are shown in the figure above. These features are:

1. Expansion frame
2. Rear door
3. Drive access door
4. Right front door
5. Operator panel
6. Optional cartridge access port (CAP)
7. Standard cartridge access port (CAP)
8. Left front door

Figure 3. Sun StorEdge L700 tape library electronic components



The major electronic components of the library are shown in the figure above. These components are located behind the right front door of the library.

1. Main processor card (MPC) and associated logic cards
2. Fan tray assembly
3. Standard DC power supply
4. Standard AC power distribution unit (PDU)
5. AC power cable
6. Circuit breaker
7. Optional second power cable
8. Optional second circuit breaker
9. Optional AC power distribution unit (PDU)
10. Library-to-host SCSI I/O connectors
11. Optional second DC power supply
12. Internal host-to-library controller cable
13. MPC card SCSI control connectors
14. Fibre Channel connections

Back to Top

Reliability, Availability, and Serviceability (RAS)

Reliability

The Sun StorEdge L700 library robotics are designed, built, and tested for extreme durability.

- Mean swaps between failure (MSBF): One million hours
- Mean time between failure (MTBF): 70,000 power-on hours (robotics)

Availability

The Sun StorEdge L700 library offers high reliability through several functional

characteristics.

Tape Drives and Trays

The tape drives and power supplies reside in hot-pluggable, customer-serviceable trays, which can be quickly replaced without special tools. The drive trays use blind-mate drawer connectors, making drive replacement easy.

Optional Redundant Power Supplies

The Sun StorEdge L700 tape library features optional redundant power supplies (for the robot only). Firmware contains failure-monitoring capabilities. The hot-swappable power supplies share the load so if one fails, the other will continue without interrupting service.

The second power option allows running the unit from two power circuits. Note that the power to the robot is completely redundant, but drives 1 through 6 are on one circuit and drives 7 through 12 are on the second circuit (for 9840 drives). Thus, if one circuit fails, all the drives on that circuit go down. Drives 1 through 10 are one circuit and drives 11 through 20 are on the second circuit for DLT 8000 drives. The application will have to steer towards the operational drives (this is not simple failover).

Cooling System

The Sun StorEdge L700 tape library's cooling system can continue to function while service personnel replace a cooling fan. The fans feature highly reliable ball-bearing construction specified for a mean time between failures (MTBF) of 70,000 hours. If one fan fails, operation continues uninterrupted. The firmware uses rotation sensing to monitor fan speed. If a fan begins to fail, it will trigger a failure event notification.

Messaging System

The Sun StorEdge L700 tape library's messaging system can notify personnel of types and locations of failures via email and pages. A network port permits monitoring and configuration while the library is in use without disturbing data movement operations.

This library supports TapeAlert, which defines a standard notification format for possible system failures. The firmware monitors drive and library performance statistics to warn of possible drive or library component failure. The automated notification system sends a warning when drive or library performance parameters fall below specified limits.

Streamlined Subassemblies

All subassemblies have been streamlined. For example, cabling was simplified to reduce the number of connectors. Also, the cartridge-gripper mechanism uses a quiet, simple design resulting in high performance. This minimalist approach helps enable the Sun StorEdge L700 tape library to yield both high value and reliability.

Maintenance

The Sun StorEdge L700 tape library requires no periodic maintenance — no lubrication or belt retensioning. It was designed with highly integrated electronics. All the main library functions reside on a single controller card, resulting in a more reliable, cost-effective solution than a motherboard with plug-in modules.

Vision System

Self-calibration of the Sun StorEdge L700 tape library's patented digital vision system helps enable it to adapt to any mechanical parameters that might change over time. It makes a more robust, reliable library that will perform dependably over the long run.

9840 Media

The 9840 media does not require retensioning, which means that the cartridge does not periodically have to be loaded into a drive and the media retensioned. The benefit is that the data and all drives are continuously available. No drives need to be dedicated to maintenance functions. In addition, the 9840 media can be stored flat or on edge without media distortion or loss of data.

Service Access Requirements

The Sun StorEdge L700 tape library has a full-size door on its right side (when viewed from the front) that provides access to the drives and host cables. This door requires a clearance of three feet. No other equipment can be placed in this clearance space in order to ensure space for servicing.

Back to Top

Specifications

CAPACITY AND PERFORMANCE

Drives	9940B	SDLT 320	LTO	DLT8000	9840B	9840
Library Capacity (native, with 678 tapes)	135.6 TB	110.4 TB	135.6 TB	27.1 TB	13.8 TB	13.56 TB
Cartridge Capacity (native)	200 GB	160 GB	100 GB	40 GB	20 GB	40 GB
Sustained Transfer Rate (native, concurrent operation of all drives)	12	20	20	20	12	12
Tape Load Time (to BOT)	12 seconds	10 seconds	12 seconds	4 seconds	4 seconds	4 seconds
Average File Access Time	70 seconds	76 seconds	76 seconds	60 seconds	11 seconds	11 seconds

LIBRARY & ROBOTICS

Average cartridge swap time	Seven seconds
Robotics MSBF	One million load/unload cycles
Robotics MTBF	70,000 power-on hours
MEBF	Two million exchanges
Hot-plug drives	Yes
Redundant power	Yes (for robotics only, via second drive column)
Startup/boot time	Three to four minutes (average)
Burst rate (each drive)	40 MB/sec
Inventory time	Less than six minutes (fully loaded, with barcodes)
Robotics	v1.0

INTERFACES

Ultra differential	Fast/Wide SCSI-2

SCSI	Wide, high-voltage differential
LVD	Low-voltage differential
Native 2 Gbit Fibre Channel	LC connection
Control Panel	Low-Voltage differential

SOFTWARE

Operating System	Solaris Operating Environment v2.6, 7, 8, and 9
Software Compatibility	Sun StorEdge Utilization Suite software VERITAS NetBackup software v3.2 or later VERITAS Storage Migrator software v3.2 or later Solstice Backup software v5.5.1 or later

HARDWARE

Hardware Compatibility	Sun Enterprise 250, 450, 3x00, 4x00, 5x00, 6x00, and 10000 servers Sun Fire V880, 3800, 4800, 4810, 6800, and 15K servers

ENVIRONMENT

Operating	15ºC to 32ºC (59ºF to 90ºF) 20% to 80% relative humidity, noncondensing
Nonoperating	-20ºC to 60ºC (-4ºF to 140ºF) 5% to 95% relative humidity, noncondensing

ELECTRICAL

	Library Enclosure	Single-drive column
Power cable US/Canada	100 VAC UL/CSA	120 VAC UL/CSA
Input voltage range	90 to 254 VAC	90 to 254 VAC
Nominal voltage (per power supply)	120 or 240 VAC	120 or 240 VAC
Power configuration US/Canada	Single-phase 100 VAC, 47 to 63 Hz	Single-phase 120 VAC, 47 to 63 Hz
Power consumption	210 W	972 W
Maximum heat output	716 BTU/hr	3314 BTU/hr

REGULATIONS

Meets or exceeds the following requirements:

Safety	UL1950 listed, CSA C22.2-No. 950-M89, TUV-EN60950
Emissions	FCC Part 15B Class A, CE Mark, VCCI Class A

DIMENSIONS AND WEIGHTS

Height	183 cm (72 in.)
Width	156 cm (62 in.)
Depth	110 cm (43.5 in.) (with expansion door) 95 cm (37.5 in.) (without expansion door)

Weight	427 kg (941 lb.) (without drives or cartridges)
WARRANTY	
One year warranty	15-day parts exchange

Back to Top

System Management

System Administration

LCD Control Panel

The Sun StorEdge L700 library control panel contains the necessary routine to enable the library configurations using the control panel, and it can run some diagnostic routines.

Diagnostics

The Sun StorEdge L700 tape library includes extensive built-in diagnostics that can be used to conduct system tests. Diagnostics are stored in flash memory and are divided into three levels:

- Startup
- Run-time
- Remote

At power-up, or reset, the Sun StorEdge L700 tape library runs through a self-check initialization sequence that verifies major systems are functional and operating within normal ranges. The system configuration, vision and targeting, servo ranges and operations, tape drive interfaces, operator panel and tape inventory are all checked, before the library goes ready. Errors that would prohibit normal use of the library cause the startup sequence to terminate, and the fault to be displayed on the front operator panel.

Run-time diagnostics can be run locally from the front operator panel of the Sun StorEdge L700 tape library or remotely via a serial port. With the run-time diagnostics, the library robotics and tape drives can be exercised and tested. The following diagnostic functions can be run:

- Get and put a tape cartridge to and from a cell, with full range of robotic motion and reach tested
- Mount and dismount cartridge to a selected tape drive
- "Demo mode" to exercise random puts and gets of tape cartridges throughout the library
- Tape drive cleaning
- View the fault symptom code event log
- View library and drive firmware levels

Supported Software

The Sun StorEdge L700 tape library supports:

- VERITAS NetBackup
- Solstice Backup
- Sun StorEdge Utilization Suite

VERITAS NetBackup and Solstice Backup Software

The Sun StorEdge L700 tape library is supported by VERITAS NetBackup software,

Solstice Backup software, and many other storage management software applications. If VERITAS NetBackup software is used, a robotics license is needed for every drive that is used in the library. If Solstice Backup software is used, an autochanger software module license (with unlimited slots) is required.

Note: *Solstice Backup software does not currently support multimedia. Also note that some versions of VERITAS NetBackup and Solstice Backup software may require patches.*

The Sun StorEdge L700 library is supported on leading database applications as shown in the table below.

Database	Solstice Backup software	VERITAS NetBackup
Oracle on UNIX® and Solaris Operating Environment	X	X
Informix on UNIX and Solaris Operating Environment	X	X
SAP on UNIX and Solaris Operating Environment	X	X
SAP on Microsoft Windows NT	X	X
Microsoft Exchange	X	X
Microsoft SQL Server	X	X
Oracle on Microsoft Windows NT	X	X
Lotus Notes on Microsoft Windows NT	X	Starts with 3.4
Lotus Notes on UNIX and Solaris Operating Environment	X	Starts with 3.4
Sybase on UNIX and Solaris Operating Environment	X	X

Useful Software Commands

For information about software commands, refer to the *Solaris Handbook for SMCC Peripherals* or the AnswerBook software documentation for your operating system. The *Solaris Handbook for SMCC Peripherals* also describes how to determine which SCSI target IDs are available and how to configure your system after installation.

Back to Top

Service and Support

The SunSpectrum program is an innovative and flexible service offering that allows customers to choose the level of service best suited to their needs, ranging from mission-critical support for maximum solution availability to backup assistance for self-support customers. The SunSpectrum program provides a simple pricing structure in which a single fee covers support for an entire system, including related hardware and peripherals, the Solaris Operating Environment software, and telephone support for Sun software packages. The majority of Sun's customers today take advantage of the SunSpectrum program, underscoring the value it represents. Customers should check with their local Sun Enterprise Services representative for program/feature variance and availability in their area.

Support Contracts

SunSpectrum program support contracts are available both during and after the warranty program. Customers may choose to uplift the service and support agreement

to meet their business needs by purchasing a SunSpectrum support contract.

The four levels of SunSpectrum support contracts are outlined below.

SunSpectrum Program Support

Program	Description
Mission-Critical SunSpectrum Platinum Support	Designed to support client-server, mission-critical solutions by focusing on failure prevention, rapid recovery and year-round technical services planning. Support is provided 24 x 7.
Business-Critical SunSpectrum Gold Support	Includes a complete package of proactive and responsive services for customers who require maximum uptime for their strategic business-critical systems. Support is provided 24 x 7.
System Coverage SunSpectrum Silver Support	Combines the service expertise, responsive on-site support, and technical support by telephone and SunSolve CD/on-line services. Support is provided 8 a.m. to 8 p.m., Mon. through Fri.
Self-Directed SunSpectrum Bronze Support	Provided for customers who rely primarily upon their own in-house service capabilities. Enables customers to deliver high-quality service by giving them access to UNIX system expertise, Sun certified replacement parts, software releases and technical tools. Support is provided 8 a.m., to 5 p.m. Mon. through Fri.

The Sun StorEdge L700 tape library is supported only by the SunSpectrum Gold or Platinum program levels.

Warranty

The Sun StorEdge L700 tape library comes with a one-year warranty and 15-day parts exchange.

Back to Top

1. This page meets my need. disagree ○ ○ ○ ○ ○ ○ ○ agree

2. This page was easy to find. disagree ○ ○ ○ ○ ○ ○ ○ agree

Sun StorEdge™ Enterprise Backup Software

Simplified, centralized, automated data protection across heterogeneous environments.

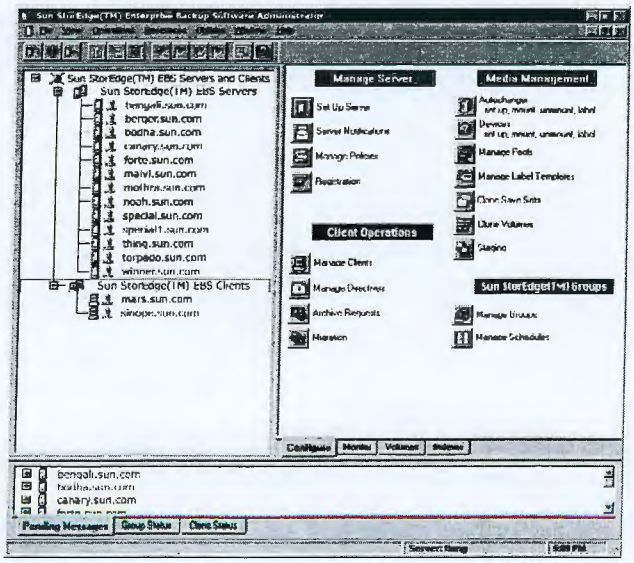
Simple
Scales seamlessly from small business/departmental environments to multi-terabyte data centers, resulting in investment protection and simplified installation, training, and support.

Centralized and open
Simplifies, centralizes, and automates data backup and recovery across a variety of operating systems, applications, and SAN, NAS, or DAS storage. Backup devices can be a single tape drive, tape libraries, silos, or disk arrays (JBOD, RAID, NAS).

Automated
Provides automated, online backup, impact-free protection, and granular-level restore for leading databases, messaging, and ERP applications, to help meet service level criteria.

Superior architecture
Automated, multi-tier storage management offers optional staging to intermediate high-speed disk. Built-in multiplexing of client backup streams enables full leverage of drive speeds and tape compression ratios. Unique write once/read many Client File Index prevents corruption and delivers optimal efficiency to speed backup and recovery operations.

Simplify the backup, recovery, and archiving needs of your enterprise.
As an integral component of Sun's data continuance solutions, Sun StorEdge™ Enterprise Backup software delivers centralized data protection and management across heterogeneous environments. Features such as advanced indexing, high speed parallelism, automated media management, LAN-free and serverless backup, cluster awareness, comprehensive network data management protocol (NDMP) support, and dynamic tape drive sharing enable administrators to fully protect storage assets and minimize downtime. For hands-free data protection, the software's Autochanger and Silo Modules support an extensive variety of Sun StorEdge tape and robotic devices. And the DiskBackup™ Option allows data to be backed up to disk, staged from disk, and automatically moved to tape, or cloned from disk to tape or disk—all with single-step recovery. The software's Application Modules deliver "hot" backup and granular recovery for Oracle, Microsoft SQL Server, IBM DB2, IBM Informix, Sybase, Microsoft Exchange, IBM Lotus Notes/Domino, and SAP. Combine Sun StorEdge Enterprise Backup software with Sun StorEdge Availability Suite software's instant snapshot capability to achieve an even higher level of impact-free data protection. Simplify your Storage with Sun StorEdge solutions.



Sun StorEdge™ Enterprise Backup Software

Product Specifications

Purchase this product from the Sun℠ Store, **sun.com/store**, or contact an authorized Sun reseller near you.

Sun StorEdge Enterprise Backup Software	Power Edition	Network Edition	Workgroup Edition	Business Edition
Number of pre-configured client connections	10	10	8	8
Parallel data streams per server	64	32	12	12
Parallel data streams per storage node (SN)	32	32	N/A	N/A
Number of devices	32 per server and/or SN	16 per server and/or SN	4	4
Cluster support—Server/Client	Server/Client	Client	N/A	Client
Storage nodes	Yes	Yes	N/A	N/A
Library sharing	Yes	Yes	No	No
Supported Options, Modules, Complementary Products				
Additional client connections	Yes	Yes	No	No
ClientPaks for heterogeneous environments	Yes	Yes	Yes	Yes
Sun StorEdge Enterprise Backup software NDMP client connections	Yes	Yes	No	Yes
Dynamic drive sharing option	Yes	Yes	No	No
Sun StorEdge Enterprise Backup software DiskBackup™ Option	Yes	Yes	Yes	Yes
Sun StorEdge Enterprise Backup software Archive Module	Yes	Yes	Yes	Yes
AutoChanger Software Modules	1-9, 1-16, 1-32, 1-64, 1-128, 1-256, 1-400, 1-700 slots		1-9, 1-16, 1-32 slots	1-26 slots (included)
Silo Software Modules	Unlimited slots	Unlimited slots	No	No
Sun StorEdge Enterprise Backup software Application Modules	Yes	Yes	Yes	Yes
DiskXtender UNIX/Linux	Yes	Yes	Yes	Yes
DiskXtender2000—Windows 2000 and NT	Yes	Yes	Yes	Yes
Sun StorEdge Enterprise Backup software Management Console	Yes	Yes	Yes	Yes
Sun StorEdge Enterprise Backup software Operations	Yes	Yes	Yes	Yes
Sun StorEdge Enterprise Backup software Availability	Yes	Yes (excluding clustering)	Yes (excluding clustering)	Yes (excluding clustering)
Sun StorEdge Enterprise Backup software AlphaStor	Yes	Yes	No	No
SNMP Module	Yes	Yes	No	No
HP-IT Operations, Tivoli, CA-UniCenter support	Yes	Yes	No	No

Sun StorEdge Enterprise Backup Software Servers/Storage Nodes/Clients

SERVERS	STORAGE NODES	CLIENTS
Sun Solaris (SPARC and 1A-32)	Microsoft Windows 2003/2000 (1A-32, 1A-64)	Microsoft Windows 2003/2000 (1A-32, 1A-64)
Red Hat Linux (1A-32)		Microsoft Windows XP
Red Hat Advanced Server Linux (1A-32)		Microsoft Windows 98
SuSE Linux (1A-32)		Microsoft Windows 95
SuSE Enterprise Server 7 (1A-32, 1A-64)	Sun Solaris (SPARC and 1A-32), Sun OS	Sun Solaris (SPARC and 1A-32), Sun OS
	HP-UX (PA-RISC)	HP-UX (PA-RISC)
	HP Tru64 UNIX (Alpha)	HP Tru64 UNIX (Alpha)
	IBM AIX (POWER)	IBM AIX (POWER)
	Red Hat Linux (1A-32)	Red Hat Linux (1A-32)
	Red Hat Advanced Server Linux (1A-32)	Red Hat Advanced Server Linux (1A-32)
	SuSE Linux (1A-32)	SuSE Linux (1A-32)
	SuSE Enterprise Server 7 (1A-32, 1A-64)	SuSE Enterprise Server 7 (1A-32, 1A-64)
		Macintosh OS X

For additional information on this product, go to *www.sun.com/storage/software/data_services/backup/*

Sun Microsystems, Inc. 4150 Network Circle, Santa Clara, CA 95054 USA **Phone** 1-800-555-9SUN or 1-650-960-1300 **Web** sun.com/storage

Sun microsystems
We make the net work.

SUN

[Return to Non Printer Friendly Page]

Sun StorEdge[tm] L700 Tape Library: Hardware Specifications

Tape Drives	
9840	Wide, HV Differential SCSI 20 GB Tape Drive
9840B	9840B Fibre Channel drive, 19 MB/sec transfer rate, 20 GB native capacity and a 2 GB Fibre Channel interface
9940B	9940B Fibre Channel, 30 MB/sec transger rate, 200GB native capacity tape drive
DLT[tm] 7000	DLT 7000 Wide, HV Differential SCSI 35 - 70 GB Tape Drive
DLT 8000	DLT 8000 Wide, HV Differential SCSI 40 - 80 GB Tape Drive
LTO	LTO High Voltage Differential SCSI Tape Drive (Seagate)
LTO2	LTO Generation II Low Voltage Differential SCSI Tape Drive
LTO FC	LTO Fibre Channel Tape Drive (IBM)
LTO Gen II Fibre Channel	LTO Fibre Channel, 30 MB/sec transfer rate, 200 GB native capacity tape drive
SDLT320	Super DLT320 High Voltage Differential SCSI Tape Drive

Environment	Library Enclosure	Single Drive Column
AC Voltage Range	90 - 254 VAC	90 - 254 VAC
Power Cable	**US/Canada** - 100 VAC UL/CSA	**US/Canada** - 120 VAC UL/CSA
Power Configuration	**US/Canada** - Single phase 100 VAC, 47 to 63 Hz	**US/Canada** - Single phase 120 VAC, 47 to 63 Hz
Power Consumption	210 W	972 W
Maximum Heat Output	716 BTU/hr	3,314 BTU/hr
Temperature & Humidity	**Operating:** 15 °C to 32 °C (59 °F to 90 °F), 20% to 80% noncondensing relative humidity **Nonoperating:** -20 °C to 60 °C (-4 °F to 140 °F), 5% to 95% noncondensing relative humidity	
Altitude	**Operating:** 0 to 3,050 M (0 to 10,000 feet) **Nonoperating:** 0 to 15,240 M (0 to 50,000 feet) shipping **Nonoperating:** 0 to 3,050 M (0 to 10,000 feet) storage	

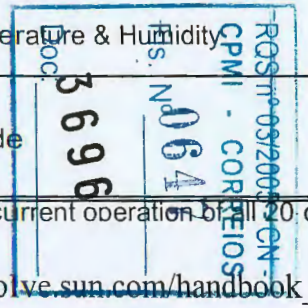
cm (72 in)

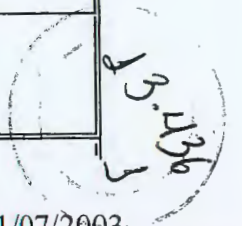
Tape Drives	
9840	Wide, HV Differential SCSI 20 GB Tape Drive
9840B	9840B Fibre Channel drive, 19 MB/sec transfer rate, 20 GB native capacity and a 2 GB Fibre Channel interface
9940B	9940B Fibre Channel, 30 MB/sec transger rate, 200GB native capacity tape drive
DLT[tm] 7000	DLT 7000 Wide, HV Differential SCSI 35 - 70 GB Tape Drive
DLT 8000	DLT 8000 Wide, HV Differential SCSI 40 - 80 GB Tape Drive
LTO	LTO High Voltage Differential SCSI Tape Drive (Seagate)
LTO2	LTO Generation II Low Voltage Differential SCSI Tape Drive
LTO FC	LTO Fibre Channel Tape Drive (IBM)
LTO Gen II Fibre Channel	LTO Fibre Channel, 30 MB/sec transfer rate, 200 GB native capacity tape drive
SDLT320	Super DLT320 High Voltage Differential SCSI Tape Drive

pansion door

Environment	Library Enclosure	Single Drive Column
AC Voltage Range	90 - 254 VAC	90 - 254 VAC
Power Cable	**US/Canada** - 100 VAC UL/CSA	**US/Canada** - 120 VAC UL/CSA
Power Configuration	**US/Canada** - Single phase 100 VAC, 47 to 63 Hz	**US/Canada** - Single phase 120 VAC, 47 to 63 Hz
Power Consumption	210 W	972 W
Maximum Heat Output	716 BTU/hr	3,314 BTU/hr
Temperature & Humidity	**Operating:** 15 °C to 32 °C (59 °F to 90 °F), 20% to 80% noncondensing relative humidity **Nonoperating:** -20 °C to 60 °C (-4 °F to 140 °F), 5% to 95% noncondensing relative humidity	
Altitude	**Operating:** 0 to 3,050 M (0 to 10,000 feet) **Nonoperating:** 0 to 15,240 M (0 to 50,000 feet) shipping **Nonoperating:** 0 to 3,050 M (0 to 10,000 feet) storage	

c (concurrent operation of all 20 drives)





Dimensions and Weights

Height	183 cm (72 in)
Width	156 cm (62 in)
Depth	110 cm (43.5 in) with expansion door 95 cm (37.5 in) without expansion door
Weight	427 kg (941 lb) without drives or cartridges 776 kg (1,710 lb) with 12 9840 drives, 690 cartridges, and expansion door 755 kg (1,664 lb) with 20 DLT 8000 drives, 690 cartridges, and expansion door

Regulations

Meets or exceeds the following requirements:

Safety	UL 1950 listed , CSA C22.2-No 950-M89, TUV-EN60950
Emission	FCC Part 15B Class A, CE Mark, VCCI Class A

Capacity and Performance	9940B	9840	9840B	DLT 7000	DLT 8000	LTO	LTO 2	LTO FC	LTO Gen II FC	SDLT320
Number of tape drives	12	12	n/a	20	20	20	20	20	20	20
Number of cartridges Data: Cleaning/Diagnostic:	678 12	678 12	n/a n/a	678 12	678 12	678 12	678 12	678 12	678 12	678 12
Cartridge capacity	200 GB (native)	20 GB (native)	20 GB (native)	35 GB (native)	40 GB (native)	100 GB	200 GB	100 GB	200 GB*	160 GB
Library capacity	135.6 TB (native)	13.8 TB (native)	n/a	24.0 TB (native)	27.6 TB (native)	67.8 TB	135.6 TB	67.8 TB	135.6 TB	110.4 TB
Drive transfer rate	30 MB/sec	9 MB/sec	19 MB/sec	5 MB/sec	6 MB/sec	15 MB/sec	30 MB/sec	15 MB/sec	30 MB/sec	16 MB/sec
	360 MB/sec	120 MB/sec		100 MB/sec	120 MB/sec	300 MB/sec	600 MB/sec	300 MB/sec	600 MB/sec	320 MB/sec

Library transfer rate	(concurrent operation of all 12 drives)	(concurrent operation of all 12 drives)	n/a	(concurrent operation of all 20 drives)	(concurrent operation of all 20 drives)	(concurrent operation of all 20 drives)	(concurrent operation of all 20 drives)	(concurrent operation of all 20 drives)	(concurrent operation of all 20 drives)	(concurrent operation of all 20 drives)
* - When using LTO Gen 2 200GB media. If using LTO Gen 1 (100GB) media in LTO Gen 2 drive, you get 33% better Read/Write performance over using the same data cartridge in an LTO Gen 1 drive.										

Doc (4

LTO Ultrium Generation 2

tape drives from StorageTek

StorageTek Tape Products

Key Business Benefits

> **Generous, scalable capacity**
Up to 200 GB uncompressed can be stored on just one cartridge, reducing media costs while accommodating data growth.

> **Significantly reduced backup windows**
Handle double the amount of information in the same amount of time as before.

> **The right drive for the job**
Get the best tape drive for your environment and meet midrange streaming backup needs well into the future.

> **Exceptional performance**
Capabilities such as dynamic data rate matching and dual mode compression enhance performance and product life.

> **Easy and seamless integration**
Backward read and write compatibility to the LTO Generation 1 drive means easy integration and seamless operation between drive and library, as well as protecting your LTO technology investment.

> **Data protection**
Powerful correction and verification capabilities protect data integrity and prevent data loss.

> **Superb reliability**
More than 100,000 load/unloads and one million tape passes before failure keep you up and running.

> **Connectivity.**
Available with either Ultra 3 SCSI at 160 MB/sec or FC-2, 2 Gigabit (200 MB/sec) Fibre.

Double your capacity without adding library slots

Nothing is going to stop rapid data growth. But the new generation of Linear Tape Open (LTO) Ultrium technology tape drives, combined with StorageTek L-Series tape libraries, provide a scalable, affordable open format solution that relieves storage stress today and positions you for tomorrow's growth.

Built on the proven reliability, performance and affordability of existing LTO technology, LTO Ultrium Generation 2 tape drives deliver twice the native capacity – up to 200 GB on a single cartridge – of earlier LTO tape drives.

Handle twice the information in the same amount of time. LTO Generation 2 tape drives also double throughput with native data transfer rates at speeds up to 35 MB per second. This dramatically reduces backup windows. And, because LTO Generation 2 tape drives fit seamlessly into StorageTek's highly scalable, mixed-media automation solutions, you have the flexibility to balance subsystems, application needs and budget realities and get the performance you need to easily handle data-intensive applications.

Protect your investments, data and future. Only StorageTek offers and supports LTO tape drives from multiple vendors. We'll help determine the best solution for your business now and in the future. And LTO Generation 2 tape drives' compatibility with StorageTek L-Series tape libraries, earlier LTO tape drives and leading backup and management software helps you leverage what you already own.

Offering LTO Generation 2 tape drives reaffirms StorageTek's commitment to providing real choices and true mixed-media automation to protect your data as well as your bottom line.

STORAGETEK

649

13.432

LTO Ultrium Generation 2 specifications

	HP	IBM
Capacity and performance		
Capacity, native (uncompressed)	200 GB	200 GB
Performance, native (uncompressed)	30 MB/sec[1]	35 MB/sec[2]
Access times[3]		
Tape load and thread to ready	19 sec	15 sec
Average file access time	52 sec	49 sec
Maximum/average rewind time	104/52 sec	98/49 sec
Unload time	13 sec	15 sec
Tape format		
Recording format	Ultrium Generation 2	Ultrium Generation 2
Number of channels	8	8
Reliability		
Mean time between failures (MTBF)		
Power on	250,000 hr @ 100% duty cycle	250,000 hr @ 100% duty cycle
Uncorrected bit error rate	$1x10^{-17}$	$1x10^{-17}$
Undetected bit error rate	$1x10^{-27}$	$1x10^{-27}$
Cartridge uses; recommended full passes	150	150
Interface data		
SCSI	Single port Ultra 3 SCSI	
Burst transfer rates	LVD 160 MB/sec	
Fibre Channel	Single port[4], Dual port[5], shortwave, multi-mode optical Fibre Channel port, LC duplex connector	
Channel data rate	200 MB/sec (maximum instantaneous)	
Interface specifications	N & NL Port, FC-PLDA (Hard and soft AL-PA capability), FC-AL-2 FCP-2, FC-TAPE	
Read/write compatibility interface	Proprietary format	
Physical data		
Form factor	5.25 in (full height)	5.25 in (full height)
Environmental data		
Form factor	5.25 in (full height)	5.25 in (full height)
Environmental data		
Temperature		
Operating	+50° F to +104° F (+10° to +40° C)	+50° F to +100° F (+10° to +38° C)
Non-operating	-40° F to +150° F (-40° C to +66° C)	-40° F to +139° F (-40° C to +60° C)
Humidity		
Operating	20% to 80%	20% to 80%
Non-operating	10% to 95%	10% to 95%
Power source		
Power Input		
L700/L180	100-240 VAC @ 50-60 Hz	100-240 VAC @ 50-60 Hz
L5500	220-240 VAC @ 50-60 hz single phase	220-240 VAC @ 50-60 hz single phase
Power consumption/dissipation (operating maximum continuous - not peak)	30 VA/99 BTU/hr	32VA/109 BTU/hr

[1] Continuously variable to 10 MB/sec to match slower channels using HP Adaptive Tape Speed system (ATS)

[2] Auto adjustable to 17.5 MB/sec to match slower channels.

[3] The actions of the tape drive can be divided into four distinct phases.

Phase 1 Load time – the amount of time required to insert a cartridge in the drive, load the tape and prepare to read, write or search.

Phase 2: Average file access time – the amount of time required to search from the beginning of the tape to the mid point, does not include load time

Phase 3 Maximum rewind time – the amount of time required to rewind the tape from the end to the beginning of the tape
The average rewind time is the time to rewind a tape from the mid-point to the beginning, i.e one-half of the maximum rewind time

Phase 4 Unload time – the amount of time required to eject the cartridge from the drive

[4] Specifications are for the IBM StorageSmart T400F tape drive

[5] Specifications are for the HP 460 Fibre Channel tape drive.

About StorageTek

StorageTek (NYSE:STK), a $2 billion worldwide company with headquarters in Louisville, Colo., delivers a broad range of storage solutions that are easy to manage, integrate well with existing infrastructures and allow universal access to data across servers, media types and networks. StorageTek provides practical and safe storage solutions in disk, networking, services, tape and tape automation. For more information, see **www.storagetek.com**, or call **1.800.786.7835**.

World Headquarters
Storage Technology Corporation
One StorageTek Drive
Louisville, Colorado 80028 USA
Phone: 1 800 786 7835
Fax: 719 536 4053

International Offices
Australia: 61.2.9438.4844
Austria: 0800.20.16.31
Belgium: 0800.75.327
Brazil: 55.11.3044.4599
Canada: 905.602.5566
Chile: 56.2.201.0490
China: 86.10.8251.1911
Denmark: 44836111
Finland: 08001.13361
France: 0800.82.83.57
Germany: 0800.181.8238
Hong Kong: 852.8200.0791
India: 91.80.226.7272
Ireland: 1800.55.33.54
Italy: 167.790.852
Japan: 81.3.3746.9711
Korea: 82.2.191.1100
Malaysia: 603.772.41125
Mexico: 52.55.9177.1800
The Netherlands: 0800.022.8486
Norway: 800.11.220
Poland: 48.22.5757.157
Singapore: 65.6774.9248
South Africa: 0800.99.5820
Spain: 900.99.33.86
Sweden: 020.798711
Switzerland: 0800.83.87.85
Taiwan: 886.2.6800.9840
United Arab Emirates: 971.4.3900162
United Kingdom: 0800.731.8852

MT 9197 D 5/03

STORAGETEK

SunPlex™ Systems and Sun™ Cluster 3.0 Software

The premier application service delivery platform.

Key feature highlights

Integration of the SunPlex system and the Solaris Operating Environment: Core Solaris services, such as devices, file systems, and networks, can operate seamlessly across a tightly coupled SunPlex system, plus maintain full Solaris compatibility with existing applications.

Continuous Availability of the Core Services: IT professionals can deliver higher service levels, reduce IT risks, and lower service costs.

Service Level Management: Scaling can occur within a system or across multiple systems, enabling administrators to increase availability, capacity, and performance while continuing to maintain service levels.

Centralized SunPlex System Management: Resources, servers, and storage can be managed as a single entity within a cluster-wide environment.

Ease of Use: Complex tasks can be performed with ease; system administrators can manage any resource on a SunPlex system from anywhere on the network. An easy-to-use API and SunPlex Agent Builder tool help administrators cluster-enable applications.

Disaster Recovery: Using Campus Clusters, Sun Cluster 3.0 nodes can be separated by up to 10 Km to allow for continuity of services in the event a catastrophic failure brings down an entire campus.

Today's explosive levels of growth — in terms of bandwidth, networks, and digital devices — are driving an even greater shift towards a services model of computing. The Services on Demand approach moves the burden of a computing infrastructure from end users and their PCs to the organizations that provide the services. Since its inception in 1982, Sun has been driven by a singular vision — The Network Is The Computer™ — and has helped businesses harness the transforming power of the network in order to create, deploy, and deliver reliable Services on Demand.

As the foundation for the Sun™ Open Net Environment (Sun ONE) — Sun's vision, architecture, platform, and expertise for delivering Services on Demand — the Solaris™ 9 Operating Environment provides an integrated yet open architecture for building and deploying Services on Demand. The Solaris 9 Operating Environment (OE) offers new levels of performance in scalability, availability, manageability, and security, and delivers a complete and highly refined environment designed to enable customers to increase service levels while decreasing costs and reducing IT risks.

Sun Cluster 3.0 and the Solaris Operating Environment

Sun Cluster 3.0 software takes general-purpose clustering beyond the realm of high availability by adding the simplicity of single system manageability and the potential of seamless scalability. It provides a single, globally coherent process and resource management view for the multiple nodes of a cluster. In essence, the cluster becomes a single managed entity, and presents itself and its services to clients as if it were an individual server.

The Sun Cluster 3.0 framework extends the Solaris Operating Environment, enabling core Solaris services — devices, file systems, and networks — to operate seamlessly across a SunPlex™ system while maintaining full Solaris compatibility with existing applications.

Sun Cluster 3.0 provides high availability (HA) and scalability to everyday Solaris applications through continuous network and data availability. Services that are written to the easy-to-use Sun Cluster 3.0 API can achieve even higher levels of availability as well as scalability.

The SunPlex system is a key element of a services-driven computing environment. SunPlex systems deliver management capabilities in tightly coupled pools of resources, making it possible to *manage the service, not the server.* Sun Cluster 3.0 software is the key to building SunPlex systems, which also include the Solaris Operating Environment; Sun server, storage, and network connectivity products; and Sun support services.

The SunPlex system is the premier integrated application service delivery platform. Combined with Sun Cluster 3.0 software, SunPlex systems are designed to manage application services for tightly coupled environments, optimizing both the availability and scalability of these services.

SunPlex System Key Benefits

The SunPlex system offers a unique approach to application service management, and is the premier, integrated application service delivery platform. SunPlex systems enable an enterprise to respond to the scalability, availability, and complexity challenges that arise in today's services-driven model of computing. With the help of SunPlex systems, enterprises can increase service levels while decreasing service level cost and risk.

Makes Service Levels Easier to Manage

SunPlex systems provide a powerful, flexible environment where failover and scalable application services can be simultaneously deployed and easily managed. Application services running on SunPlex systems receive the full benefits of the Sun Cluster 3.0 HA framework. You can deploy them across the SunPlex system without worrying about how they will find and access network and file services.

Provides Continuous Access

SunPlex systems deliver Global Network and File Services. Data, network, and devices are continuously available to all domains in the SunPlex system as well as to applications running on any domain.

Simplifies Administration, Lowers Costs

SunPlex systems incorporate system management tools, such as Sun Management Center and SunPlex Manager software, to create a centrally managed environment that provides easy administration and lower operating costs.

Summary of Features

Global Network Services

In the Sun Cluster 3.0 architecture, incoming requests from the network go to a global IP address, which is always available and shared by all domains in the SunPlex system. To clients on the network, the entire SunPlex system looks like a single computing resource.

Through load balancing of the incoming requests, Global Network Services help increase the performance of the scalable application services running on SunPlex systems. Application services can run on any domain in the SunPlex system, independent of the exact path taken by network requests and responses. Centralization of Global Network Services on behalf of the SunPlex system facilitates a simple "single point of management" paradigm.

Global Devices and Global File Services

Data access is significantly enhanced in Sun Cluster 3.0 with the addition of Global Devices and Global File Services. With Global Devices, every domain has access to any device on the SunPlex system — such as a disk or CD-ROM drive — even if that device is not physically connected to that domain.

Global File Services extend these capabilities by using shared storage devices — storage with physical connections to more than one domain — so that data is both highly available and accessible to application services running on any domain of the SunPlex system. Centralization of Global File Services on behalf of the SunPlex system facilitates a simple "single point of management" paradigm. Customers who prefer to failover the file system can use the Failover File Service feature of the Sun Cluster 3.0 5/02 release instead of the Global File Services.

Scalable Services

The Sun Cluster 3.0 framework allows a single application, or series of applications from a service, to run across multiple domains or systems. By adding more domains or systems to the SunPlex system, capacity and continuity are increased. Service levels are maintained in the event of any number of potential outages — planned or unplanned.

Failover Services

The Sun Cluster 3.0 architecture delivers inherent HA services. It enables IT organizations to maintain service levels on critical applications and services. Failover Services provide high availability to single instance applications by failing over the application to a backup node in the event of a failure.

Faster Failover

Sun Cluster 3.0 software provides fast error detection, fast software switch-over, and parallelized application and infrastructure restarts.

When a failover occurs, clients might see a brief interruption in service and may need to reconnect (depending on the characteristics of the application) after the failover has finished. However, once reconnected, the physical server from which they get applications and data is transparent.

Diskless Failover
With the foundation of these key abstracted capabilities — Global Network Services, Global Devices, and Global File Services — there is no concept of logical host in Sun Cluster 3.0. Services need not reside on servers physically attached to storage devices, which means service failover does not require storage device or file system failover. Diskless Failover enhances flexibility as well as minimizes failover time.

Centralized System Administration and Management Tools
The Sun Cluster 3.0 framework simplifies administration by enabling SunPlex system resources to be managed and administered as if they were on a single system. Administrators have access to all system management tools from any system in the SunPlex system. And because of the integration with the Solaris Operating Environment, familiar Solaris commands execute just as if only a single system were being administered.

SunPlex system management is accomplished through either a command-line interface (CLI) or GUI-based management tools (Sun Management Center or SunPlex Manager). The GUI-based tools allow complex tasks to be performed with ease by enabling system administrators to manage any resource on a SunPlex system from anywhere on the network. This provides tremendous cost savings for organizations where administrators are responsible for systems located in different buildings, cities, and even countries.

Easy Agent Development Environment
Sun provides a list of qualified Scalable and HA Agents. Alternatively, developers can use the SunPlex Agent Builder to develop Scalable or HA Agents. The SunPlex Agent Builder generates agent code in Ksh or C with two simple clicks. For fast agent deployment with no code writing or modification, developers can also use the Generic Agent functionality of the Agent Builder. The Generic Agent functionality generates a precompiled agent binary that shortens the agent deployment cycle. In the Sun Cluster 3.0 5/02 release, the Generic Agent functionality has been enhanced to offer tunable parameters that allow for customization of the Generic Agent.

Fast Application Messaging Via Remote Shared Memory Technology
Sun Cluster 3.0 software includes Remote Shared Memory (RSM) technology, which offers improved service levels for distributed applications running in the Sun Cluster environment. The RSM API offered in the Solaris 8 Operating Environment 10/01 release enables application developers to bypass the TCP/IP stack and access high-speed, high-bandwidth, and low-latency interconnect hardware directly for fast messaging in the Sun Cluster environment. RSM technology in the Sun Cluster 3.0 5/02 release has been tuned for optimal performance of Oracle9i RAC.

Dynamic Reconfiguration (DR) Support
Sun Cluster 3.0 software provides support for dynamic additions or removals of hardware resources such as processors, memory, and I/O devices. DR support checks the safety of a DR operation and rejects any unsafe operations.

Security Hardened
Security Hardening is supported on all of the Sun Cluster 3.0 supported agents with the exception of the BroadVision agent. The DB2 agent from IBM is also security hardened.

Prioritized Service Management (PSM)
PSM is a policy-based service level management feature that provides high service levels for a high-priority service in the event of its failover to a backup node. It automatically offloads low-priority services on the backup node to free resources for the high-priority service. The low-priority services can either be shut down or failed over to another node.

Campus Cluster Support
Both two-room (quorum device in the same room as the primary node) and three-room (quorum device in its own room) Campus Clusters are supported by SunPlex systems.

Easy Upgrades
Upgrading from the Sun Cluster 3.0 12/01 release to the Sun Cluster 3.0 5/02 release can be done with minimal downtime. Nodes can be upgraded one at a time without shutting down the entire cluster. This minimizes planned service downtime during the Sun Cluster 3.0 software upgrade.

Eight-Node Support
Sun Cluster 3.0 supports up to eight nodes in a SunPlex system. Customers can mix and match from Sun's extensive server offerings.

About Sun ONE
The Sun Open Net Environment (Sun ONE) is Sun's vision, architecture, platform, and expertise for delivering Services on Demand today and in the future. Based on open standards such as Java™ and XML technology, Sun ONE provides a highly scalable and robust framework for building and deploying a variety of Services on Demand — from traditional Web-based applications to future context-aware Web services. By simplifying the way Web services are created, assembled, and deployed, the Sun ONE platform can enhance productivity, speed time to market, and increase business opportunities for enterprises worldwide.

SunPlex™ Systems and Sun™ Cluster 3.0 Software

SunPlex System Configurations

A SunPlex system comprises two or more SunPlex system-qualified servers (up to eight nodes are supported), storage products, SunPlex system interconnects, and public networks running Solaris 9 software.

Supported Server Platforms

The following server platforms are supported. Additional platforms will be available in the future.

- Netra™ t 1120/1125, t 1400/1405, T1 AC200/DC200, and 20 servers
- Sun Enterprise™ 220R, 250, 280R, 420R, 450, 3500, 4500, 5500, 6500, and 10000 servers
- Sun Fire™ V880, 3800, 4800/4810, 6800, 12K, and 15K servers

Supported Storage Products

The following storage products are supported. Additional storage products will be available in the future.

- Sun StorEdge™ MultiPack, D1000, A3500 (SCSI/FC), A5000, A5100, A5200, T3, SE 3910/3960, 9910/9960, and S1 arrays
- Netra st D130 and st D1000 servers

Supported Third-Party Storage

- EMC Symmetrix[1]

Supported SAN Switches

- Sun StorEdge Network FC Switch-8 and Switch-16
- Brocade Silkworm 2400 and 2800

Supported Interconnects[2]

The following SunPlex system interconnects are supported. Additional SunPlex system interconnects will be available in the future.

- On-board 100 Mbits/sec port, Sun Quad FastEthernet™, SunFastEthernet™, and SunSwift™ adapters
- Sun Gigabit Ethernet adapter
- PCI-Scalable Coherent Interface (SCI)

Supported Public Networks

The following public networks are supported. Additional public networks will be available in the future.

- On-board 100 Mbits/sec port, Sun Quad FastEthernet, SunFastEthernet, and SunSwift adapters
- Sun Gigabit Ethernet adapter

Supported SunPlex Topologies

- Clustered Pairs
- N+1
- Pair+M

Supported Volume Managers

- Solaris Volume Manager software
- VERITAS Volume Manager (VxVM)

Supported SunPlex Agents

The following agents are available now:

- HA DNS
- HA NFS
- HA Oracle
- Oracle Parallel Server (OPS)
- Oracle9i RAC
- HA Sybase
- Scalable SAP
- HA Sun ONE Web Server[3]
- HA Sun ONE Messaging Server[3]
- HA Sun ONE Directory Server[3]
- HA Sun ONE Calendar Server[3]
- HA Netscape™ Directory Server (LDAP)
- HA Apache Web/Proxy Server
- HA NetBackup
- HA Solstice Backup™ software
- Scalable Sun ONE Web Server
- Scalable Apache Web/Proxy Server
- Scalable BroadVision One-To-One

Agents Available Through Third Parties

- IBM DB2 (EE and EEE)
- HA Informix Dynamic Server
- Sybase ASE

Sun Cluster Software Coexistence

- Solaris Resource Manager
- Sun StorEdge Instant Image
- Sun StorEdge Network Data Replicator

For More Information

To learn more about Sun Cluster 3.0 software and SunPlex systems, visit sun.com/clusters.

For more information on the Solaris 9 Operating Environment, visit sun.com/solaris.

For additional information on Sun ONE, visit sun.com/sunone.

1. Please contact your Sun Sales Representative for more information.
2. Up to six links of interconnects transferring data in parallel are supported in one SunPlex system.
3. Formerly iPlanet™ Web Server, iPlanet Messaging Server, iPlanet Directory Server, and iPlanet Calendar Server.

Sun Microsystems, Inc. 901 San Antonio Road, Palo Alto, CA 94303-4900 USA **Phone** 800 786-7638 or +1 512 434-1577 **Web** sun.com

1348

654

General Information

1

This chapter describes the hardware components of the library, the cell locations for cartridge tapes, and the two library operating modes (automatic and manual). For software information and drive information, refer to the publications that pertain to these specific topics.

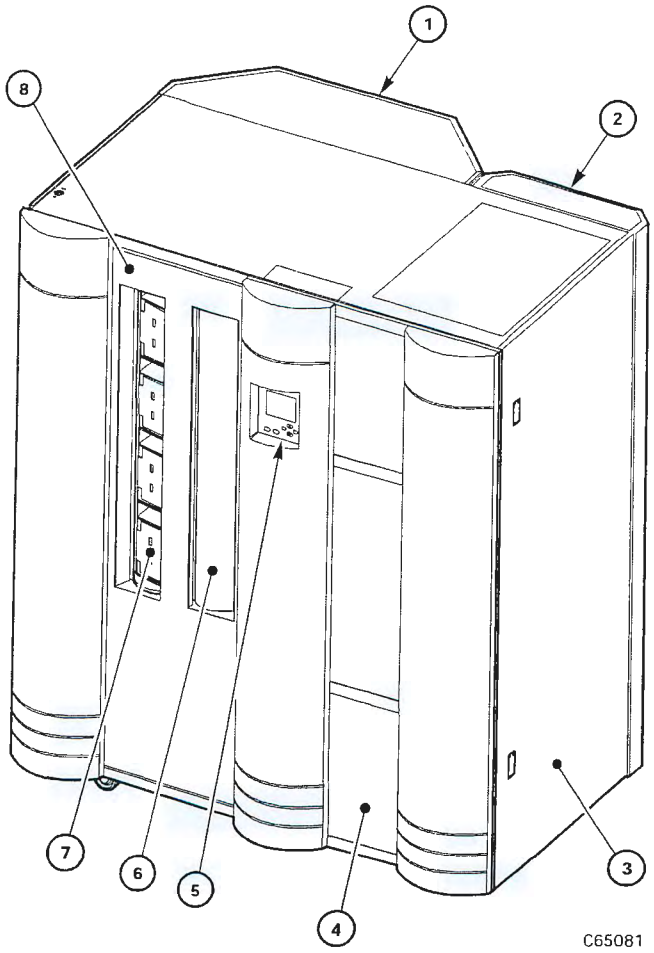
The library is a robotic system that mounts cartridges into a storage cell or into a drive for read/write operations. It also moves cartridges from the cartridge access port (CAP) to storage cell or from cell to cell. Figure 1-1 on page 1-2 through Figure 1-4 on page 1-8 show the major components of the library, described in the following pages.

Tape Library Components

The tape library has four major components:

- A robot, which mounts and dismounts cartridges
- Storage cells for 156 to 678 cartridges
- A CAP that holds up to 20 cartridges in four magazines, with an optional second CAP that holds the same number of cartridges
- Drives, which perform read/write operations

Figure 1-1. Library Major External Components (C65081)



1. Expansion frame
2. Rear door
3. Drive access door
4. Right door
5. Operator panel
6. Optional CAP B (shown closed)
7. Standard CAP A (shown open)
8. Left access door

Robot

The robot moves cartridges between storage cells, between cells and tape drives, and between the CAP and cells. The robot consists of the Z column assembly (vertical motion), the theta mechanism (lateral motion), and the hand-camera assembly. Figure 1-2 on page 1-4 shows these robot components.

The Z column assembly contains a Z column and Z carriage. The Z column attaches to the floor and ceiling of the tape library. The Z column can rotate almost 360 degrees to enable access to all the cells in the tape library.

The hand-camera assembly, which is attached to the Z carriage, grasps and releases cartridges. The Z carriage moves the hand up and down the Z column to storage cells, drives, or the CAP.

The camera, which is on the hand, is active only during a library audit. An audit occurs when you:

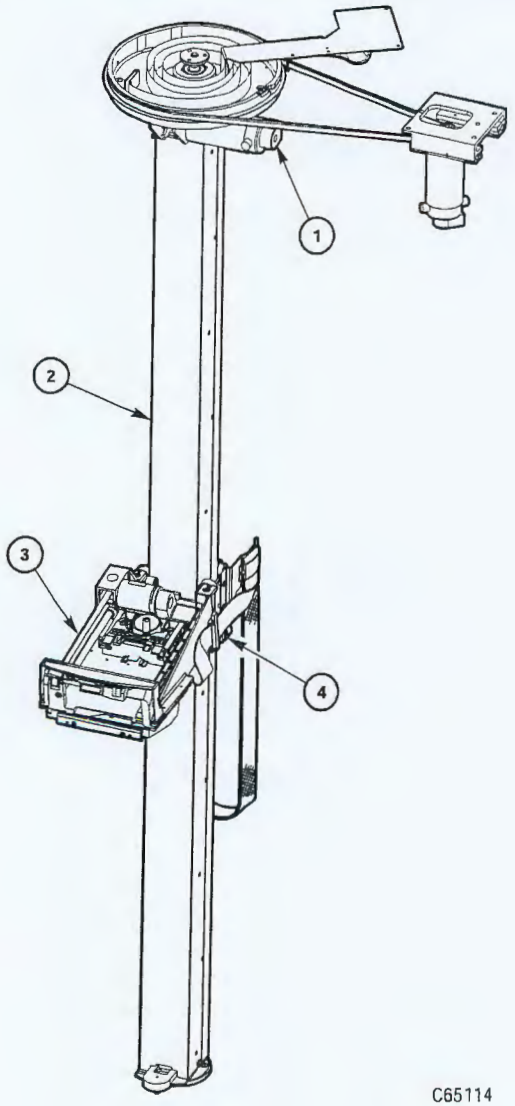
- Power-on the tape library.
- Open and close the left access library door.
- Make a request at the customer server console to audit the tape library.

During an audit, the camera reads the location and volume serial number (VOLSER) of each cartridge in the storage cells and reserved cells. Since this information is stored in the library's memory, the library does not rely on the camera to read cartridge cartridge locations or VOLSERs during mount and dismount operations.

The storage of audit data within the library has two implications for operation:

- Each time an audit occurs, you must use the system console to request a host update. This procedure adds the library audit information to the host memory.
- If you manually exchange a cartridge from a drive for one in storage, the host memory will continue to apply the VOLSER and location information from the first cartridge to the second cartridge. This might cause an error.

Figure 1-2. Robot Components (C65114)



1. Z motor
2. Z column
3. Hand-camera assembly
4. Z carriage

Storage Cells

Host software locates cartridges by panel, column, row, and cell. The library contains storage cells for 156 to 678 cartridges, excluding the CAP cells. The number of cells is determined by how many drives are installed and whether the tape library has the standard rear window panel or the expansion frame. The expansion frame provides additional storage cells for 294 cartridges.

Cell Locations

Cartridges are stored in cell arrays that hold six cartridges. Cell arrays are stacked in columns and these columns are arranged in a circle around the robot assembly. Columns can hold up to 42 cartridges.

Table 1-1 on page 1-6 lists tape library storage capacities. Figure 1-3 on page 1-7 through Figure 1-4 on page 1-8 show cell locations for the L700e tape library in its various configurations.

Note: The following statements apply to cell locations:

1. The library uses array targets for robotic calibration during an Initial Program Load (IPL).
2. Never put data cartridges in the reserved cells (refer to "Reserved Cells" on page 1-9 for more information). If you do not want to store diagnostic and/or cleaning tapes in these cells, you must leave them empty.
3. The library does *not* use the drive and CAP locations to store cartridges.
4. The robot uses the swap cell (the top-most cell in the reserved area) for in-transit cartridges, to place a cartridge that is left in the hand-camera assembly when a power failure occurs, or to perform a swap operation.

Library Capacity

Table 1-1 on page 1-6 lists the library storage capacities. Although library capacity is automatically configured when you bring the library online, check the operator panel to be sure that the capacity information is accurate.

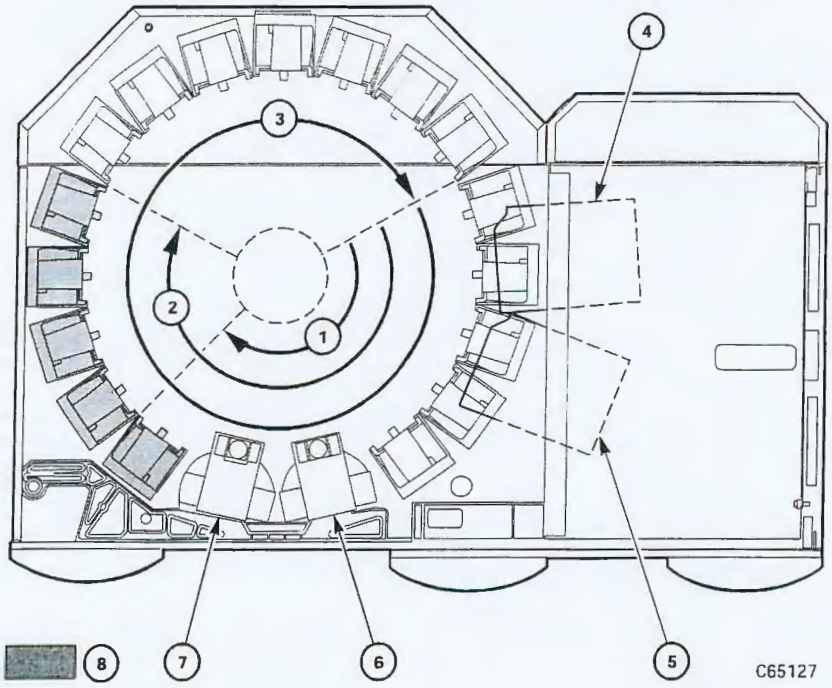
Table 1-1. Tape Library Capacity

Expansion Frame	Second Drive Column	Drives Installed (Maximum)	Panel 2 Access	Total Data Cartridge Cells[1]	Reserved Cells[2]
Yes (Full)	No	10 DLT/Ultrium or 6 9840/T9840B/ T9940 + 1 DLT or 1 Ultrium	Entire	678	12
	Yes	20 DLT/Ultrium or 12 9840/ T9840B/9940 + 2 DLT, or 2 Ultrium	Entire	618	12
No (2/3)	No	10 DLT/Ultrium or 6 9840/T9840B/ T9940 + 1 DLT or 1 Ultrium	Entire	384	12
	Yes	20 DLT/Ultrium or 12 9840/ T9840B/T9940 + 2 DLT or 2 Ultrium	Entire	324	12
No (1/3)	No	10 DLT/Ultrium or 6 9840/T9840B/ T9940 + 1 DLT or 1 Ultrium	Partial	216	12
	Yes	20 DLT/Ultrium or 12 9840/ T9840B/T9940 + 2 DLT or 2 Ultrium	Partial	156	12

Notes: 1. These numbers do not include cells in the CAP or the reserved area.

2. The reserved cells are composed of one swap cell and 11 cleaning and/or diagnostic cartridge slots. They are shown in Figure 1-5 on page 1-10.

Figure 1-3. Locating Cartridges—Top View (C65127)



1. 1/3 capacity (partial access to Panel 2)
2. 2/3 capacity (entire access to Panel 2)
3. Full capacity (with optional expansion frame)
4. Drive column 0
5. Drive column 1 (optional)
6. CAP B (optional)
7. CAP A
8. Panel 2

Figure 1-4. Locating Cartridges—Panels, Cells, Rows (C65091)

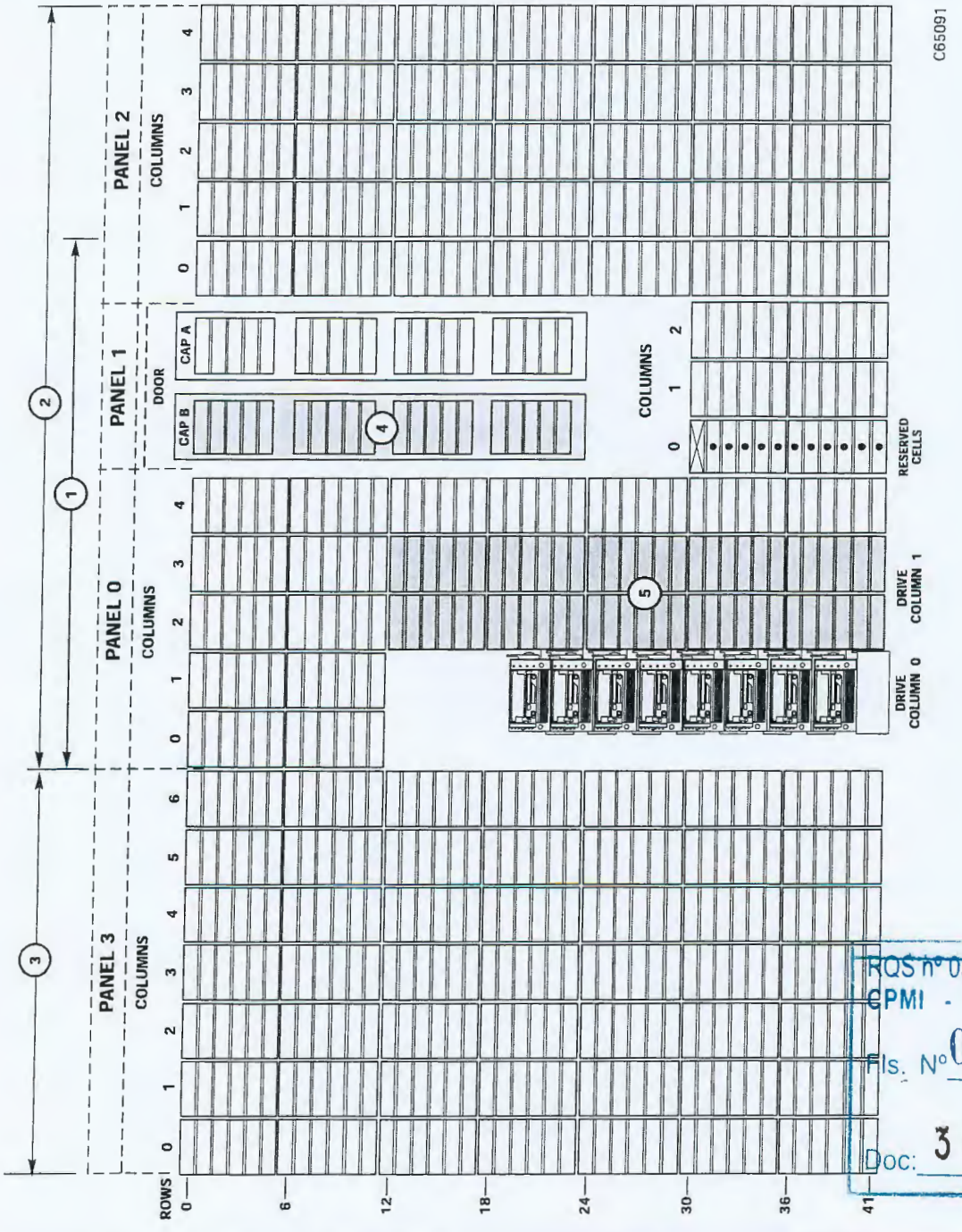


Figure 1-4. Locating Cartridges—Panels, Cells, Rows (Continued) (C65091)

1. 216-cartridge-cell configuration
2. 384-cartridge-cell configuration
3. Expansion frame (See note)

Note: 678-cartridge-cell configuration equals 384-cartridge-cell configuration plus Expansion frame.

4. Optional second CAP (See note)
5. Optional second drive column

Note: The optional second CAP replaces the front window. The optional second drive column replaces the 60 shaded cells.

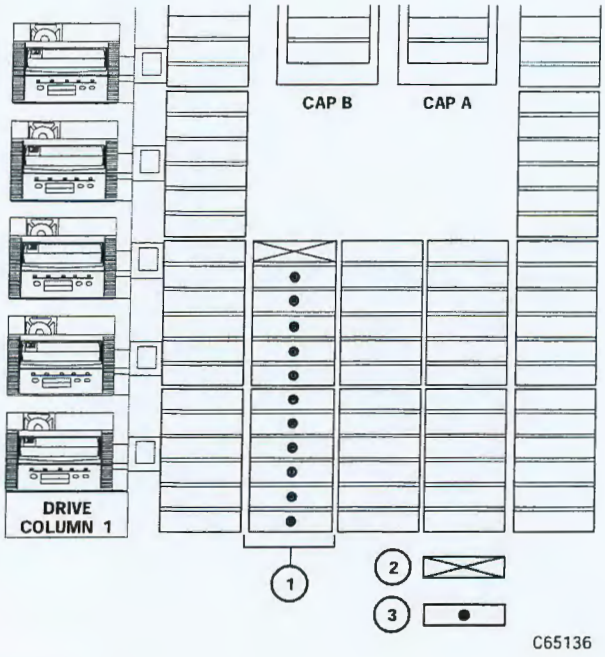
Reserved Cells

Figure 1-5 on page 1-10 shows the cells reserved for swapping cartridges and for diagnostic and cleaning cartridges. The top cell is the swap cell, which is reserved for in-transit cartridges. Do *not* place any cartridges into this cell. You may place any type of cleaning or diagnostic cartridges into the other 11 cells.

Note: Loading cleaning cartridges into any of these 11 cells enables Auto Clean upon the next IPL.

CAUTION:
***System degradation:* Do not insert data cartridges into these reserved cells. The host software will not find these cartridges.**

Figure 1-5. Reserved Cell Locations (C65136)



1. Location of reserved cells
2. Swap cell (leave empty)
3. Diagnostic and cleaning cartridges

Cartridge Access Port

A cartridge access port (CAP) is the location where you add cartridges to or remove cartridges from a library without interrupting normal cartridge mounts and dismounts by the robot. The library may have an optional, second CAP. Both CAPs are located on the right front door.

The CAP magazine is designed for easy loading. You can access the magazine by simply pulling down on the magazine handle and adding cartridges. Or, you can remove the magazine by lifting it out, load the cells, and place the magazine back into the CAP. Snap-on cartridge retention covers allow you to keep cartridges in place when transporting magazines.

For detailed procedures, refer to"Importing Data Cartridges through the CAP" and "" in Chapter 4, "Library Operation."

Drives

The library can contain the following drive types:

- Digital Linear Tape (DLT) 8000 or DLT 7000E
- 9840/T9840B[1]/T9940
- IBM Ultrium
- Hewlett Packard Ultrium
- Seagate Ultrium

CAUTION:
***Possible data loss:* StorageTek does not advise mixing DLT 7000 and DLT 8000 drives in the same library. If a DLT 7000 cartridge is inserted into a DLT 8000 drive, the tape can be read and written in 7000 mode.**

If a DLT 8000 cartridge is inserted into a DLT 7000 drive, the drive will indicate "Medium Error/Calibration Error (03/8000)" if a read command is issued and, as with most tape drives, will write over any data present on the tape if a write command is issued at load point.

The maximum number of DLT or Ultrium drives is 20. The maximum number of 9840/T9840B/T9940 drives is 12.

As an operator, you might have to:

- Configure a drive in a library; refer to "Drive Entries (SCSI Drives Only)" on page 3-10.
- Check drive status information; refer to "Drive Status" on page 4-3.
- Manually mount a cartridge to a drive or dismount a cartridge from a drive; refer to "Loading/Unloading Cartridges Manually" on page 4-28.

Note: During typical operation (or automated mode), the library's robotic hand-camera assembly automatically places a cartridge into the drive or removes a cartridge from the drive when a command is sent from the host software.

For specific drive information, refer to your drive publications.

1. 9840 drive operator panel buttons are yellow ; T9840B drive buttons are purple.

Horizon L Series Library Monitor Feature

The optional Horizon L Series Library Monitor feature incorporates a web interface to the library. In addition to the feature, you will need a personal computer attached to the library's Ethernet port. The feature enables you to:

- "View" the library interior and visually check the status of tapes, drives, and CAP
- Initiate diagnostic tests on the library from the personal computer
- Make configuration changes or additions

Consult the compact disk which accompanies this feature for more information.

Tape Library Safety Features

Safety features are incorporated into the tape library. If the left access door is opened, an electrical interlock removes power from the robot assembly.

Behind the right front door, covers are placed over the logic card, the AC power supply, and the DC power supply to prevent you from coming into contact with hazardous voltages and sensitive electronics.

Controlling Software

Controlling software, within the client/server, requests tape read and write operations to the drives and robotic move operations for the tape library robotic components. Software determines where the cartridge is located by tracking the VOLSER and cell location during audits, then allocates which drive receives the cartridge. For specific information, refer to your software publications.

When the control path is a direct attachment, the software resides within the client central processing unit (CPU). When the control path is an indirect attachment, the software is divided between the server and the client CPUs. For specific information, refer to your software publications.

Library Operating Modes

An operating mode is the manner in which a tape library and the controlling software (also referred to as the customer's server software) interact. A library can operate in either automated mode or manual mode.

Automated Mode

Automated mode is the normal operating mode of the tape library. The controlling software instructs the robot to move the cartridge among the storage cells, drives, and CAP without operator intervention. Your tasks may include:

- Monitoring the tape library operator display for messages
- Importing a cartridge through the CAP
- Exporting a cartridge through the CAP
- Replacing a cleaning cartridge

Refer to Chapter 4, "Library Operation," for the procedures.

Manual Mode

Manual mode occurs when the tape library is offline. Your tasks may include:

- Opening the tape library doors
- Moving the robot
- Locating a cartridge
- Removing a cartridge from the hand
- Mounting a cartridge into a drive
- Dismounting a cartridge from a drive
- Returning the tape library to online status

Refer to Chapter 4, "Library Operation," for the procedures.

Auto Clean Feature

Drives occasionally need to be cleaned to prevent read/write errors.

The Auto Clean feature is enabled when your tape library is initializing and detects cleaning cartridges in the reserved cells. When a drive requires cleaning while Auto Clean is enabled, the robot will receive a software message telling it to retrieve a cleaning cartridge and place it into the drive.

If Auto Clean is not enabled, you must manually import a cleaning cartridge for the drive that requires cleaning. The "Clean Drive" request appears on the operator panel's display.

Refer to "Cleaning Cartridge Warning Count" in Chapter 3, "Configuration," for more information and procedures.

13U Rack Area

You may use the internal 13U (0.57 m [22.75 in.] x 0.48 m [19 in.]) rack area, located behind the right front door, for additional equipment. Refer to "Rack Safety and Precautions" on page xxiii for precautions you must follow before installing equipment in this area.

Power cable space is provided in the cutout area of the rear door.

CAUTION:
Heat within rack area: **Cooling considerations should be made based upon the power dissipation within the rack space, as well as the external library room ambient conditions. Cooling must be provided for moderate power dissipation within the rack space. Additional cooling is available from StorageTek.**

Table 2-1. Operations Guide (Continued)

Task	Page for Operator Panel Instructions
• Set library Fibre Channel Port 0 address	page 3-5
• Enable/disable Fast Load	page 3-7
• Set date and time	page 3-8
• Set drive configuration	page 3-10
• Set network configuration	page 3-12
• Set screen characteristics	page 3-15

Library Power Switch

The library power switch is a circuit breaker or breakers behind the right front door of the library. Figure 2-18 on page 2-19 shows the power switch location. This switch, attached to the AC power distribution unit (PDU), controls the AC power to the library and drive column.

The power switch has two configurations:

- A single breaker on the AC power distribution unit controls the library and a single drive column.
- An optional second breaker, located on the second power distribution unit, powers the second drive column and an optional second library power supply.

Notes: If your library has two circuit breakers:

1. The optional PDU must be connected to a separate electrical circuit.
2. If only one breaker is powered off, the second breaker will still be powered on.

To apply power to the library and drive column, lift the switch or switches.

To remove power from the library and drive column:

- Make sure all jobs are complete.
- Push down on the library power switch or switches.

SUN STOREDGE ENTERPRISE BACKUP SOFTWARE
Detailed View

Sun StorEdge Enterprise Backup Software

» Features, Functions & Benefits
□ Detailed View

Storage Related:

» White Papers
» Success Stories
» Press Releases

See Also:

» Remote Management
» Professional Services
» Sun Servers
» PatchPro

Price & Buy Contact Me

Introduction

Sun StorEdge[tm] Enterprise Backup software 7.0 (EBS 7.0), formerly Solstice Backup software, reduces management overhead by providing "lights out" protection of storage assets throughout the enterprise, from the largest corporate data centers to the smallest branch offices. Built upon an open, highly scalable client-server architecture, it is an integrated product that addresses the backup, recovery, and archival needs of heterogeneous computing environments in large enterprises or departmental workgroups. It supports SolarisTM Operating Environment servers, as well as LAN-, WAN-, NAS and SAN-attached, multi-vendor UNIX®, Linux, Microsoft Windows, and NetWare platforms.

Sun StorEdge Enterprise Backup software is a key component of Sun's Data Continuance offering, which also includes Sun StorEdge Availability Suite software for point in time copy and real time data replication, and Sun Cluster for Solaris OE application availability with Sun StorEdge tape and disk arrays.

The software is deployed worldwide at Sun Microsystems to protect over 125 terabytes of data across 500 backup servers including six terabyte-class data centers. Support is provided for Sun's tape drives, tape libraries and the latest Sun storage.

Advanced Sun StorEdge Enterprise Backup software capabilities such as indexing and media management, cluster support, high speed parallelism, tape interoperability, comprehensive NDMP support, disk backup, tape cloning, archive, and dynamic drive sharing are among key components that enable administrators to protect storage assets and minimize downtime.

Database, messaging and ERP modules deliver online protection and granular recovery. Storage nodes enable load sharing and distribution of backup traffic, as well as LAN-free protection of servers with large data volumes. Autochanger/Silo modules enable hands-free protection using a wide variety of robotic devices. Sun StorEdge Enterprise Backup software is also tightly integrated with complimentary Legato applications such as hierarchical storage management (HSM), systems management frameworks, simplified operator administration, and web-enabled management of multiple Sun StorEdge EBS servers.

With Sun StorEdge Enterprise Backup software, you can standardize on one application to provide complete, fast, and reliable protection of business-critical information across a heterogeneous enterprise, resulting in lower downtime costs, less management overhead, and greater ROI of storage resources.

Sun StorEdge Enterprise Backup software 7.0 is available in four editions to match the IT requirements of each customer. Additionally, various options are available for extending coverage, capability, and throughput. Options can be purchased at any time after installation and can be easily added to a site without interrupting ongoing operations. This allows you to scale your data protection solution as storage needs increase.

Sun StorEdge Enterprise Backup software takes capabilities such as heterogeneous platform support, disk backup, automated media handling, consistent interoperable tape format, data stream parallelism, remote management, and client-server frameworks for storage management to a new level, making it one of the most flexible and scalable storage management solutions available. The software is an ideal complement to every Sun server and Sun StorEdge tape library and disk array purchase.

Back to Top

Features, Functions & Benefits

- HETEROGENEOUS SUPPORT
- ADVANCED ARCHITECTURE
- ENHANCED BACKUP PERFORMANCE
- EXPANDABLE NETWORK CONNECTIVITY
- HIGH PERFORMANCE
- AUTOMATED MEDIA MANAGEMENT
- ENHANCED NETWORK AND APPLICATION SERVICE LEVELS
- DATA PROTECTION AND RECOVERY
- HIGH-AVAILABILITY CLUSTER SUPPORT
- ENTERPRISE-CLASS NAS PROTECTION

HETEROGENEOUS SUPPORT

Feature: Centralized, automated protection for heterogeneous enterprises.

Function: Support for a wide range of backup platforms, clients, storage systems, file systems, and volume managers.

Benefit: Allows you to protect terabytes of information for hundreds to thousands of networked servers and workstations. You can standardize on one application to protect your largest data centers as well as your smallest branch offices, while minimizing downtime costs, reducing management overhead, and increasing return on your storage resource investments.

ADVANCED ARCHITECTURE

Feature: Robust, scalable client-server architecture.

Function: Provides advanced indexing architecture; single meta-data index; and tape interoperability between Unix, Windows, and Linux backup platforms.

Benefit: Increases disaster recovery and platform migration capabilities, eliminates risk of corruption, and speeds file recovery. This simplifies management, increases resiliency, allows you to recover data without administrative assistance.

ENHANCED BACKUP PERFORMANCE

Feature: Disk-to-disk backup option.

Function: Performs simultaneous reads-from and writes-to disk, as well as concurrent staging/cloning operations and backups. It also automatically senses and removes incomplete backups from disk and purges expired data.

Benefit: Backs up unlimited clients directly to disk, increasing backup performance. This also allows you to recover individual files directly from online disk to reduce downtime.

EXPANDABLE NETWORK CONNECTIVITY

Feature: Full LAN, SAN, and WAN connectivity.

Function: Easy, dynamic expansion of client connections, storage nodes, and storage devices.

Benefit: Provides flexible, scalable backup and recovery capabilities and expandable support of your heterogeneous storage infrastructure.

HIGH PERFORMANCE

Feature: Superior performance for fast backup and recovery.

Function: Built-in data multiplexing and data compression.

Benefit: Provides extensive support for high-speed tape drives, libraries, and silos.

AUTOMATED MEDIA MANAGEMENT

Feature: Advanced media management.

Function: Automated media handling, cartridge cleaning, electronic labeling, bar coding, and media verification.

Benefit: Enables proactive corrections to minimize downtime and provide database integrity in event of unexpected or incomplete shutdowns.

ENHANCED NETWORK AND APPLICATION SERVICE LEVELS

Feature: Storage Nodes provide load sharing and LAN-free protection in DAS and SAN environments.

Function: Perform "hot" backups to maintain user access.

Benefit: Serverless backup frees your enterprise from the impact of data protection operations, maximizing network and application service levels.

DATA PROTECTION AND RECOVERY

Feature: Application modules that provide database, messaging, and enterprise resource planning (ERP) backup and recovery for 24x7 environments.

Function: Provide online protection and granular recovery.

Benefit: Provides data protection for Oracle, Sybase, Informix, Microsoft SQL Server, IBM DB2, Microsoft Exchange Server, Lotus Notes/Domino, and SAP R/3 on Oracle applications.

HIGH-AVAILABILITY CLUSTER SUPPORT

Feature: Sun Cluster software support.

Function: Support for backup clients and Sun StorEdge Enterprise Backup server in Sun Cluster and Solaris Operating Environments.

Benefit: Provides data backup and recovery in high-availability clustered environments.

ENTERPRISE-CLASS NAS PROTECTION

Feature: Expanded Network Data Management Protocol (NDMP) Support.

Function: Clones NDMP savesets from tape.

Benefit: Provides Direct Access Restore (DAR), increasing speed of recovery of NDMP-based backups.

Back to Top

Enabling Technology

Improved data availability
Sun StorEdge Enterprise Backup software 7.0 helps improve data availability and data protection. It is designed to allow you to establish a policy for each system so that if the primary backup server is not available, the scheduled backups are directed to secondary systems and completed. With Sun StorEdge Enterprise Backup software, duplicate copies of data can be automatically created at an offsite location for safekeeping. The software also supports fast system recovery by requiring only the backup server indexes to be available to recover all data.

High-performance network backup
For mission-critical environments, high-performance data protection and storage management applications are crucial. Sun StorEdge Enterprise Backup software is designed for rapid data movement. It delivers high-speed backup through parallel processing of multiple client backups, which are directed to multiple devices simultaneously. Using parallel backup sessions, the software can backup or restore faster than a single tape drive. This helps improve client performance and backup throughput. Additionally, magnetic disks may be used as backup media, further improving fast data backup and recovery speeds.

Integrated database and application backup
Sun StorEdge Enterprise Backup software not only provides backup and storage management services for file systems, it also extends those services to databases and mission-critical applications. Sun StorEdge Enterprise Backup software modules for key databases and applications-such as Oracle, Informix, Sybase, Lotus Notes/Domino, Microsoft SQL Server, and Microsoft Exchange-provide automated, online backup and storage management of these environments. The software also includes support for raw partitions for databases that access file systems directly.

Improved utilization of resources
Many of the advanced storage management applications allow more effective use of system, storage, and administrative resources. Through Sun StorEdge Enterprise Backup software's Archive module, data can be optionally removed from a disk for conservation of storage space once it has been safely stored offline. The Archive module is an advanced data management application that delivers file-level archiving and file-grooming services for authorized clients on the network. It allows logical grouping of associated files under a common archive name for simpler restoration.

Storage Nodes
Sun StorEdge Enterprise Backup software supports large enterprise networks and allows the backup of data to a remote device attached to a secondary backup server called a storage node. A storage node is a Sun StorEdge Enterprise Backup software client that runs on the Solaris[tm] Operating Environment and uses local devices for backup and recovery, yet relies on the primary backup server for index and control information. Storage nodes facilitate the distribution of backup performance around the network and improve the reliability of those backups without increasing management overhead. Network users can also backup, recover, or archive their local files without assistance from the system administrator and without knowledge of where the data is located.

Dedicated Storage Node
The dedicated storage node provides a cost-effective method to achieve local area network (LAN)-free backup utilizing a storage area network (SAN) infrastructure. It delivers the same advanced features and functions of a traditional storage node, but it does not accept data streams from remote Sun StorEdge Enterprise Backup software client hosts. Both the dedicated storage node and the traditional storage node fully support SAN technologies for LAN-free backup. The dedicated storage node is designed to provide a low-cost method for upgrading Sun StorEdge Enterprise Backup software client hosts (LAN backup) to use storage node technology for LAN-free backup.

Dynamic drive sharing
Sun StorEdge Enterprise Backup software builds on Solstice Backup 6 software's library sharing by adding the capability of dynamically allocating a tape drive to a Sun StorEdge Enterprise Backup software server or storage nodes or NDMP-enabled NAS storage devices. Tape drives on centralized libraries can now be allocated to a Sun StorEdge Enterprise Backup software server or to multiple storage nodes as needed for backups and restores. Dynamic drive sharing leverages the capability of Fibre Channel tape drives and libraries to enhance efficiency in physical resource management.

Fibre Channel tape drive support

Sun StorEdge Enterprise Backup software offers support for Sun's Fibre Channel tape option. The software also offers support of Sun's Fibre Channel driver module and tape drives to enable the latest capability in high-speed, distributed data movement for both backup and restore.

Back to Top

System Architecture

Sun StorEdge Enterprise Backup Software has a client/server architecture comprised of three distinct functions-client, storage node, and server-that offers the flexibility and performance required to protect and manage data. The data protection process is encompassed in a data zone, which is the collection of clients, storage nodes, and data protected by a single Sun StorEdge Enterprise Backup software backup server. A software data zone can be collectively administered with a single set of storage management policies and procedures.

Sun StorEdge Enterprise Backup Software 7.0 was built from the ground up to benefit from its client/server architecture. With Sun StorEdge Enterprise Backup Software 7.0 the processing responsibilities are effectively "shared" between the client and the server. The immediate benefits of this approach are two-fold:

- It provides the ability to harness the distributed network computing model to provide a flexible backup operation.
- "Any client" to "any server" to "any storage device" interoperability helps allow Sun StorEdge Enterprise Backup software to provide an approach to storage management that is consistent across most major server platforms.

Key Points: Client
In the Sun StorEdge Enterprise Backup software storage management model, the client has several active roles:

- Automates response to backup requests, navigates the file system, and pushes the data to the server
- Supports client-side data compression, encryption, and password protection
- Administrative mode-provides the interface for monitoring and control of multiple storage management servers
- User mode-provides the interface for user-initiated backup/recovery or archive/retrieval operations

Sun StorEdge Enterprise Backup software's client-side data generation, data compression, and data encryption capabilities accelerate throughput while helping to minimize server load and network traffic for exceptional scalability and performance.

In addition, the software's ability to run parallel data streams simultaneously from multiple clients delivers excellent performance.

Key Points: Server
By delegating data sourcing to the client, the Solaris Operating Environment-based Sun StorEdge Enterprise Backup software server can dedicate itself to the role of resource manager, including:

- Executing backup schedules and policies
- Automated multiplexing of several simultaneous client sessions into a single, interleaved data stream out to one or more storage devices-client parallelism and device level interleaving
- Automated resource management for concurrent device operation
- Staged storage management to attached storage automatically
- Dynamic load balancing among available storage devices
- Maintaining separate on-line client file indexes for each client
- Robust client file index management with high-speed indexing and efficient segmentation
- Administration via Microsoft Windows, X-Windows Motif, or full function CLI

Sun StorEdge Enterprise Backup software assigns much of the processing for backup and recovery to the client, allowing the server to take better advantage of network and backup server bandwidth to process multiple client data streams in parallel.

- Client parallelism for automated multiplexing of client data streams with up to 512 parallel

13.407

sessions for backup and recovery
- Automated resource management for concurrent device operation with up to 32 concurrent devices

Sun StorEdge Enterprise Backup software provides multi-client file index management. The software has been optimized for rapid insertion of file entries in the on-line index. Each client using the software has a separate client file index to distribute index management workload and reduce lock contention.

Key Points: Media
Sun StorEdge Enterprise Backup software's intelligent media management handles and automates such tasks as media labeling, media rotation, and media tracking. The software delivers a consistent set of media management features across a wide range of media technologies.

- Facilitates robust, unattended operation with a powerful suite of automated media management routines
- Exploits the capabilities of high-performance, high-capacity autoloaders for enhanced throughput and automated operation
- Offers broad device support. The software's media and robotics-independent architecture provides uniform support for a wide variety of tape and auto-changer technologies, including QIC, 4-mm DAT, 8-mm, DLT, and optical devices from Sun and other suppliers

Sun StorEdge Enterprise Backup software's shared intelligence between client and server functions allows it to deliver efficient, cost-effective storage management solutions that range from standalone systems to enterprise-wide networks involving hundreds of clients and terabytes of data. The software's smart client server/architecture harnesses the resources of the network computing model for distributed processing of storage management tasks. In addition, its performance characteristics allow backups to be completed in less time by exploiting the power of high-performance servers, network connections, and storage devices for outstanding throughput.

Sun StorEdge Enterprise Backup software's client/server capabilities coupled with advanced device I/O management, exploit high-performance device technologies to accelerate throughput while helping to minimize server load and network traffic.

Interleaving protected data from different clients onto a common storage medium along with client parallelism allows Sun StorEdge Enterprise Backup software to stream one or more storage devices at full speed-a level of performance that is otherwise very difficult for network backup to achieve.

Sun StorEdge Enterprise Backup Software 7.0's client parallelism for both backup and recovery helps it maximize the effective throughput to the media device for storage management. Moreover, the software's performance scales efficiently as additional storage devices are dynamically added to the backup pool.

Self-defining, removable media provides for automatic recreation of Sun StorEdge Enterprise Backup software catalog information resulting in easy reconfiguration of Sun StorEdge Enterprise Backup software servers, catalog-independent recovery capabilities, and virtually fail-proof disaster recovery.

There is a limited backup window available for storage management. If you rely on the availability of critical applications that run the business, you must take full advantage of limited backup windows. Sun StorEdge Enterprise Backup software rapidly backs up large quantities of data by allowing multiple clients to be backed up simultaneously. This is called parallelism in a storage management operation.

And the same holds true for storage devices. Multiple tape drives and optical devices can be written to at the same time to help optimize data movement. This is called multiplexing. Sun StorEdge Enterprise Backup software can write save sets from multiple clients to the same tape drive, intermixing the save sets on the tape cartridge at the block level. On any given tape cartridge, backup data from multiple clients is intermixed.

Sun StorEdge Enterprise Backup Software is one of the few applications that can help drive high-speed tape devices at their maximum throughput rates. The software achieves this by constantly providing data to the tape drive, allowing for long-term data streaming. Tape devices do not reach maximum data throughput rates if they are regularly starting and stopping. If the tape drive is rated at 5 MB per second, Sun StorEdge Enterprise Backup software is one of the few applications that can backup data to the tape at near 5 MB per second speed. For companies with large amounts of data to back up, usually during off-hours, this concept can become critical.

Sun StorEdge Enterprise Backup software works in small environments with only a few servers and in

large environments with hundreds of servers. This type of scalability is provided through flexible configuration options within a data zone, as well as by the ability to configure multiple data zones into a common control zone. Sun StorEdge Enterprise Backup software grows dynamically with the fast-paced growth of distributed applications and the client/server architectures deployed for mission-critical applications.

Key Points: Storage Nodes
You can add capacity to deployed Sun StorEdge Enterprise Backup software data zones simply by assigning a Solaris Operating Environment-based networked server with available attached storage devices as a Sun StorEdge Enterprise Backup software storage node. Data and applications on the storage node or remote from it can use the storage management capacity at the storage node, while control and management remains centralized at the Sun StorEdge Enterprise Backup software server. This provides high-speed, localized storage management without using network bandwidth. It also allows redundant storage management devices for client services to "fail over" to in the event of hardware failures.

Key Points: Immediate Technology
Immediate technology is available in the Sun StorEdge Enterprise Backup Software Power Edition software that provides for very fast backup of large quantities of data with minimal CPU impact. The technology maximizes throughput by passing the TCP/IP layer for local backup/recovery. So storage nodes or backup servers that have locally attached disk and tape, can do backup and recovery faster as they do NOT have to go up and down the 7-layer TCP/IP stack when doing backups and recoveries.

Immediate technologies are for backing up, recovering, and copying backups using locally attached tape drives (on the same system where the data being backed up or cloned is stored). Immediate technologies use a shared memory buffer for "passing" the blocks in a data stream between the Sun StorEdge Enterprise Backup software client component and the Sun StorEdge Enterprise Backup software server component (save and recover).

Standard technology for save and recover relies on TCP and UDP for transmitting save set data streams between clients and servers, both for the data portion of the save set and for the control information for synchronizing the Sun StorEdge Enterprise Backup software client and server. Immediate technology only uses TCP for control information and passing pointers where the data block resides in the shared memory buffer.

Immediate cloning bypasses TCP/IP for local copies. Standard cloning technology uses TCP/IP for transmitting save set data streams, allowing for storage node cloning to Sun StorEdge Enterprise Backup software server or other storage nodes.

Key Points: Advanced Media Management
Sun StorEdge Enterprise Backup software offers many advanced media management features. It exploits the capabilities of high-capacity autoloaders for very high performance and fully automated operation. The software makes this possible with a powerful suite of media management routines. These routines simplify administration of media management, including disk device media support and automatic staging.

Media Handling Automation

- Media spanning and media changing for high capacity autoloaders
- Support for cartridge access ports and bar code readers allows rapid loading and inventory of media
- Cleaning cartridge support for regularly scheduled device maintenance and tracking of cleaning cartridge usage

Automated Resource Management

Sun StorEdge Enterprise Backup software offers exceptional flexibility for configuration of media resources, while helping reduce complexity for resource scheduling by automating resource management.

Media pools offer a flexible way to logically segregate data onto a particular set of media based on multiple criteria, such as clients, groups, backup schedules, and backup types.

Concurrent device support allows simultaneous operation of up to 32 storage devices including multi-device autoloaders. Sun StorEdge Enterprise Backup software supports concurrent device operation for mixed device pools, so devices do not need to be of identical make and model, or even of the same

media type.

Automatic, multi-tier backup staging helps reduce tape operations and helps increase performance by staging smaller volume backup, migration, and archive data to direct access storage devices. Sun StorEdge Enterprise Backup software automatically manages device capacity.

Dynamic load balancing automatically allocates client sessions among available storage devices within a media pool to help optimize throughput and device utilization.

Network loading offers the administrator the ability to control network data loading for backup and recovery by adjusting client parallelism and sessions per device settings.

Advanced Media Format

The OpenTape format is the key to many of Sun StorEdge Enterprise Backup software's advanced media management capabilities:

- The OpenTape format allows interleaved data to help enable client parallelism
- Self-identifying block headers provide transparent tape spanning and the ability to recover past bad spots on media
- Auto-verification helps ensure media integrity
- OpenTape allows Sun StorEdge Enterprise Backup software to recover indexes without searching the media
- OpenTape provides cross-platform compatibility across virtually every major network operating environment including the Solaris Operating Environment, Microsoft Windows 2000/XP, UNIX® platform, and NetWare

Sun StorEdge Enterprise Backup software's administrative model is designed to reduce complexity, and easily accommodate change and growth within the enterprise. Sun StorEdge Enterprise Backup software delivers a single, consistent solution for heterogeneous networks, allowing organizations to integrate their operating system environments into an enterprise-wide storage management strategy. The software's global approach for network-wide administration significantly reduces the time required to implement backup strategies. An operator can configure, schedule, or monitor network-wide backups for one or more Sun StorEdge Enterprise Backup software servers from any administrative nodes on the network.

Key Points: Updated User Interface
The user interface has been updated and includes the following features:

- Provides a consistent interface for centralized, local, or remote administration
- Provides monitoring of all server functions via a well-organized, on-screen console
- Allows administration of multiple servers from one screen simultaneously
- Wizards to help configure servers, clients, groups, and media

Group Schedules and Policies

- Backup administration is organized around groups of clients
- Menu-based policies and schedules can be easily created or edited for each group
- Point-and-click scheduling is available for nine differential levels of backup in addition to full, incremental, and skip
- The default policy allows new client volumes to be protected automatically as client capacity grows
- Powerful directives allow backups to be customized for the needs of each client
- Sun StorEdge Enterprise Backup software's approach virtually eliminates the need to create or maintain job scripts
- A full-function command line interface (CLI) is provided
- All GUI functions are available in command line format
- Custom productivity is provided via script-initiated Sun StorEdge Enterprise Backup software functions

Systems Management Framework Integration

- Sun StorEdge Enterprise Backup software offers customized integration with Tivoli's TME, CA's Unicenter and HP's IT/Operations through optional Legato complementary products
- Software can be launched directly from the central systems management framework console, providing consolidation of messages on a common console, and so on

Event Notification

Sun StorEdge Enterprise Backup software's powerful, yet flexible, event notification system allows the administrator to be selectively notified of high-priority alerts as well as routine events through e-mail, pager, or SNMP. The event notification system:

- Provides preconfigured priority alerts for all important storage management events
- Automates routine notification for daily reporting of backup session status
- Allows unattended lights out mode until operator intervention is required
- Integrates easily with corporate e-mail systems and systems management tools

Back to Top

System Management

There are four editions of Sun StorEdge Enterprise Backup software designed to fit the needs of high-end enterprise and mid-range corporate computing environments.

Sun StorEdge Enterprise Backup Software 7.0 - Business Edition

The Sun StorEdge Enterprise Backup Software Business Edition is a high-performance storage management solution ideally suited for small business, remote branch offices, mixed-platform LANs, and new deployments of LANs inside growing enterprises. This edition goes far beyond the feature set of a typical entry-level network backup product, providing scalability and investment protection through an easy upgrade path to the Network and Power Editions. It supports full, incremental, and differential backup operations. It also provides active backup support for a 2-node cluster (database and/or Email application) and NDMP-based small network attached storage (NAS).

Sun StorEdge Enterprise Backup Software 7.0 - Workgroup Edition

The Sun StorEdge Enterprise Backup Software Workgroup Edition is a high-performance storage management solution for small networks in corporate environments. This edition is ideally suited for remote branch offices, mixed-platform LANs, and new deployments of LANs inside growing enterprises. It goes far beyond the feature set of a typical entry-level network backup product, providing scalability and investment protection through an easy upgrade path to the Network and Power Editions. It supports full, incremental, and differential backup, and has the following capabilities:

- Increased scalability: Local or remote centralized administration capabilities and client/server architecture support automated backup for up to seven network-attached workstations and file servers. Sun StorEdge Enterprise Backup software also offers a seamless upgrade path to the Network Edition or Power Edition. This provides investment protection and allows your customers to "pay as you grow."
- Enhanced performance: A unique parallel streaming feature supports up to 12 simultaneous client backup/recover sessions on a single Workgroup Edition system.
- Outstanding reliability: Industry-standard OpenTape format, from Legato, supports data multiplexing for backup and recover operations, offering excellent performance and data reliability.
- Concurrent device support: This edition provides support for backup and recovery operation using up to four backup devices simultaneously per Sun StorEdge Enterprise Backup software server or storage node, including multiple autochangers.
- Autochanger ready: Systems running Workgroup Edition software can be extended to operate up to a 1 to 32 autochangers through the addition of the appropriate Autochanger Software Module. The Workgroup Edition software is ideal for a remote office or small department that needs an entry-level Sun StorEdge tape library.
- Sun StorEdge Enterprise Backup Software 7.0 -ready: The capabilities of Workgroup Edition software can be extended to provide online data protection for business-critical database and applications with the addition of Sun StorEdge EBS Modules.

Sun StorEdge Enterprise Backup Software 7.0 - Network Edition

The Sun StorEdge Enterprise Backup Software Network Edition is a highly reliable, enterprise-strength storage management solution for distributed networks. Sun StorEdge Enterprise Backup software is highly scalable, with outstanding manageability, availability, and performance. The Network Edition software supports ten clients, as well as options that add client connections, cluster client connections,

and expanded client platform coverage, and deliver services such as archiving, library sharing, SNMP manageability, and StorEdge EBS database/applications support. Sun StorEdge Enterprise Backup software options include the following powerful capabilities:

- Virtually unlimited scalability: Local or remote centralized administration capabilities and client/server architecture support automated backup for hundreds to thousands of network-attached workstations and file servers.
- Excellent performance: A parallel streaming feature supports up to 32 simultaneous client backup/recover sessions on a single Network Edition system.
- Outstanding reliability: Industry-standard Legato OpenTape format supports data multiplexing for backup and recover operations, giving unmatched performance and data reliability.
- Concurrent device support: The Network Edition provides support for backup and recovery operation using up to 16 backup devices simultaneously per Sun StorEdge Enterprise Backup software server or storage node, including multiple autochangers.
- StorEdge Enterprise Backup Storage Nodes: Support provides load sharing within a StorEdge EBS data zone, helping enable large servers to be protected LAN-free and in less time, and increasing scalability as your backup environment grows.
- NDMP ready: Sun StorEdge Enterprise Backup software can be enabled to backup network attached storage (NAS) devices using NDMP.
- Native Library Sharing and Dynamic Drive Sharing (DDS) Ready: DDS Options allow tape drives to be dynamically allocated as needed within a Data Zone over a Fibre Channel SAN between a Sun StorEdge Enterprise Backup software server, storage node(s), and NDMP-compliant NAS file servers delivering faster backup and recovery and maximum library ROI.
- Autochanger ready: Systems running Network Edition software can be extended to operate with a very wide range of tape and optical autochangers through the addition of the appropriate Autochanger Software Module.
- StorEdge Enterprise Backup DiskBackup Option Ready (all Editions): This option leverages the performance of high capacity, high-speed disk arrays to protect and recover data faster. It is an deal compliment to tape storage to maximize protection, reduce backup window needs, and minimize downtime costs.
- Archive ready: Sun StorEdge Enterprise Backup software can be expanded into a full-feature storage management platform through the addition of the Sun StorEdge Enterprise Backup Software Archive modules.
- Cluster client ready: Network Edition software includes extensive support for clustered environments using Sun Cluster, Hewlett Packard MCSG, IBM HACMP, Compaq TruCluster, Microsoft Cluster Services, and Legato Availability Manager.
- SNMP ready: The Sun StorEdge Enterprise Backup software SNMP Module runs on any supported hardware platform and in any environment or system management framework that supports SNMP traps.
- SSun StorEdge Enterprise Backup Software Module ready: The capabilities of Network Edition software can be extended to provide online data protection for business-critical database and applications with the addition of Sun StorEdge Enterprise Backup Software 7.0 Modules.

Sun StorEdge Enterprise Backup Software - Power Edition

Sun StorEdge Enterprise Backup Software Power Edition is a high-performance storage management solution for customers with very large servers, clusters, or the requirement to drive high-speed devices. Power Edition features enhanced local architecture designed to dramatically increase local throughput, while minimizing use of system resources. The Power Edition software supports all standard Sun SorEdge Enterprise Backup software options. It includes two like-kind cluster client connections. With the addition of Power Edition storage nodes, it can support up to 512 parallel streams of data, and a maximum of 256 concurrent devices.

Back to Top

Service and Support

Sun Services Software Support (S4) makes available the following levels of service:

Standard Support - 1.The Sun Software Standard Support offering provides a comprehensive support plan. Features include:

- Extended local business hours (5x12) for telephone and online support
- Four (4) business hour response on Priority 1 (Urgent) requests
- Two (2) authorized contacts
- Online incident submission and tracking

- Software updates and patches
- Access to online self-solve resources

Premium Support - The Sun Software Premium Support offering is designed for critical environments where high availability is a priority and round-the-clock support is a customer requirement. This level of service offers:

- 7x24 coverage with live call transfer for Priority 1 (Urgent) requests
- Three (3) authorized contacts per 8-hour shift
- Plus, all of the features of the Standard support level

Back to Top

13.401

SUN STOREDGE L700 TAPE LIBRARY
Specifications

Sun StorEdge L700
» Features, Functions & Benefits
□ Specifications
» Detailed View
» In the Spotlight

Storage Related:
» White Papers
» Success Stories
» Press Releases

See Also:
» Remote Management
» Professional Services
» Sun Servers
» PatchPro

Contact Me

CAPACITY AND PERFORMANCE

Drives	9940B	SDLT 320	LTO	DLT8000	9840B	9840
Library Capacity (native, with 678 tapes)	135.6 TB	110.4 TB	135.6 TB	27.1 TB	13.8 TB	13.56 TB
Cartridge Capacity (native)	200 GB	160 GB	100 GB	40 GB	20 GB	40 GB
Sustained Transfer Rate (native, concurrent operation of all drives)	12	20	20	20	12	12
Tape Load Time (to BOT)	12 seconds	10 seconds	12 seconds	4 seconds	4 seconds	4 seconds
Average File Access Time	70 seconds	76 seconds	76 seconds	60 seconds	11 seconds	11 seconds

LIBRARY & ROBOTICS

Average cartridge swap time	Seven seconds
Robotics MSBF	One million load/unload cycles
Robotics MTBF	70,000 power-on hours
MEBF	Two million exchanges
Hot-plug drives	Yes
Redundant power	Yes (for robotics only, via second drive column)
Startup/boot time	Three to four minutes (average)
Burst rate (each drive)	40 MB/sec
Inventory time	Less than six minutes (fully loaded, with barcodes)
Robotics	v1.0

INTERFACES

Ultra differential	Fast/Wide SCSI-2
SCSI	Wide, high-voltage differential
LVD	Low-voltage differential
Native 2 Gbit Fibre Channel	LC connection
Control Panel	Low-Voltage differential

SOFTWARE

Operating System	Solaris Operating Environment v2.6, 7, 8, and 9
	Sun StorEdge Utilization Suite software

Software Compatibility	VERITAS NetBackup software v3.2 or later VERITAS Storage Migrator software v3.2 or later Solstice Backup software v5.5.1 or later

HARDWARE

Hardware Compatibility	Sun Enterprise 250, 450, 3x00, 4x00, 5x00, 6x00, and 10000 servers Sun Fire V880, 3800, 4800, 4810, 6800, and 15K servers

ENVIRONMENT

Operating	15ºC to 32ºC (59ºF to 90ºF) 20% to 80% relative humidity, noncondensing
Nonoperating	-20ºC to 60ºC (-4ºF to 140ºF) 5% to 95% relative humidity, noncondensing

ELECTRICAL

	Library Enclosure	Single-drive column
Power cable US/Canada	100 VAC UL/CSA	120 VAC UL/CSA
Input voltage range	90 to 254 VAC	90 to 254 VAC
Nominal voltage (per power supply)	120 or 240 VAC	120 or 240 VAC
Power configuration US/Canada	Single-phase 100 VAC, 47 to 63 Hz	Single-phase 120 VAC, 47 to 63 Hz
Power consumption	210 W	972 W
Maximum heat output	716 BTU/hr	3314 BTU/hr

REGULATIONS

Meets or exceeds the following requirements:

Safety	UL1950 listed, CSA C22.2-No. 950-M89, TUV-EN60950
Emissions	FCC Part 15B Class A, CE Mark, VCCI Class A

DIMENSIONS AND WEIGHTS

Height	183 cm (72 in.)
Width	156 cm (62 in.)
Depth	110 cm (43.5 in.) (with expansion door) 95 cm (37.5 in.) (without expansion door)
Weight	427 kg (941 lb.) (without drives or cartridges)

WARRANTY

One year warranty	15-day parts exchange

1. This page meets my need. disagree ○ ○ ○ ○ ○ ○ ○ agree
2. This page was easy to find. disagree ○ ○ ○ ○ ○ ○ ○ agree

Comprovação das Especificações Exigidas no Edital 050/2003

6. Ambiente de segurança

NEC

13.398

Comprovação das Especificações Exigidas no Edital 050/2003

6.1. Servidor de segurança lógica tipo 1

Servidor de Segurança Lógica Tipo 01	
535_ds.pdf	Cisco PIX 535 Security Appliance
pix_qa.pdf	Cisco Secure PIX Firewall Series
idsdp_rg.pdf	Cisco IOS Intrusion Detection Systems

CISCO SYSTEMS

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

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.

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

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

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+)

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

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)

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

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

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

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

RD/LW3946 04/03

Cisco Systems

Design Guide

Cisco IOS **Intrusion Detection** Systems

Executive Summary

Intrusion detection has become a critical component of Enterprise and Service Provider infrasturctures. Increasing complexity in public networks for data transport in light of new business applications, e-commerce, extranets and virtual private networks (VPNs) has created increased risks to the integrity and security of internal network.

In order to counter increasing security threats, Cisco IOS, Intrusion Detection Systems (IDS) offers added abilities for detection, logging, auditing and mitigation to a variety of existing security products. Cisco offers complementary technologies in firewall products (Cisco IOS Firewall, PIX, etc), encryption technologies (Cisco IOS IPSec VPNs, Cisco VPN-3000, Authentication, Authorization, and Accounting [AAA]) for a full-layered approach security.

Cisco IOS IDS includes intrusion detection technology for the full range of Cisco IOS routers. Cisco 1700, 2600, 3600, 7100, 7200, 7500, and RSM Series Routers support Cisco IOS IDS. The Cisco 830 Series router will support Cisco IOS IDS. It is targeted for November 2003 . These intrusion detection capabilities are ideal for monitoring intranet, extranet, and branch office Internet perimeters against network violations. Integrated into the routing path, Cisco IOS IDS uses signatures to identify common attacks, and to subsequently protect the network.

Cisco IOS IDS acts as an in-line intrusion detection sensor, watching packets as they traverse the router's interfaces and acting upon them in a definable fashion. When one or more packets in a session match a signature, Cisco IOS IDS may perform the following configurable actions:

- *Alarm*: sends an alarm to a syslog server or Net Ranger Director
- *Drop*: drops the packet
- *Reset*: resets the TCP connection

Through the use of syslog and integration with CiscoWorks VPN/Security Management Solution (VMS), security operations can quantify their security posture and determine any threats to the networks. These metrics provide a machanism to track unauthorized network activity over time and evaluate security policy effectiveness, security activities, and budgeting considerations from a quantifiable perspective.

The remainder of this guide provides a background of information for Cisco IOS IDS, design considerations and scenarios for deployment. Cisco IOS IDS is available in Cisco IOS Software Release 12.0.(5)T and later releases. Advanced performance improvements for Cisco IOS IDS were released in Release 12.2.(8)T.

Cisco Comprehensive Security Solution

Intrusion detection implementation requires planning. Intrusion detection technology is a complementary tool that should be utilized alongside traditional security products. Cisco IOS IDS is one part of the end-to-end security solution. Products such as Firewalls, Encryption and Authentication, and Access Control Lists should be part of an integrated approach to implementing any Corporate Security Policy.

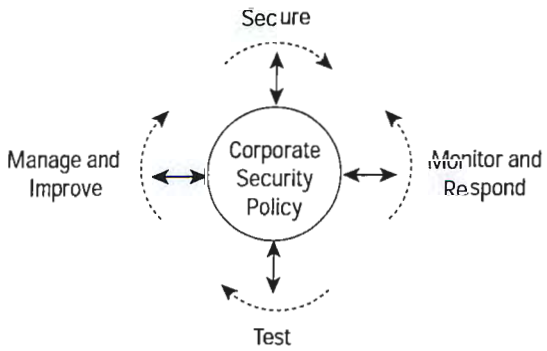
Considerations for the following should be taken into account to understand overall security concerns:

- Security Wheel
- Developing a Strong Security Policy
- Securing the Network
- Monitoring the Network
- Testing Security
- Improving Security

The Security Wheel

The Cisco security solution approach is one of an operational perspective rather than one of a products or policy approach. Like network management, the philosophy is one that addresses a dynamic, process towards security.

Figure 1. The Security Wheel



The Security Wheel is cylical, ensuring diligence and imporvement. The paradigm incorporates the following five step:

1. Develop a strong security policy
2. Secure the network
3. Monitor the network and respond to attacks
4. Test existing security safeguards
5. Manage and improve corporate security

Data gained from Steps 2 through 5 should always be reflected back to the corporate security policy in Step 1, so that high-level security expectations are being met.

Developing a Strong Security Policy

Consideration of the following is crucial in developing a strong security policy:

- What assets must be protected?
- What is the risk to those assets?
- What is the impact (in terms of reputation, revenues, profits, research) of a successful attack?
- How much sensitive information is available online? What is the impact if this information is damaged or stolen?
- Which users have access to those assets?
- What do users (including partners and customers) expect in terms of security control procedures and mechanisms?
- Should users be trusted?
- Are users accessing assets locally or remotely, or a mixture of both?
- Do distinct parts of the organization have different security requirements?
- What types of traffic exist on the network?
- Are the needs of security consistent with the business/operational needs of the organization?
- Is there a strong commitment from management to provide sufficient resources to implement security policies and technologies?
- Is there a strong commitment for security awareness training?

A strong security policy should be clearly defined, implemented, and documented, yet simple enough that users can easily conduct business within its parameters. A policy of strong password creation can only work if there is a system to validate password selection.

In many ways, the security policy is a risk management plan, as it documents the risk threshold an organization is willing to accept. Because no security technology provides one hundred percent protection, and in most cases organizations do not have the budget to implement all required security elements, the security policy rates assets and applies commensurable levels of security.

A critical element often overlooked is the policy on incident response. What is the official organization response if a policy is violated?

For additional information on the development and implementation of information security policies, refer to SANS Institute Resources: http://www.sans.org/newlook/resources/policies/policies.htm

Securing Your Network

Once the security policy is developing, the network must be secured with multiple technologies: firewalls, intrusion detection, AAA, etc. However, this cannot occur without complete understanding of the user, assets, and network topology.

Understand Your Network Topology

Careful inspection of the following will help to prevent possible miscalculations in deploying and configuring Cisco IOS IDS:

- Network size and complexity
- Locations of critical resources (file servers, hosts, etc.) on the network
- Connections with other networks, both Internet and extranets
- The amount and type of network traffic

Consideration of these placement points will help determine where Cisco IOS IDS can be enabled. All connections to the network that require protection should receive the same degree of consideration.

Monitoring the Network

Once the network has been secured, activity should be monitored, either via syslog or through the use CiscoWorks VMS. When a security violation does occur, an appropriate response is crucial:

- Logging the event
- Resetting the TCP connection
- Dropping the offending packets
- Possible reconfiguration of the ACLs on the router, in order to deny the attack

Specific responses should be detailed within the security policy.

Testing Security

Periodic scans of the network for new vulnerabilities are appropriate. Changes in the network and service/technology advancement can create new "security holes". These aspects are inevitable and should be considered normal operations within a growing network. New test procedures for testing security as well as testing the pre-established policy should be part of this review procedure for improvement.

Improving Security

Analyze all the metrics that are collected. Each part of the security cycle will produce different information, which can then be prioritized. When responding to a threat, consider:

A) Identify resources required to respond

B) Incident response policy

C) Chart ownership and monitoring of security

Keep abreast of any new network threats by improving on the established security policy. Continue to implement the Security Wheel cycle.

Technical Highlights

Cisco IOS IDS supports intrusion detection technology for midrange and high-end router platforms with firewall support. It is ideal for any network perimeter, and especially for locations in which a router is deployed, and additional security between network segments is required. It also can protect intranet and extranet connections where additional security is mandated, and branch-office sites connecting to the corporate office or Internet.

Intrusion detection systems provide a level of protection beyond the firewall by protecting the network from internal and external attacks and threats. Cisco IOS IDS enhances perimeter firewall protection by taking appropriate action on packets and flows that violate the security policy or represent malicious network activity.

Cisco IOS IDS acts as an in-line intrusion detection sensor, watching packets as they traverse the router's interfaces and acting upon them in a definable fashion. When one or more packets in a session match a signature, Cisco IOS IDS may perform the following configurable actions:

- *Alarm*: sends an alarm to a syslog server or Net Ranger Director
- *Drop*: drops the packet
- *Reset*: resets the TCP connection

Intrusion detection systems customers that have already deployed Cisco IDS "appliance sensors" can deploy Cisco IOS IDS signatures to complement their existing systems. This allows an intrusion detection system to be deployed in areas that may not support a Cisco IDS Sensor. Cisco IOS IDS signatures can be deployed alongside or independently of other Cisco IOS Firewall features.

Cisco IOS Firewall with intrusion detection can be added as an icon on the Cisco VMS Security Monitor screen, providing a consistent view of all intrusion detection sensors throughout a network. Cisco IOS Firewall intrusion detection capabilities have an enhanced reporting mechanism that permits event logging to the Security Monitor console via Cisco IOS syslog.

Cisco IOS IDS utilizes signatures to detect patters of misuse in the network. Each signature is categorized by severity and complexity. Signatures are classified by both severity and complexity:

Severity:

Informational signatures: detect information (ie: port sweep)

Attack signatures: detect malicious activity (ie: illegal ftp commands; Denial of Service (DoS attempt),

Complexity:

Atomic signatures: detect simple patterns (ie: attempt on a specific host or within a single packet)

Compound signatures: detect complex patterns (ie: attack on multiple hosts, over extended time periods with multiple packets)

Configuration Basics

1. Initialize Cisco IOS IDS—ip audit parameters (alarm, drop, and/or reset)

An audit rule specifies the signatures that should be applied to a packet traffic and the actions to be taken when a match is found. The signature list can include any number of signatures. Signatures can be disabled in case of false positives, or based on the needs of the network.

Note: it is generally recommended that drop and reset actions be used together.

Command Syntax:

```
   ip audit info {action [alarm] [drop] [reset]}        ! Sets the default actions for
info and attack signatures
   ip audit attack {action [alarm] [drop] [reset]}
   ip audit name audit-name {info | attack} [list standard-acl] [action [alarm] [drop]
[reset]] ! Creates audit rules, where audit-name is a user-defined name for an audit rule.
```

2. Determine logging Policy

Command Syntax:

```
ip audit notify log    ! Sends event notifications (alarms) to either a Cisco Secure
IDS Director, a syslog server, or both.
```

3. Configure and Apply Audit Rules—which interfaces, what routing path?

Audit rules can be applied to an interface on the router with a specific direction (*in* or *out*).

If the audit rule is applied to the in direction on the interface, packets passing through the interface are audited before the inbound ACL can to discard them. This alerts an administrator if an attack or information-gathering activity is underway. Because of this sequences of events, IDS can trigger even if the router would otherwise reject the activity.

Audit rules that are applied in the out direction on an interface are conversly auditing packets after they have entered the router through another interface. Inbound ACLs of other interfaces may discard packets before they are audited. As such, IDS alarms may be lost even though the attack or information-gathering activity was thwarted.

Command Syntax:

```
interface interface-number          ! Enters interface configuration mode.
ip audit audit-name {in | out}      ! Applies an audit rule at an interface. With this
command, audit-name is the name of an existing audit rule, and direction is either in or
out.
```

4. Verify the Configuration

```
show ip audit configuration
show ip audit interface
show ip audit statistics
```

5. Optionally Disabling Signatures

```
ip audit signature signature-id {disable | list acl-list}    ! Disables individual
signatures.
```

Cisco IOS IDS Deployment Scenarios

Cisco IOS IDS capabilities are ideal for providing additional visibility at intranet, extranet, and branch-office Internet perimeters. Network administrators enjoy more robust protection against attacks on the network and can automatically respond to threats from internal or external hosts.

Cisco IOS IDS is intended to satisfy the security goals of all of our customers, and is particularly appropriate for the following scenarios:

- *Enterprise*: interested in a cost-effective way to extend perimeter security across all network boundaries, specifically branch-office, intranet, and extranet perimeters.
- *Small and medium businesses*: need a cost-effective router that has an integrated firewall with intrusion-detection capabilities.
- *Service Providers*: may want to deploy this as the router/firewall for a managed service. They can set this at subscribers' sites to provide firewalling and intrusion detection within the necessary function of a router.

Commonly referred to as "perimeter protection" Cisco IOS IDS can be placed to monitor traffic between the network and the Internet. Companies generally also use a firewall to protect the perimter, which the most common deployment scenario. This enables the both incoming and outgoing traffic to be monitored.

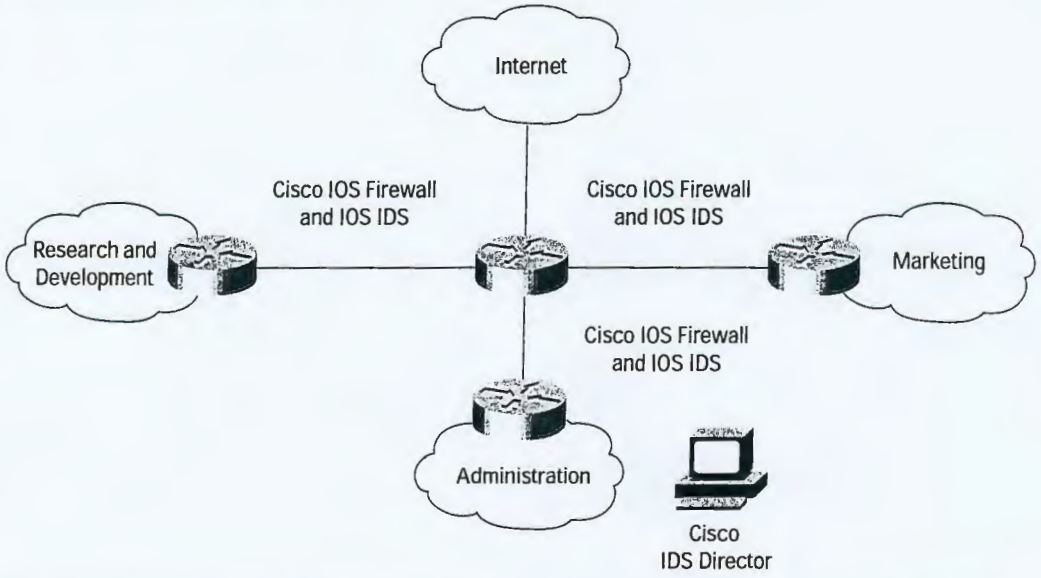
An internal attacker can additionally take advantagte of network services that otherwise go unprotected. For this reason, the perimeter protection offers little help. Placing Cisco IOS IDS on other segments, and in the routing path solves this problem and can shield from outside attacks, while addressing often overlooked networks: extranet, remote access, and less secure intranet networks.

Although partner companies generally have security policies of their own, there is often little reassurrance that these policies are adequately enforced. Outsiders often may enter a network through this type of connection, so it should also be protected and firewalled.

Remote access networks are also notorious for their vulnerability to attack. Although generally designated for employee use, external attackers often expliot vunerabilities in authorization, authentication and or wireless technologies. Cisco IOS IDS defends and monitors against such weaknesses in this area.

As mentioned earlier, intranet connections should also be monitored and protected with Cisco IOS IDS. Research and Development networks and Engineering resources, for example, often require additional security mesurements to protect proprietary information. For these areas, a robust security solution can be achieved by utilizing a combined approach of strong access control lists, Cisco IOS Firewall, and Cisco IOS IDS. (Figure 2).

Figure 2. Combined Security Approach



When Cisco IOS IDS is deployed, audit rules are applied specifying the direction of traffic through an interface (in or out).

Audit rules applied to the in direction on an interface will allow packets passing through the interface to be audited before inbound ACLs.

Audit rules applied to the out direction of an interface allow signature matching to occur against packets after they enter the router through another interface. In this case, inbound ACLs may discard packets before they are audited. Unintentional loss of Cisco IOS IDS alarms may result, despite the avoidance of an attack or information-gathering activity. Detection of such unsuccessful violations and attack attempts are often equally as important as detecting successful attacks.

Memory and Performance Impact

The performance impact of intrusion detection will depend on the configuration of the signatures, the level of traffic on the router, the router platform, and other individual features enabled on the router (ie: encryption, source route bridging). Enabling or disabling individual signatures will not alter performance significantly; however, signatures that are configured to use ACLs will have a significant performance impact.

The network only uses this router as a security device; therefore, no packet is allowed to bypass the security mechanisms. Cisco IOS IDS sits directly in the packet path, so it searches each packet for signature matches. In some cases, the entire packet will need to be searched, while the router must maintain state information, application state, and awareness.

There is no traffic-dependent memory requirement for auditing atomic signatures. For auditing compound signatures, CBAC allocates memory to maintain the state of each session for each connection. Memory is also allocated for the configuration database and for internal caching.

Differing Cisco IDS Products

- Cisco IOS IDS (Router Sensor): Cisco IOS IDS delivers in-line integrated intrusion protection in the routing path with a feature-rich set of networking services. It provides real-time monitoring, interception, and response to network misuse with a broad set of the most common attack and information-gathering intrusion detection signatures.
- Cisco IDS -4210, 4235, 4250 (Network Sensor Appliance): Network sensor provides a comprehensive dedicated appliance model to protect the network of observation from malicious activity.
- Cisco IDS Module (Integrated Switch sensor): Integrated Switch Sensor is designed to protect switched environments by integrating full-featured IDS functionality directly into the network infrastructure. This allows the user to monitor traffic directly off the switch backplane.
- Cisco IDS Host Sensor: The Host Sensor provides comprehensive protection for the server operating system and the applications running on the servers. It is installed on each server, guarding operating system and applications, as well as access to those applications. The system employs call interception techniques to provide the only proactive server security system.
- Firewall Sensor: Integration of IDS functionality into Cisco PIX Series Firewalls. This protects common network-based attacks.

Conclusion

Cisco IOS IDS supports intrusion detection technology for midrange and high-end router platforms with firewall support. It is ideal for any network perimeter, and especially for locations which a router is being deployed and additional security between network segments is required. It also can protect intranet and extranet connections where additional security is mandated, as well as branch-office sites connecting to the corporate office or Internet.

Intrusion detection should be considered an integral component when designing and implementing a layered approach towards security. Sensors may be placed on almost any network segment of the enterprise-wide network where security visibility is required. Perimeter placements, internal network segments where critical resources are located, extranet connections, and DMZs are the most minimal of locations to consider when implementing and maintaining a security policy.

The Security Wheel can help to attain the goal of security in an ever-changing environment. To ensure that a high percentage of security objectives are achived, always secure, monitor, test, and improve.

References

Cisco IOS IDS (Product Documentation)

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t5/iosfw2/ios_ids.htm

Improving Security on Cisco Routers

http://www.cisco.com/warp/public/707/21.html

Security Technical Tips

http://www.cisco.com/warp/customer/707/index.shtml#IOS

Configuring Context-Based Access Control

http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a00800ca7c5.html

Configuring Cisco IOS IDS

http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a00800ca7c6.html

Defining Strategies to Protect Against TCP SYN Denial of Service Attacks

http://www.cisco.com/warp/public/707/4.html

Cisco IOS IDS Signature List

http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a00800ca7c6.html

SANS Institute Resource Project—The SANS Security Policy Project

http://www.sans.org/newlook/resources/policies/policies.htm

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

Cisco Secure PIX Firewall Series

Q. What type of firewall is the Cisco Secure PIX™ Firewall? How is it different from other firewall products on the market?

A. The Cisco Secure PIX Firewall is a family of stand-alone, special-purpose firewalls that delivers stateful security and extremely fast performance to corporate and service provider networks. These firewalls thoroughly conceal an internal network from the outside world—providing full firewall security protection. Unlike typical CPU-intensive proxy servers running on general purpose operating systems that perform extensive processing on each data packet, PIX Firewalls use stateful technology implemented in a secure, real-time, embedded operating system. This technology enables The Cisco Secure PIX Firewall series to deliver outstanding performance for more than 250,000 simultaneous connections, dramatically surpassing the performance of "general purpose" operating system-based firewalls. The Cisco Secure PIX Firewall is now extensible, with support for up to six fast Ethernet network interfaces.

Q. What is the difference between the new PIX 515 platform and the PIX 520?

A. The PIX 515 is a slimline, Ethernet-only PIX hardware platform designed for small-to-medium locations. The PIX 520 is an enterprise-class chassis with more processor power, interface options and support for high volumes of traffic than any firewall device in the world. Both platforms provide PIX Firewall-quality performance and stability.

Table 1 Specifications for the Cisco Secure PIX 515 vs. the PIX 520 Firewalls

PIX 515	PIX 520
200-MHz processor	350-MHz processor
Two expansion slots	Four expansion slots
64-MB RAM, maximum	128-MB RAM

Q. Does fail-over work with the Cisco Secure PIX Firewall?

A. Most Cisco Secure PIX Firewall models can be run in redundant mode with a secondary PIX Firewall, but both firewall chassis must be identical in model number, interfaces, and amount of RAM. (Special fail-over bundles that allow the purchase of a second PIX at a reduced cost are available for the PIX 520 and PIX 515. The product numbers are PIX-515-FO-BUN and PIX-515-FO-BUN). The Cisco Secure PIX Firewalls as fail-over devices **will not operate** without one being a primary, fully-licensed PIX Firewall. The PIX 515 with restricted software (designated by an "R" in the software or bundle part number) does not support failover mode. PIX v5.0 enhances the fail-over feature available in previous versions with true stateful fail-over functionality.

This new Stateful Fail-over feature provides an enhanced mechanism for hardware and software redundancy by allowing two identical PIX Firewall units to serve the same functionality in case one fails in an unattended environment. Normally, one PIX Firewall is considered the Active unit while the other is the Standby unit. The Active unit actively performs normal network functions while the Standby unit only monitors, ready to take control should the Active unit fail.

CISCO SYSTEMS

The Stateful Fail-over feature was enhanced so that the stateful connection information is passed on to the Standby unit during a fail-over. Previously, the existing connections would be lost after a switchover because stateful connection information was not passed on to the Standby unit. As a result, client applications had to perform a new connect to restart communication. With the release of version 5.0(1) during a fail-over the active unit passes all stateful connection information to the Standby unit, thereby continuing connection with the client application.

Q. What additional performance enhancements does the Cisco Secure PIX Firewall series offer?

A. In contrast to traditional firewalls, the Cisco Secure PIX Firewall series offers dramatically enhanced performance through a major new feature called cut-through proxy. Whereas UNIX-based proxy servers can provide user authentication and maintain "state" (information about a packet's origin and destination) to offer good security, performance suffers because UNIX-based proxy servers inefficiently process all packets at the application layer of the Open System Interconnection (OSI) model. The PIX Firewall's cut-through proxy, on the other hand, challenges a user initially at the application layer, then authenticates against standard RADIUS or TACACS+ databases. After policy is checked, The Cisco Secure PIX Firewall shifts the session flow, and all traffic flows directly and quickly between the two parties while maintaining session state information. This cut-through capability is one of the reasons The Cisco Secure PIX Firewall performs dramatically faster than other firewall solutions. Cut-through proxy also contributes to a lower cost of ownership, because it enables organizations to leverage their existing network access server (NAS) databases based on TACACS+ or RADIUS. Doing so results in significant savings over proxy-based firewalls that may require organizations to maintain separate databases, thereby incurring additional installation and maintenance costs.

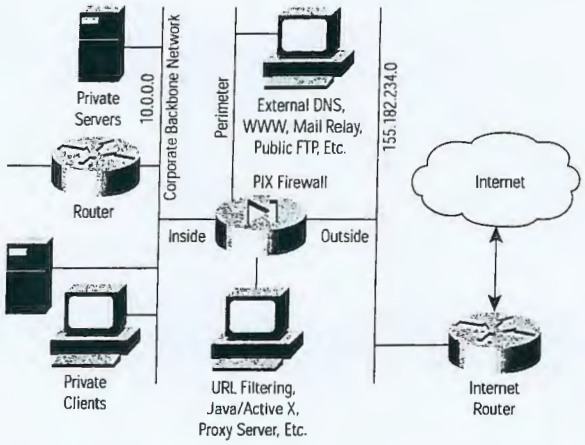
Q. How easy is the Cisco Secure PIX Firewall to use?

A. Extremely easy. The Cisco Secure PIX Firewall series includes the Firewall Manager—a Java-based, graphical configuration and management tool allowing The Cisco Secure PIX Firewall to be installed and configured with little network downtime. The Firewall Manager software also includes enhanced accounting and reporting tools that allow users to analyze and account for PIX Firewall activity. Users can generate reports for planning purposes or to charge back costs to various departments. In addition, The Cisco Secure PIX Firewall permits transparent support of Internet multimedia applications, which eliminates the need to physically modify and reconfigure each client workstation or PC—a tremendous administrative burden required by competing firewalls.

Q. What is the primary Cisco Secure PIX Firewall application?

A. As shown in Figure 1, the ideal application for The Cisco Secure PIX Firewall is in a multi-layered configuration—a configuration that is supported by most networking security experts and is endorsed in Cheswick and Bellovin's book *Firewalls and Internet Security*. The first line of defense is Cisco packet-filtering routers that use Cisco IOS® software and its access control lists to filter out undesired traffic. Routers are effective for many of the initial threats to the network. Sophisticated hackers, however, who could potentially penetrate routers, then encounter the second line of defense—The Cisco Secure PIX Firewall.

Figure 1 With four interfaces, the Cisco Secure PIX Firewall fully secures the internal network and allows publicly accessible servers to reside on separate, perimeter networks.



Q. How secure is the Cisco Secure PIX Firewall?

A. The Cisco Secure PIX Firewall offers one of the most secure options for high-level networks. The US National Security Agency-sponsored Trusted Technology Assessment Program (TTAP) recently awarded the PIX Firewall 520 (with version 4.3.1 PIX software) the highest security rating of any commercial firewall product (http://www.cisco.com/warp/public/779/gov/federal/TTAP/)

Independent tests conducted by SRI Consulting, a subsidiary of SRI International in Menlo Park, California, showed that the Cisco Secure PIX Firewall successfully resisted all tested security threats, even when subjected to extreme network traffic. The Cisco Secure PIX Firewall series has also been certified by the International Computer Security Association (ICSA), an independent, international organization based in Carlisle, Pennsylvania.

Q. Can the Cisco Secure PIX Firewall series be hacked using SATAN?

A. No. SATAN identifies certain known security problems within UNIX. Although UNIX is an ideal, open operating system for development, this openness inherently provides vulnerabilities for firewalls in areas of installation and maintenance. The Cisco Secure PIX Firewall runs a secure, real-time system that is not based on UNIX—a solution that makes the firewall, itself, secure while contributing significantly to its performance and reliability. (See security audit from SRI at http://www.cisco.com/go/pix)

Q. Which Internet applications can clients run on the protected LAN? How about multimedia?

A. The Cisco Secure PIX Firewall transparently supports all common TCP/IP Internet services, including Web, File Transfer Protocol (FTP), Telnet, Archie, Gopher, rlogin, and others. In addition, extensive multimedia data types are supported transparently, including RealNetworks RealAudio, Microsoft NetShow, VDOnet VDOLive, White Pines CuSeeMe, Intel ProShare, Xing Technologies Streamworks, and Vocal Tec Internet Phone. The Cisco Secure PIX Firewall also transparently supports videoconferencing applications that implement the H.323 standards such as Intel InternetVideo Phone and Microsoft NetMeeting. Because The Cisco Secure PIX Firewall transparently supports these multimedia applications—unlike proxy servers—organizations do not need to reconfigure each client workstation or PC, which dramatically reduces installation and maintenance costs.

Q. Can Oracle SQL*Net applications be used with the Cisco Secure PIX Firewall?

A. Yes. Cisco is the first to market transparent secure access for Oracle database users. Oracle client applications can successfully connect with database servers located on the internal network.

Q. Do you need additional hardware platforms in order to run the Cisco Secure PIX Firewall?

A. The Cisco Secure PIX Firewall itself is a turnkey hardware solution—a network appliance with embedded software, so no additional platforms are required. To add remote management or URL filtering services, though, would required a UNIX or Windows NT platform.

Q. Are there any special environmental considerations?

A. No. The Cisco Secure PIX Firewall operates in environments where 110-240 VAC is available, and a frequency of 50-60 Hz. It can be rack-mounted or placed freestanding. A new DC-powered version is also available.

Q. What network interfaces are supported?

A. The current PIX 520 product supports 10/100BaseT Ethernet, 4- to 6-Mbps Token Ring, and FDDI. These interfaces can be interchanged with mixed modes with Ethernet and Token Ring, but not FDDI. Currently, the PIX 515 product line only supports 10/100Base T Ethernet interfaces.

Q. How many network interface cards can be installed in one Cisco Secure PIX Firewall device?

A. The Cisco Secure PIX Firewall series now supports six interfaces (using the new four-port Ethernet cards). (See http://www.cisco.com/warp/customer/cc/cisco/mkt/security/pix/prodlit/pie_ds.htm for specifics on how many cards can be supported in one chassis.) These multiple interfaces allow separate networks for publicly accessible services such as Web, mail, and DNS servers, as well as separate network support for other servers such as Web-based and traditional EDI applications that link vendors and customers and are now more secure with a physically separate network.

Q. What is included in the initial purchase price?

A. The Cisco Secure PIX Firewall series' price structure was created based on the current order process. Customers can individually purchase the base PIX Firewall hardware platform, software license, network interface cards (NICs), and optional failover/hot standby cable as individual components. In addition, for IPSec users, a separate order must be made for a 3DES encryption license. Cisco also offers a full range of SMARTnet and onsite maintenance contracts for service on The Cisco Secure PIX Firewall series.

Q. Can I run my Web, TCP, or mail service on The Cisco Secure PIX Firewall?

A. No. To achieve the highest levels of security, reliability, and performance, a firewall should not run any applications. This wisdom is commonly accepted among security experts and is presented in greater depth in *Firewalls and Internet Security* by Cheswick and Bellovin. The publicly accessible, but secure, third interface in The Cisco Secure PIX Firewall series, often called the perimeter, is the ideal attachment point for servers dedicated to such functions.

Q. Why did Cisco choose to write its own real-time embedded system for the Cisco Secure PIX Firewall series?

A. Analogous to the pioneering breakthrough that took routing off of UNIX platforms and placed it onto dedicated routers, Cisco determined that general-purpose operating systems provide limited performance for firewalling. The tightly coded real-time operating system of The Cisco Secure PIX Firewall resulted in increased reliability, security, performance, scalability, and ease of installation and ongoing administration.

Q. What is Network Address Translation (NAT)?

A. NAT is a methodology that allows organizations with existing networks that want to access the Internet to resolve the problem of IP address depletion. Sites that do not yet possess NIC-registered IP addresses must acquire them, and if more than 254 clients are present or planned, the scarcity of Class B addresses becomes a serious issue. The Cisco Secure PIX Firewall eliminates concern and bureaucratic delay by dynamically mapping thousands of hidden internal addresses to a range of easy-to-get Class C addresses. At the opposite extreme, sites that already have registered IP addresses for clients on the internal LAN must hide those addresses from the Internet, lest hackers directly attack the clients. With client addresses hidden, users enjoy strong security. The Cisco Secure PIX Firewall gives LAN administrators complete freedom to expand Class A addressing, which is drawn from the Internet Assigned Numbers Authority's (IANA's) reserve pool (RFC 1597), within the organization without concern for addressing changes at the LAN/Internet interface.

Q. Do I have to turn on NAT for all addresses?

A. No. The Cisco Secure PIX Firewall can selectively or dynamically perform NAT. This scenario allows the administrator to use a mix of RFC 1597/1918 addresses or registered addresses.

Q. Is NAT unique to the Cisco Secure PIX Firewall series?

A. The concept of NAT is not unique to Cisco firewalls. NAT can't be patented and it is fully described in RFC 1631. What is unique is The Cisco Secure PIX Firewall series' implementation—a completely new design, the first in the industry, and to this day, the highest performing firewall in the industry. Cisco routers support NAT in Cisco IOS software version 11.2, ideal for branch offices that do not host public services.

Q. What are the main differences between Cisco IOS NAT and the NAT capability offered in the Cisco Secure PIX Firewall series?

A. The Cisco IOS NAT is designed for use on remote access routers for IP address simplification and conservation. This is a cost-effective firewalling/NAT solution ideal that is ideal for branch offices. The Cisco Secure PIX Firewall provides NAT and much more. The Cisco Secure PIX Firewall is a high-performance, standalone, special-purpose firewall that offers stateful security. To effectively use Cisco IOS NAT in the router for a primary NAT device, performance considerations dictate at least a Cisco 4700M router. At this price range, it makes more sense to use the Cisco Secure PIX Firewall because it provides added value as a dedicated firewall, especially with features such as cut-through proxies that provide state and authentication (RADIUS/TACACS+), but without the overhead of UNIX-based firewalls. The Cisco Secure PIX Firewall also provides the ability to select which internal hosts get "NATed." In addition, the Cisco Secure PIX Firewall series includes the Firewall Manager, a configuration and management tool, and cut-through proxies for Telnet, FTP, and HTTP authentication. The Cisco Secure PIX Firewall is essentially a firewall product with NAT capabilities, whereas the Cisco IOS NAT implementation is designed for addressing simplification and conservation.

Q. Does the Cisco Secure PIX Firewall support IPSec and VPN tunnels?

A. Yes. The PIX 5.0 now supports IPSec. The PIX implementation of the IPSec (IP Security) feature is based on the Cisco IOS IPSec implementation and provides seamless functionality with those IPSec-compliant products that already work with Cisco IOS IPSec, such as the Cisco Secure VPN Client.

IPSec provides a mechanism for secure data transmission, ensuring confidentiality, integrity, and authenticity of data communications across a public IP network. The Cisco Secure PIX Firewall IPSec implementation supports both data transmission through the Cisco Secure PIX Firewall for establishing a VPN and termination of IPSec traffic at The Cisco Secure PIX Firewall.

Q. Will the Cisco Secure PIX Firewall continue to support the propreitary "PrivateLink" connection feature?

A. No. Support for PrivateLink was discontinued with the release of v5.0. It will continue to be supported in versions of the PIX OS previous to 5.0 (v4.x and below), but all development efforts for the PrivateLink feature have been replaced with the IPSec VPN solution.

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

European Headquarters
Cisco Systems Europe s.a.r.l.
Parc Evolic, Batiment L1/L2
16 Avenue du Quebec
Villebon, BP 706
91961 Courtaboeuf Cedex
France
http://www-europe.cisco.com
Tel: 33 1 69 18 61 00
Fax: 33 1 69 28 83 26

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

Asia Headquarters
Nihon Cisco Systems K.K.
Fuji Building, 9th Floor
3-2-3 Marunouchi
Chiyoda-ku, Tokyo 100
Japan
http://www.cisco.com
Tel: 81 3 5219 6250
Fax: 81 3 5219 6001

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

Argentina • Australia • Austria • Belgium • Brazil • 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 • Singapore Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States

Comprovação das Especificações Exigidas no Edital 050/2003

6.2. Servidor de segurança lógica tipo 2

23/07/03

Servidor de Segurança Lógica Tipo 02	
mcpix_ds.pdf	CiscoWorks Management Center for Firewalls
pix2_ds.pdf	Cisco PIX 525 Security Appliance

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

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.

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

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

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+)

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

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)

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+

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

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

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

RD/LW3946 04/03

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.

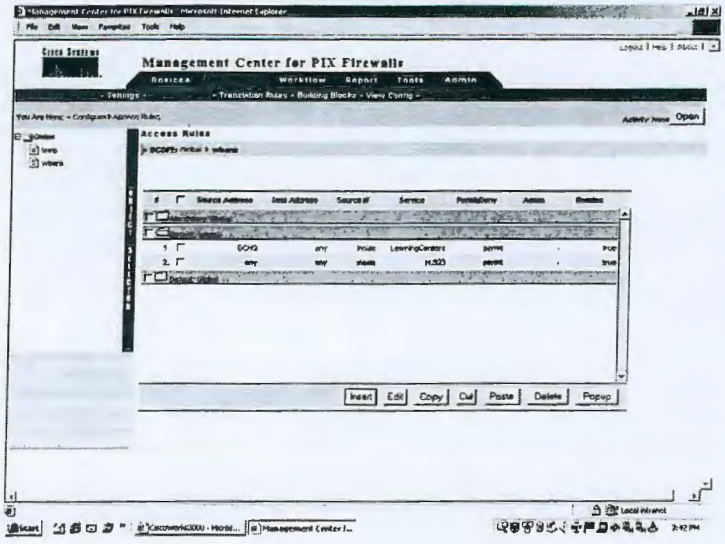
This management center component of CiscoWorks VMS, is an integral part of the SAFE blueprint, and combines Web-based tools for configuring, monitoring, and troubleshooting the following:

- 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 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

- 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

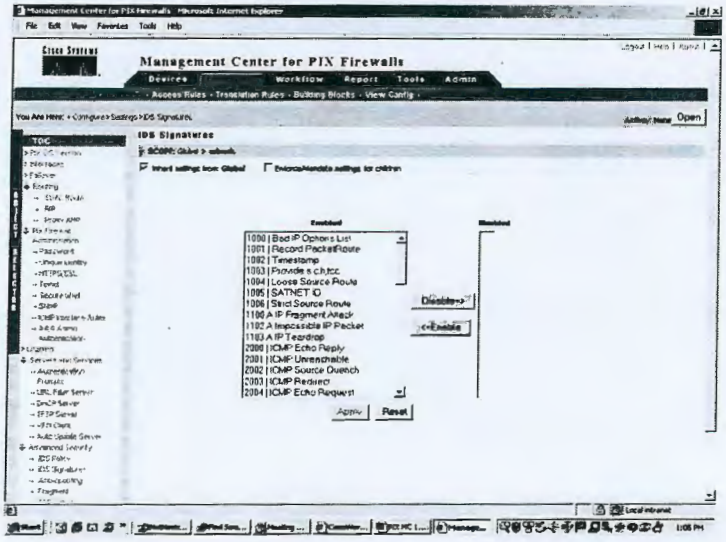
Smart Rules

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.

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.

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

2000170/ETMG 9/02

NEC

Comprovação das Especificações Exigidas no Edital 050/2003

6.3. Servidor para detecção de intrusão

23/07/03

Sistema de Detecção de Intrusão	
idsdp_rg.pdf	Cisco IOS Intrusion Detection Systems
vpids_qa.pdf	Cisco Intrusion Detection System
ids4f_ds.pdf	Cisco IDS 4200 Series Sensors
ch01.pdf	Overview
cwvpn_ov.pdf	CiscoWorks VPN/ Security Management Solution Version
ch02.pdf	VMS Bundle Component Installation
intro.pdf	Introducing the Cisco IDS Director
idssl_ds.pdf	Cisco IOS Intrusion Detection Systems Signature List
lrlot_ds.pdf	Cisco IDS 3.0 Sensor Software for Cisco 4200 Series Appliances
swchap5.pdf	IDS Device Manager Administration Tasks
ch07.pdf	Tuning Sensor Configurations
ccmigration_09186a008015e3ab.pdf	Installing and Using the Cisco Intrusion Detection System Device Manager and Event Viewer Version 4.0

Cisco Systems

CiscoWorks **VPN/Security Management** Solution Version 2.2

CiscoWorks VPN/Security Management Solution (VMS) is the flagship integrated security management solution from Cisco, and is an integral part of the SAFE Blueprint from Cisco for network security. CiscoWorks VMS protects the productivity and reduces operating costs for enterprises, by combining Web-based tools for configuring, monitoring, and troubleshooting enterprise VPNs, firewalls, and network and host-based intrusion detection systems (IDS). CiscoWorks VMS delivers the industry's first robust and scalable foundation and feature set that addresses the needs of small and large-scale VPN and security deployments.

Today's business challenges and resulting security deployments require more scalability than merely supporting a large number of devices. Many customers have limited staffing, yet are asked to manage a myriad of security devices. These customers must manage the security and network infrastructure; frequently update many remote devices; implement change control and auditing when multiple organizations are involved in defining and deploying policies; enhance security without adding more headcount; or roll out remote access VPNs to all employees and monitor the VPN service.

CiscoWorks VMS enables customers to deploy security infrastructures from a small to large environment, using the following multifaceted scalability features:

- Complete SAFE Blueprint Coverage

  To completely manage a SAFE environment, a network management solution must manage SAFE infrastructure components, support features based upon an appliance or Cisco IOS® Software, and support a range of management functions. CiscoWorks VMS is uniquely able to scale across SAFE Blueprint components, including firewalls, VPNs, and network- and host-based IDSs. CiscoWorks VMS also takes advantage of Cisco Secure Access Control Server (ACS) by using a common ACS logon. CiscoWorks VMS can manage a feature set through an appliance, for example, the Cisco PIX® Firewall, or through the Cisco IOS Software. Scalable management also involves more than configuring devices. CiscoWorks VMS provides the complete range of management with features to configure, monitor, and troubleshoot the network.
- Scalable Foundation

  CiscoWorks VMS implements a foundation with a consistent user experience, which makes it easier to scale management to many devices. CiscoWorks VMS provides users with a consistent GUI, workflow, ACS logon, roles definition, platforms, database

engine, installation, and more. An industry-leading feature of this foundation is the Auto Update feature, which allows numerous devices to be updated easily and quickly. Auto Update enables devices, even remote and dynamically addressed devices, to periodically "call home" to an update server and "pull" the most current security configurations or Cisco PIX operating system. Auto Update is required to effectively scale remote office firewall deployments across intermittent links or dynamic addresses. Prior policy updating methods relied on a "push" model. Although this model works for known devices, it does not work for remote devices with unknown addresses or devices that are not always active. Without Auto Update a more manual process is required to update each remote device. The Auto Update feature provides a dramatic scalability improvement for organizations that want to deploy devices with many remote and local locations. In addition to easier and faster policy updates, Auto Update also provides consistent policy deployments.

- Enterprise Operational Integration

  CiscoWorks VMS enables organizations to easily integrate management into their operations. One operational need is to replicate policies to multiple locations. The Smart Rules hierarchy addresses this need, by enabling administrators to define device groups and implement policy inheritance. For example, an administrator can define a device group for the New York sales office and deploy that same policy to all other sales offices quickly and consistently. The Command and Control Workflow feature provides change control and auditing, and is particularly important for customers who have separate groups for network and security operations. The solution includes processes for generating, approving, and deploying configurations. This can help security operations to define and approve new policies. Network operations can later deploy the new policies during their regular maintenance window. An audit of the changes can be maintained.

- Centralized Role-Based Access Control (RBAC)

  Role-based access control enables organizations to scale access privileges. CiscoWorks VMS conveniently uses a common ACS logon for users, administrators, devices, and applications. CiscoWorks VMS enables different groups to have different access rights across different devices and applications.

- Integrated Infrastructure Management

  Scalability requires that multiple components be managed, not just firewalls, but also VPNs, network- and host-based IDSs, routers, and switches. CiscoWorks VMS not only manages the security infrastructure, but also manages the network infrastructure. Customers benefit from being able to manage these components from one solution. Integrated monitoring is also required to see the larger picture. CiscoWorks VMS provides integrated monitoring of Cisco PIX and Cisco IOS syslogs, and events from network and host-based IDSs, along with event correlation.

CiscoWorks VMS Functions

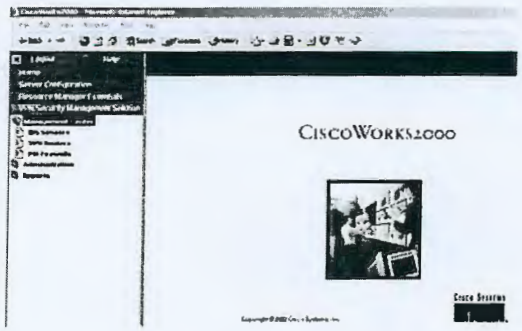
CiscoWorks VMS is launched from the CiscoWorks dashboard and is organized into several functional areas:

- Firewall management
- Auto Update Server
- IDS management, network and host-based
- VPN router management
- Security monitoring
- VPN monitoring
- Operational management

These functional areas supply multifaceted scalability by offering features such as a consistent user experience, auto update, command and control workflow, and role-based access control.

Figure 1 shows CiscoWorks VMS displayed as a "drawer" in the CiscoWorks dashboard.

Figure 1



Firewall Management

CiscoWorks VMS enables the large-scale deployment of Cisco PIX firewalls, by providing the following features:

- Smart Rules hierarchy and inheritance
- User-defined device and customer groups including nesting
- Global role-based access with administrative privileges per device and customer groups with other CiscoWorks products and Cisco Secure ACS
- Mandatory and default device settings inheritance
- Workflow deployment to device, directory, or Auto Update Server
- Look and feel of Cisco PIX Device Manager but with scalability to thousands of PIX firewalls
- Integration with other CiscoWorks network management software
- Complete SAFE Blueprint coverage for centralized management of Cisco PIX firewalls, including access control, VPN, IDS, and authentication, authorization, and accounting (AAA)

Smart Rules is an innovative feature that allows common information including access rules and settings to be inherited for all firewalls in a device or customer group. Smart Rules allows a user to define common rules once, which results in reduced configuration time, fewer administrative errors, and higher device scalability. Using Smart Rules, a user can configure a common rule such as allowing all HTTP traffic once and can apply this rule globally to all firewalls. Smart Rules can also be defined on a device or customer group basis. For specific information on the firewall management functionality of VMS, refer to: http://www.cisco.com/en/US/products/sw/cscowork/ps3992/index.html

Auto Update Server for Firewall Management

CiscoWorks VMS introduces the industry's first firewall Auto Update Server that allows users to implement a "pull" model for security and Cisco PIX operating system management. Auto Update Server permits remote firewall networks with unprecedented scalability. The Auto Update Server allows Cisco PIX firewalls to both periodically and automatically contact the update server for any security configuration, Cisco PIX Operating System, and PIX Device Manager (PDM) updates. The Auto Update Server supports the following features:

- Security management of remote Cisco PIX firewalls that use Dynamic Host Control Protocol (DHCP)
- Automated Cisco PIX OS distribution to groups of Cisco PIX firewalls
- Automated Cisco PDM updates to remote firewalls
- Configuration verification at periodic intervals
- Automated replacement of inaccurate or tampered configurations
- New firewalls configured at "boot time"

The Auto Update Server is an indispensable component of any large-scale remote Cisco PIX firewall deployment. Auto Update Server is an easy-to-use solution to automatically update all remote or local firewalls with new operating system releases. Cisco is the industry's first vendor to provide this pull model of security policy and operating system management. For specific information on the Auto Update Server component of VMS, refer to: http://www.cisco.com/en/US/products/sw/cscowork/ps3993/index.html

Network-Based IDS Management

Administrators can use CiscoWorks VMS to configure network and switch IDS sensors. Many sensors can be quickly configured using group profiles. Additionally, a more powerful signature management feature is included to increase the accuracy and specificity of detection. Some prominent features are:

- Easy-to-use Web-based interface
- Wizards that lead users through common management tasks
- Access to the Network Security Database (NSDB), which provides meaningful information about alarms for users without IDS security expertise
- Ability to define a hierarchy of sensors containing groups and subgroups, and the ability to configure multiple sensors concurrently using group profiles
- Support for several hundred sensor deployments from each console
- Use of a robust relational database to store a high volume of data

For specific information on the network-based IDS management functionality of VMS, refer to:

http://www.cisco.com/en/US/products/sw/cscowork/ps3990/index.html

Host-Based IDS Management

CiscoWorks VMS provides threat protection for server and desktop computing systems, also known as "endpoints." VMS goes beyond conventional endpoint security solutions by identifying and preventing malicious behavior before it can occur, thereby removing potential known and unknown security risks that threaten enterprise networks and applications. Because CiscoWorks VMS analyzes behavior rather than relying on signature matching, its solution provides robust protection with reduced operational costs. Features of host-based IDS management include:

- Aggregates and extends multiple endpoint security functions by providing host intrusion prevention, distributed firewall, malicious mobile code protection, operating system integrity assurance, and audit log consolidation all within a single agent.
- Provides preventive protection against entire classes of attacks including port scans, buffer overflows, Trojan horses, malformed packets, and e-mail worms.
- Offers "zero update" prevention for known and unknown attacks

- Provides industry-leading protection for UNIX and Windows servers and Windows desktops allowing customers to patch systems on their own schedules.
- Open and extensible architecture offers the capability to define and enforce security according to corporate policy.
- Scalable to thousands of agents per manager to support large enterprise deployments.

For specific information on the host-based IDS management functionality of VMS, refer to: the Management Center for Cisco Security Agents Datasheet.

VPN Router Management

CiscoWorks VMS includes functions for the setup and maintenance of large deployments of VPN connections and provides users with a point-and-click interface for setting up and deploying connections. This application is intended for scalable configuration of site-to-site VPN connections in a hub-and-spoke topology for centralized, multidevice configuration and deployment of Internet Key Exchange (IKE) and IP Security (IPsec) tunneling policies on VPN routers.

Major features include:

- Wizard-based interface for the creation of IKE and VPN tunneling policies.
- Hierarchical inheritance and Smart Rules hierarchy to reflect the organizational and common setup of devices and simplified device management
- IKE-KA (IKE Keepalive) or generic routing encapsulation (GRE) with Open Shortest Path First (OSPF) and Enhanced Interior Gateway Routing Protocol (EIGRP) for failover routing scenarios.
- Centralized role-based access control model allows for centralized management of users and accounts.

For specific information on the VPN router management functionality of VMS, refer to: http://www.cisco.com/en/US/products/sw/cscowork/ps3994/index.html

Security Monitoring

CiscoWorks VMS provides integrated monitoring to reduce the number of security monitoring consoles, reduce the number of events to monitor, and provide a broader view of security status.

- Integrated monitoring is used to capture, store, view, correlate, and report on events from many of the devices in the SAFE Blueprint such as Cisco network IDSs, switch IDSs, host IDSs, firewalls, and routers.
- Event correlation is used to identify attacks that are not easily recognizable from a single event. A flexible notification scheme and automated responses to critical events also aid in quick action.
- The event viewer can read both real-time and historical events.
- Events are color-coded and administrators can quickly isolate problems. Administrators can also define thresholds and time periods when rules can be triggered to provide notification.
- On-demand and scheduled reports facilitate ongoing monitoring.

For specific information on the security monitoring component of VMS, refer to: http://www.cisco.com/en/US/products/sw/cscowork/ps3991/index.html

VPN Monitoring

CiscoWorks VMS offers a Web-based management tool that allows network administrators to collect, store, and view information on IPsec VPN connections for remote-access or site-to-site VPN terminations. Multiple devices can be viewed from an easy-to-use dashboard that is configured using a Web browser. This dashboard provides the following capabilities:

- Provides data on system resources related to real-time memory usage, percent CPU usage per device, and active tunnel and active sessions. This data simplifies the identification of devices with potential performance problems and devices with the highest usage.
- Enables viewing of current and long-term packet rates and packet dropped percentage which can aid in determining where excess capacity can be tapped or quickly identify bottlenecks and device throughput problems.
- Enables identification of the devices with the most persistent problems through the event log; key device and VPN statistics are evaluated against a set of global and device-specific thresholds, and exceptions are recorded in the event log.
- Provides graphing of important common metrics. Device performance comparisons provide a global view of short-term trends in VPN performance, enabling administrators to identify problem areas before they become critical failures.

For specific information on the VPN monitoring component of VMS, refer to: http://www.cisco.com/en/US/products/sw/cscowork/ps2326/index.html

Operational Management

CiscoWorks VMS provides the operational management for the network, allowing network managers to perform the following:

- Quickly build a complete network inventory
- Manage device credentials information
- Monitor and report on hardware, software, configuration, and inventory changes
- Manage and deploy configuration changes and software image updates to multiple devices
- Monitor and troubleshoot critical LAN and WAN resources
- Quickly identify devices that can be used for VPNs, if upgraded with the appropriate Cisco IOS Software
- Discover which VPN devices have hardware encryption modules
- Graphically compare configurations of VPN devices
- Isolate IPsec-related problems by running customized Syslog reports

For specific information on the operational management functionality of VMS, refer to: http://www.cisco.com/en/US/products/sw/cscowork/ps2073/index.html

Server Specifications (Minimum requirements)

Server Hardware

- PC-compatible computer with 1 GHz or faster Pentium processor
- Sun UltraSPARC 60 MP with 440 MHz or faster processor
- Sun UltraSPARCIII (Sun Blade 2000 Workstation or Sun Fire 280R Workgroup Server)

- CD-ROM drive
- 100BASE-T or faster connection
- 1 GB RAM
- 9 GB available disk drive space
- 2 GB virtual memory
- Color monitor with video card capable of 16-bit color

Server Operating System

CiscoWorks VMS requires the following operating systems:

- Windows 2000 Professional, Server, and Advanced Server (Service Pack 3)

Note: Support for Advanced Server requires that Terminal Services be turned off.

Sun Solaris 2.8 with patches:

109742 has been replaced by 108528-13

109322 has been replaced by 108827-15

109279 has been replaced by 108528-13

108991 has been replaced by 108827-15

Java Requirements

Sun Java plug-in 1.3.1-b24

Client Requirements

Hardware

- PC-compatible computer with 300 MHz or faster Pentium processor
- Solaris SPARCstation or Sun Ultra 10

Client Operating System

- Windows 2000 Server or Professional Edition with Service Pack 3, or Windows XP SP1 with Microsoft VM.
- Solaris 2.8

Client Browser

- Internet Explorer 6.0 Service Pack 1, on Windows operating systems
- Netscape Navigator 4.79, on Windows 2000 Server or Professional Edition with Service Pack 3, or Windows XP; Netscape Navigator 4.76 on Solaris 2.8

The CiscoWorks Management Center for Firewalls, and CiscoWorks Management Center for VPN Routers, are supported on Internet Explorer 6.0, but not on Netscape Navigator. In addition to supporting Internet Explorer The Management Center for IDS and the Monitoring Center for Security are also supported on Netscape Navigator.

Service and Support

CiscoWorks products are eligible for coverage under the Cisco Software Application Service (SAS) program. This service program offers customers contract-based 24-hour access to the Cisco Technical Assistance Center (TAC), full Cisco.com privileges, and software maintenance updates. A SAS contract ensures that customers have easy access to the information and services needed to stay current with newly supported device packages, patches, and minor updates. For further information about service and support offerings, contact your local sales office.

Ordering Information

CiscoWorks VMS is available for purchase through regular Cisco sales and distribution channels worldwide. CiscoWorks VMS includes all the necessary components needed for an independent installation on a Microsoft Windows or Sun Solaris workstation.

For More Information

For more information, go to http://www.cisco.com/warp/public/cc/pd/wr2k/vpmnso/prodlit/ or send e-mail to ciscoworks@cisco.com

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

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

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

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

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

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

203031/ETMG/04/03

Cisco Systems

Data Sheet

Cisco **IDS 4200** Series Sensors

Cisco integrated network security solutions enable organizations to protect productivity gains and reduce operating costs.

The Cisco IDS 4200 Series sensors are used in the Cisco Intrusion Protection System. These intrusion detection system sensors work in concert with the other components to efficiently protect your data and information infrastructure. With the increased complexity of security threats, achieving efficient network intrusion security solutions is critical to maintaining a high level of protection. Vigilant protection ensures business continuity and minimizes the effect of costly intrusions.

Additionally, Cisco's flexible deployment options allow businesses to minimize the total cost of ownership of their IDS deployments by delivering:

- unprecedented price/performance ratios
- the ability to simultaneously protect multiple network subnets through the support for multiple sniffing interfaces, thereby delivering up to five sensors in one
- a wide array of performance options
- investment protection by delivering modular, upgradable components
- support for multi-VLAN traffic
- embedded web-based management solutions packaged with the IDS sensors

Please refer to Table 1 for information on the characteristics of the Cisco IDS 4200 Series Sensors.

For details on the complete Cisco Intrusion Protection System, go to http://www.cisco.com/go/ids.

Deploying the Cisco IDS 4200 Series Sensors

The Cisco IDS 4200 Series includes four products: the Cisco IDS 4215, IDS 4235, IDS 4250 and IDS 4250-XL sensors. The Cisco IDS product line delivers a broad range of solutions that allow easy integration into many different environments, including enterprise and service provider environments. Each sensor addresses the bandwidth requirements at one of several speeds, from 80 Mbps to gigabits per second.

The Cisco IDS 4215 can monitor up to 80 Mbps of traffic and is suitable for T1/E1 and T3 environments. Additionally, multiple sniffing interfaces are supported on the IDS-4215 which allow the ability to simultaneously protect multiple subnets, thereby delivering five sensors in a single unit.

At 250 Mbps, the Cisco IDS 4235 can be deployed to provide protection in switched environments, on multiple T3 subnets, and with the support of 10/100/1000 interfaces it can also be deployed on partially utilized gigabit links.

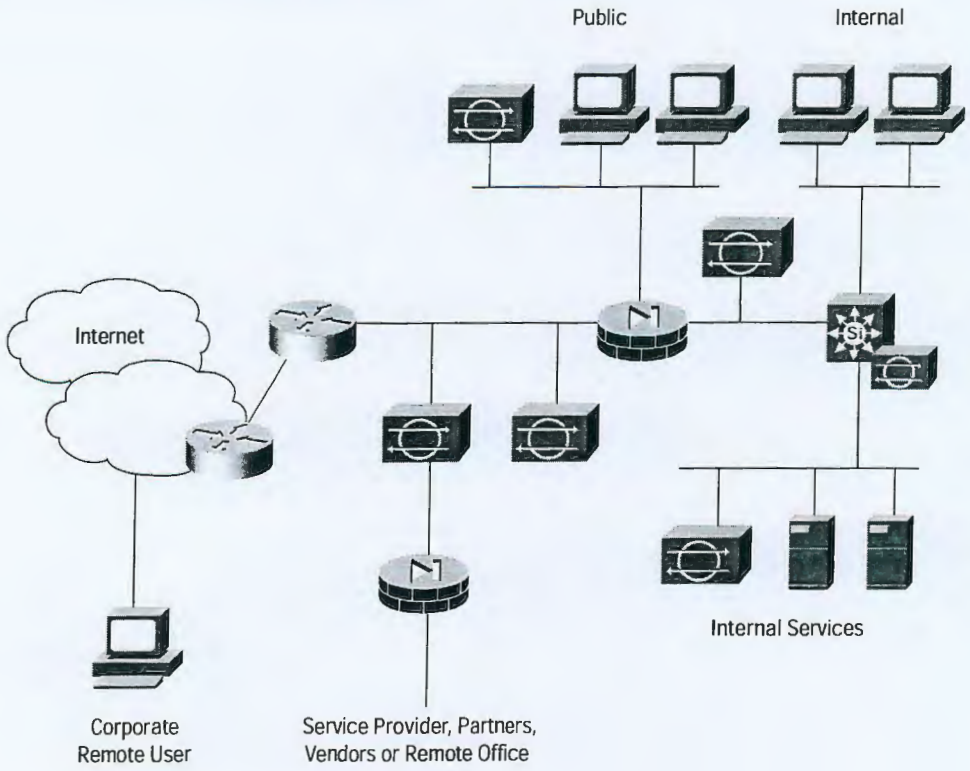
The Cisco IDS 4250 supports a 500 Mbps speed and can be used to protect gigabit subnets and traffic traversing switches that are being used to aggregate traffic from numerous subnets. In addition, the Cisco IDS 4250 provides the flexibility to accommodate a simple hardware upgrade to scale to full line-rate gigabit performance.

At 1 Gbps, the Cisco IDS 4250-XL provides unprecedented performance by providing customized hardware acceleration to protect fully-saturated gigabit links as well as multiple partially-utilized gigabit subnets.

As shown in Figure 1, sensors can be placed on almost any network segment of the enterprise-wide network where security visibility is required.

Please refer to Table 2 for ordering information for the Cisco IDS 4200 Series Sensors.

Figure 1
Deployment Scenarios for the 4200 Series Appliance Sensors



Product Specifications

Table 1 Characteristics of Cisco IDS 4215, 4235, 4250, and 4250-XL Sensors

	Cisco IDS 4215	Cisco IDS 4235	Cisco IDS 4250	Cisco IDS 4250-XL
				
Performance	80 Mbps	250 Mbps	500 Mbps	1000 Mbps
Standard monitoring interface	10/100BASE-Tx	10/100/1000BASE-TX	10/100/1000BASE-TX	Dual 1000BASE-SX interface with MTRJ
Standard command and control interface	10/100BASE-Tx	10/100/1000BASE-TX	10/100/1000BASE-TX	10/100/1000BASE-TX
Optional interface	Four 10/100BaseTx (4FE) sniffing interfaces (allowing a total of 5 sniffing interfaces).	Four 10/100BaseTx (4FE) sniffing interfaces (allowing a total of 5 sniffing interfaces).	-1000BASE-SX (fiber) -Four 10/100BaseTx (4FE) sniffing interfaces (allowing a total of 5 sniffing interfaces).	1000BASE-SX (fiber)
Performance upgradable	No	No	Yes	No
Form factor	One rack unit	One rack unit	One rack unit	One rack unit
Advanced protection algorithms				
Stateful pattern recognition	Yes	Yes	Yes	Yes
Protocol parsing	Yes	Yes	Yes	Yes
Heuristic detection	Yes	Yes	Yes	Yes
Anomaly detection	Yes	Yes	Yes	Yes
Attack protection				
Sweeps or floods	Yes	Yes	Yes	Yes
Denial-of-service (DoS) mitigation	Yes	Yes	Yes	Yes
Worms or viruses	Yes	Yes	Yes	Yes
Common gateway interface (CGI) or WWW attacks	Yes	Yes	Yes	Yes
Buffer overflow protection	Yes	Yes	Yes	Yes

Table 1 Characteristics of Cisco IDS 4215, 4235, 4250, and 4250-XL Sensors

	Cisco IDS 4215	Cisco IDS 4235	Cisco IDS 4250	Cisco IDS 4250-XL
Remote-procedure call (RPC) attack detection	Yes	Yes	Yes	Yes
IP fragmentation attacks	Yes	Yes	Yes	Yes
Internet Control Message Protocol (ICMP) attacks	Yes	Yes	Yes	Yes
Simple Message Transfer Protocol (SMTP), Sendmail, Internet Message Access Protocol (IMAP), or Post Office Protocol (POP) attacks	Yes	Yes	Yes	Yes
File Transfer Protocol (FTP), Secure Shell Protocol (SSH), Telnet, and rlogin attacks	Yes	Yes	Yes	Yes
Domain Name System (DNS) attacks	Yes	Yes	Yes	Yes
TCP hijacks	Yes	Yes	Yes	Yes
Windows or NetBios attacks	Yes	Yes	Yes	Yes
TCP application protection	Yes	Yes	Yes	Yes
BackOrifice attacks	Yes	Yes	Yes	Yes
Network Timing Protocol (NTP) attacks	Yes	Yes	Yes	Yes
Customizable signatures using Signature Micro-Engine technology	Yes	Yes	Yes	Yes
Automated signature updates	Yes	Yes	Yes	Yes

Table 1 Characteristics of Cisco IDS 4215, 4235, 4250, and 4250-XL Sensors

	Cisco IDS 4215	Cisco IDS 4235	Cisco IDS 4250	Cisco IDS 4250-XL
Alarm summarization	Yes	Yes	Yes	Yes
Support for 802.1q traffic	Yes	Yes	Yes	Yes
P2P / file sharing detection techniques	Yes	Yes	Yes	Yes
Secure communication				
IP Security (IPSec) or Secure Sockets Layer (SSL) between sensor and management console	Yes	Yes	Yes	Yes
Encrypted signature packages	Yes	Yes	Yes	Yes
SSH for remote administration	Yes	Yes	Yes	Yes
Serial Control Protocol (SCP) support for secure file transfer	Yes	Yes	Yes	Yes
IDS evasion protection				
IP fragmentation re-assembly	Yes	Yes	Yes	Yes
TCP stream re-assembly	Yes	Yes	Yes	Yes
Unicode deobfuscation	Yes	Yes	Yes	Yes
Active response actions				
Router access-control-list (ACL) modifications	Yes	Yes	Yes	Yes
Firewall policy modifications	Yes	Yes	Yes	Yes
Switch ACL modifications	Yes	Yes	Yes	Yes
Session termination via TCP resets	Yes	Yes	Yes	Yes
IP session logging or session replay	Yes	Yes	Yes	Yes

Table 1 Characteristics of Cisco IDS 4215, 4235, 4250, and 4250-XL Sensors

	Cisco IDS 4215	Cisco IDS 4235	Cisco IDS 4250	Cisco IDS 4250-XL
Active notification actions				
Alarm display	Yes	Yes	Yes	Yes
E-mail alerts	Yes	Yes	Yes	Yes
E-page alerts	Yes	Yes	Yes	Yes
Customizable script execution	Yes	Yes	Yes	Yes
Multiple alarm destinations	Yes	Yes	Yes	Yes
Third-party tool integration	Yes	Yes	Yes	Yes
IDS active update bulletins	Yes	Yes	Yes	Yes
Administration				
Web user interface (Secure Hypertext Transfer Protocol [HTTPS])	Yes	Yes	Yes	Yes
Command-line interface (CLI) (console)	Yes	Yes	Yes	Yes
CLI (Telnet or SSH)	Yes	Yes	Yes	Yes
CiscoWorks VPN Security Management Solution (VMS) support	Yes	Yes	Yes	Yes
High availability				
Redundant power supply	No	Yes	Yes	Yes
Failure detection				
Monitoring link failure detection	Yes	Yes	Yes	Yes
Communications failure detection	Yes	Yes	Yes	Yes
Services failure detection	Yes	Yes	Yes	Yes
Device failure detection	Yes	Yes	Yes	Yes
Dimensions				

Table 1 Characteristics of Cisco IDS 4215, 4235, 4250, and 4250-XL Sensors

	Cisco IDS 4215	Cisco IDS 4235	Cisco IDS 4250	Cisco IDS 4250-XL
Height	1.7 in. (4.37 cm)	1.67 in. (4.24 cm)	1.67 in. (4.24 cm)	1.67 in. (4.24 cm)
Width	16.8 in. (42.72 cm)	17.6 in. (44.70 cm)	17.6 in. (44.70 cm)	17.6 in. (44.70 cm)
Depth	11.8 in. (29.97 cm)	27.0 in. (68.58 cm)	27.0 in. (68.58 cm)	27.0 in. (68.58 cm)
Weight	11.5 lb (4.11 kg)	35 lb (15.88 kg)	35 lb (15.88 kg)	35 lb (15.88 kg)
Rack-mountable	Yes	Yes	Yes	Yes
Power				
Autoswitching	100V to 240V AC	110–220 VAC	110–220 VAC	110–220 VAC
Frequency	50 to 60 Hz	50–60 Hz	50–60 Hz	50–60 Hz
Operating current	1.5A	2.7A at 115V 1.3A at 220V	2.7A at 115V 1.3A at 220V	2.7A at 115V 1.3A at 220V
Operating environment				
Operating temperature	+5°C to +40°C (+41°F to +104°F)	10 to 35°C (50 to 95°F)	10 to 35°C (50 to 95°F)	10 to 35°C (50 to 95°F)
Nonoperating temperature	-25°C to +701/4°C (–13F to +1581/4°F)	–40 to 65°C (–40 to 149°F)	–40 to 65°C (–40 to 149°F)	–40 to 65°C (–40 to 149°F)
Operating relative humidity	5 to 95% (noncondensing)	8 to 80% (noncondensing)	8 to 80% (noncondensing)	8 to 80% (noncondensing)
Nonoperating relative humidity	5 to 95% (noncondensing)	5 to 95% (noncondensing)	5 to 95% (noncondensing)	5 to 95% (noncondensing)
Heat dissipation (most severe case with full power usage)	410 Btu/hr (full power usage (65W))	983 Btu/hr (maximum)	983 Btu/hr (maximum)	983 Btu/hr (maximum)

Note:

- This 80-Mbps performance for the Cisco IDS 4215 is based on the following conditions:
  - 800 new TCP connections per second
  - 800 HTTP transactions per second
  - Average packet size of 445 bytes,
  - Running Cisco IDS 4.0 Sensor Software
- This 250-Mbps performance for the Cisco IDS 4235 is based on the following conditions:
  - 3000 new TCP connections per second
  - 3000 HTTP transactions per second
  - Average packet size of 445 bytes

- Running Cisco IDS 4.0 Sensor Software

- This 500-Mbps performance for the Cisco IDS 4250 is based on the following conditions:
  - 5000 new TCP connections per second
  - 5000 HTTP transactions per second
  - Average packet size of 445 bytes
  - Running Cisco IDS 4.1 Sensor Software
- This 1000-Mbps performance for the Cisco IDS 4250-XL is based on the following conditions:
  - 5000 new TCP connections per second
  - 5000 HTTP transactions per second
  - Average packet size of 595 bytes
  - Running Cisco IDS 4.0 Sensor Software

Regulatory Compliance

- EMC—FCC (CFR 47 Part 15) Class A, CISPR 22 Class A, EN 55022 Class A, EN 55024, EN61000-3-2, EN61000-3-3, VCCI Class A, AS/NZS 3548 Class A, CE marking
- Safety UL 60950, CSA 22.2 No.60950, IEC 60950, EN 60950, AS/NZS 3260, CE marking.

Table 2 Ordering Information for the Cisco IDS 4200 Series Sensor

Product number	Product description
IDS-4215-K9	Cisco IDS 4215 Sensor (chassis, software, SSH, 2 onboard 10/100BASE-Tx interfaces with RJ-45 connector), 80-Mbps
IDS-4215-4FE-K9	Cisco IDS 4215 Sensor (chassis, software, SSH, 2 onboard 10/100BASE-Tx interfaces with RJ-45 connector plus 4FE interface card), 80-Mbps
IDS-4235-K9	Cisco IDS 4235 Sensor (chassis, software, SSH, 10/100/1000BASE-T with RJ-45 connector)
IDS-4250-TX-K9	Cisco IDS 4250 Sensor (chassis, software, SSH, 10/100/1000BASE-T with RJ-45 connector)
IDS-4250-SX-K9	Cisco IDS 4250 Sensor (chassis, software, SSH, 1000BASE-SX with SC connector)
IDS-4250-XL-K9	Cisco IDS 4250-XL Sensor (chassis, software, SSH, hardware accelerator, with dual 1000BASE-SX and MTRJ connectors)
IDS-XL-INT=	Cisco IDS Accelerator Card with dual 1000BASE-SX interfaces and MTRJ connectors
IDS-4250-SX-INT=	1000BASE-SX monitoring interface with SC connector
IDS-4FE-INT=	Spare 4FE (10/100 BaseTx) sniffing interfaces for 4215, 4235, & 4250
IDS-PWR=	Spare power supply for the Cisco IDS 4235 and 4250 sensors
IDS-SCSI=	Spare Small Computer Systems Interface (SCSI) hard disk drive for Cisco IDS 4250 Sensor
IDS-RAIL-2=	Two post rail kits for the Cisco IDS 4235 and 4250 sensor platforms
IDS-RAIL-4=	Four post rail kits for the Cisco IDS 4235 and 4250 sensor platforms

Table 2 Ordering Information for the Cisco IDS 4200 Series Sensor

Product number	Product description
CON-SNT-IDS4215XK	Cisco SMARTnet support 8 x 5 x NBD (Cisco IDS 4215-K9)
CON-SNTE-IDS4215XK	Cisco SMARTnet support 8 x 5 x 4 (Cisco IDS 4215-K9)
CON-SNTP-IDS4215XK	Cisco SMARTnet support 24 x 7 x 4 (Cisco IDS 4215-K9)
CON-OS-IDS4215XK	Cisco SMARTnet Onsite support 8 x 5 x NBD (Cisco IDS 4215-K9)
CON-OSE-IDS4215XK	Cisco SMARTnet Onsite support 8 x 5 x 4 (Cisco IDS 4215-K9)
CON-OSP-IDS4215XK	Cisco SMARTnet Onsite support 24 x 7 x 4 (Cisco IDS 4215-K9)
CON-SNT-IDS4215-4FEXK	Cisco SMARTnet support 8 x 5 x NBD (Cisco IDS 4215-4FE-K9)
CON-SNTE-IDS4215-4FEXK	Cisco SMARTnet support 8 x 5 x 4 (Cisco IDS 4215-4FE-K9)
CON-SNTP-IDS4215-4FEXK	Cisco SMARTnet support 24 x 7 x 4 (Cisco IDS 4215-4FE-K9)
CON-OS-IDS4215-4FEXK	Cisco SMARTnet Onsite support 8 x 5 x NBD (Cisco IDS 4215-4FE-K9)
CON-OSE-IDS4215-4FEXK	Cisco SMARTnet Onsite support 8 x 5 x 4 (Cisco IDS 4215-4FE-K9)
CON-OSP-IDS4215-4FEXK	Cisco SMARTnet Onsite support 24 x 7 x 4 (Cisco IDS 4215-4FE-K9)
CON-SNT-IDS4235K9	Cisco SMARTnet support 8 x 5 x NBD (Cisco IDS 4235)
CON-SNTE-IDS4235K9	Cisco SMARTnet support 8 x 5 x 4 (Cisco IDS 4235)
CON-SNTP-IDS4235K9	Cisco SMARTnet support 24 x 7 x 4 (Cisco IDS 4235)
CON-OS-IDS4235K9	Cisco SMARTnet onsite support 8 x 5 x NBD (Cisco IDS 4235)
CON-OSE-IDS4235K9	Cisco SMARTnet onsite support 8 x 5 x 4 (Cisco IDS 4235)
CON-OSP-IDS4235K9	Cisco SMARTnet onsite support 24 x 7 x 4 (Cisco IDS 4235)
CON-SNT-IDS4250TK	Cisco SMARTnet support 8 x 5 x NBD (Cisco IDS 4250-TX)
CON-SNTE-IDS4250TK	Cisco SMARTnet support 8 x 5 x 4 (Cisco IDS 4250-TX)
CON-SNTP-IDS4250T	Cisco SMARTnet support 24 x 7 x 4 (Cisco IDS 4250-TX)
CON-OS-IDS4250TK	Cisco SMARTnet onsite support 8 x 5 x NBD (Cisco IDS 4250-TX)
CON-OSE-IDS4250TK	Cisco SMARTnet onsite support 8 x 5 x 4 Cisco (IDS 4250-TX)
CON-OSP-IDS4250TK	Cisco SMARTnet onsite support 24 x 7 x 4 (Cisco IDS 4250-TX)
CON-SNT-IDS4250SK	Cisco SMARTnet support 8 x 5 x NBD Cisco (IDS 4250-SX)
CON-SNTE-IDS4250SK	Cisco SMARTnet support 8 x 5 x 4 (Cisco IDS 4250-SX)
CON-SNTP-IDS4250SK	Cisco SMARTnet support 24 x 7 x 4 (Cisco IDS 4250-SX)
CON-OS-IDS4250SK	Cisco SMARTnet onsite support 8 x 5 x NBD (Cisco IDS 4250-SX)
CON-OSE-IDS4250SK	Cisco SMARTnet onsite support 8 x 5 x 4 (Cisco IDS 4250-SX)
CON-OSP-IDS4250SK	Cisco SMARTnet onsite support 24 x 7 x 4 (Cisco IDS 4250-SX)
CON-SNT-IDS4250XK	Cisco SMARTnet support 8 x 5 x NBD Cisco (IDS 4250-XL)
CON-SNTE-IDS4250XK	Cisco SMARTnet support 8 x 5 x 4 (Cisco IDS 4250-XL)
CON-SNTP-IDS4250XK	Cisco SMARTnet support 24 x 7 x 4 (Cisco IDS 4250-XL)
CON-OS-IDS4250XK	Cisco SMARTnet onsite support 8 x 5 x NBD (Cisco IDS 4250-XL)
CON-OSE-IDS4250XK	Cisco SMARTnet onsite support 8 x 5 x 4 (Cisco IDS 4250-XL)
CON-OSP-IDS4250XK	Cisco SMARTnet onsite support 24 x 7 x 4 (Cisco IDS 4250-XL)

Table 2 Ordering Information for the Cisco IDS 4200 Series Sensor

Product number	Product description
CON-SNT-IDS4FE	Cisco SMARTnet support 8 x 5 x NBD (IDS-4FE-INT=)
CON-SNTE-IDS4FE	Cisco SMARTnet support 8 x 5 x 4 (IDS-4FE-INT=)
CON-SNTP-IDS4FE	Cisco SMARTnet support 24 x 7 x 4 (IDS-4FE-INT=)
CON-OS-IDS4FE	Cisco SMARTnet onsite support 8 x 5 x NBD (IDS-4FE-INT=)
CON-OSE-IDS4FE	SMARTnet onsite support 8 x 5 x 4 (IDS-4FE-INT=)
CON-OSP-IDS4FE	SMARTnet onsite support 24 x 7 x 4 (IDS-4FE-INT=)
CON-SNT-IDSXL	Cisco SMARTnet support 8 x 5 x NBD (IDS-XL-INT=)
CON-SNTE-IDSXL	Cisco SMARTnet support 8 x 5 x 4 (IDS-XL-INT=)
CON-SNTP-IDSXL	Cisco SMARTnet support 24 x 7 x 4 (IDS-XL-INT=)
CON-OS-IDSXL	Cisco SMARTnet onsite support 8 x 5 x NBD (IDS-XL-INT=)
CON-OSE-IDSXL	SMARTnet onsite support 8 x 5 x 4 (IDS-XL-INT=)
CON-OSP-IDSXL	SMARTnet onsite support 24 x 7 x 4 (IDS-XL-INT=)

Export Considerations

The Cisco IDS 4200 Series sensors are subject to export controls. Refer to the export compliance Web site for guidance at: http://www.cisco.com/wwl/export/crypto/.

For specific export questions, contact export@cisco.com.

Additional Information

For more information about the Cisco Intrusion Protection System, go to: http://www.cisco.com/go/ids

For more information about the CiscoWorks VMS Solutions (IDS management), go to: http://www.cisco.com/go/vms

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

RD/LW4599 0503

DATA SHEET

Cisco **IDS 3.0** Sensor Software for Cisco 4200 Series Appliances

The industry-leading Cisco IDS Intrusion Detection System solution provides customers with unmatched intrusion protection technology through the Cisco Active Defense System. The integrated hardware and software solution delivers best-of-breed protection for both perimeter and internal resources.

Version 3.0 is the latest release of the Cisco IDS application software for the Cisco 4200 Series appliances. It delivers the latest in innovative IDS features, including Active Update signature distribution mechanisms, customizable signature language, extensions to the Active Response capabilities, and secure administration.

Key Features and Benefits

Signature Definition and Distribution Enhancements

Active Update Mechanism

Cisco IDS now provides a facility to automatically distribute new signature files and application upgrades to sensors without operator involvement. Utilizing a secure staging technique, new signature files are placed on a central server and passed to the sensor at scheduled intervals. After verifying the integrity of the package, the sensor automatically installs the update. This new capability significantly streamlines the process of regularly updating remote sensors, thereby lowering the recurring operational costs associated with this task. Additionally, users can subscribe to Cisco Active Update notification services to stay informed about breaking vulnerability news and posted countermeasures.

Signature Instruction Language for Verifying Exploits and Reconnaissance (SILVER)

Cisco IDS continues to innovate with the release of the Cisco SILVER signature language. Users can now develop custom signatures spanning Layer 2 through Layer 7 attributes. Developed by the Cisco Countermeasures Research Team, SILVER is the mechanism that this team uses to develop all new signatures for the IDS product. Now Cisco is exposing this capability to its customers, providing them unparalleled flexibility to develop new signatures.

This new language also decreases the time between signature releases because the signatures can be released as update files rather than compiled in the core sensor binary. Similar to antivirus products, the signature engines and the data files can be released separately.

Tunable Signatures

One of the challenges of event monitoring for IDS is to reduce the occurrence of false positives, thereby allowing the user to focus only on alarms that are deemed security relevant. However, because the security objectives for each IDS deployment are unique, Cisco IDS 3.0 adds granularity to the way in which sensors may be tuned to specifically suit the environment in which they are deployed. Users may now tune signature threshold parameters to meet their unique security objectives. For example, for the ping sweep signature, the user can now define the number of hosts pinged before the signature fires.

Alarm Summarization

Attackers may use tools such as Stick to cause sensors to send numerous alarms to management consoles as a way of flooding the management console. The Alarm Throttle feature in Cisco IDS 3.0 allows users to consolidate alarms to a single event, thereby preventing the management console from being overwhelmed with numerous events. For example, if the rate of alarms being sent by the sensor exceeds a certain threshold value, the signature may be set to automatically throttle to a summarization mode to produce a single alarm that comprises numerous alarm firings. A time interval may also be specified that determines the rate at which subsequent consolidated alarms are sent to the management console.

Detection of Network DoS Attacks

Cisco IDS 3.0 adds functionality to detect network denial-of-service (DoS) attacks that are targeted at consuming network resources. An inspector monitors the data capture by maintaining a counter that tracks the number of packets being captured per second. If the rate of packets being captured exceeds a specified rate and such peaks occur at a certain frequency, an alarm is generated to alert the user of a possible DoS attempt.

Active Response Extensions

Shunning with the Cisco PIX Firewall and Cisco Catalyst Switches

Cisco IDS incorporates proactive response functionality into the sensor appliances by allowing users to configure the IDS to dynamically respond to an attacking host by preventing new connections and disallowing packets from any existing connection. Cisco IDS 3.0 extends this Active Response capability beyond Cisco routers into a wide range of Cisco's high-performance networking devices, including the Cisco PIX® Firewall (running PIX 6.0+), Cisco Catalyst® 6000 Switch, and Cisco Catalyst 5000 Switch. This shunning gives security operators unparalleled control to reach across the network to quickly stop misuse and end intruders' access to the network.

Interoperability with Existing ACLs

Shunning is accomplished by the dynamic modification of access control lists (ACLs) on managed devices. Cisco IDS 3.0 allows the user to configure the sensor to shun while maintaining any user-defined access control entries on the specified interface and direction.

Secure Administration

In addition to existing functionality that provides secure communications between the sensor and the management console using IP Security (IPSec), Cisco IDS 3.0 also supports the Secure Shell Protocol (SSH) to allow users to remotely access sensors over a secure connection.

IP Session Replay

IP session logging provides extensive logging that is important for system troubleshooting as well as for reconstructing system events before and after attacks. Cisco IDS 3.0 augments this existing capability by converting these logs to a standard TCP dump format that allows them to be viewed and replayed using public domain utilities, such as Ethereal and TCPReplay.

Enhanced Filtering

Users have the ability to specify which source or destination IP addresses that specified signatures must alarm on. Because certain signatures may be classified as security relevant for certain source or destination IP addresses and yet do not need to be analyzed for other IP addresses, this level of enhanced filtering minimizes the occurrence of false positives.

Alarm Generation When Sniffing Interface is Disconnected

Sensors are equipped with a monitoring interface for data packet capture and a command and control interface for transmitting alarms to the management console and receiving configuration information from the

management console. With Cisco IDS 3.0, when the sniffing interface is disconnected, an alarm is triggered. This setup provides the user with an alert mechanism when the interface is tampered with and hence assures persistent operation.

Technical Specifications

Ordering Information

SMARTnet™ customers may download Cisco IDS 3.0 from Software Center on CCO at http://www.cisco.com

Part number for IDS Software Upgrade for Non-Support Customers: IDS-SW-U

Export Considerations

IDS sensors are subject to export controls. Please refer to the export compliance Web site at

http://www.cisco.com/wwl/export/crypto/ for guidance.

For specific export questions, please contact export@cisco.com.

Additional Information

Cisco Secure Intrusion Detection System:

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

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 Camil le 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

LW2654 09/01

Printed in the USA

CISCO SYSTEMS

Q & A

Cisco Intrusion **Detection** System

Q. What is a "network-based" IDS?

A. Two basic types of IDSs are on the market today: host-based and network-based systems. The fundamental difference between them is the source of the activity that they monitor and analyze to detect intrusions. Host-based IDSs monitor activity on a host or end system, while network-based IDSs monitor network traffic. Host-based IDSs are used to protect critical network servers or other individual systems containing sensitive information.

Network-based IDSs are used to monitor activity on a specific network segment. Whereas a host-based IDS resides on a workstation and shares CPU with other user applications, a network-based solution is a dedicated platform. Network-based IDSs perform a rule-based or expert system analysis of traffic using parameters set up by the security manager, and the signatures, which flag suspicious or attack activity. The systems analyze network packet headers to make security decisions based on source, destination, and packet type. They also analyze packet data to make decisions based on the actual data being transmitted. These systems scale well for network protection because the number of actual workstations, servers, or user systems on the network is not critical, the amount of traffic is what matters. In addition, sensors placed around the globe can be configured to report back to a central site, enabling a small team of security experts to support a large enterprise. The Cisco® network-based Intrusion Detection System provides network administrators with enhanced security technology and capabilities to secure their networks.

Q. If I already have a firewall, do I really need an IDS?

A. Absolutely. Although an IDS will not replace your firewalls or other security devices for that matter, it serves a very complementary role and addresses certain risks that firewalls cannot. The primary function of the firewall is to control access to services and hosts based on your site security policy. If a service or connection to a specific host is permitted, firewalls typically permit all such traffic, and they do not inspect the content of the permitted traffic. An example is permitting public access to a Web server on a DMZ. All connection requests to the Hypertext Transfer Protocol (HTTP) port on that Web server will be permitted by the firewall, including malicious traffic directed at the HTTP server to exploit a buffer overflow vulnerability. Although most firewalls will not protect against data/content-driven attacks (for example, buffer overflow), IDSs will. Furthermore, firewalls typically will not protect you against attacks originating from inside your network or entering your environment from other ingress points not protected by firewalls (for example, remote access servers). IDSs can be strategically deployed to monitor activity from internal sources and other network ingress points without impacting your network. Deploying an IDS to complement your firewall(s) will significantly enhance your security posture.

Q. Is there a mechanism by which users may contact the IDS Product Team at Cisco?

A. Yes. Users may pose questions, requests, and comments to the following e-mail address:

ids-news@cisco.com

In addition, users have the ability to share experiences with other users and also pose questions to the Cisco IDS Engineering & Product Marketing teams at the IDS Networking Professionals Forum at:

http://forums.cisco.com/eforum/servlet/
NetProf?page=netprof&CommCmd=MB%3FcmdDdisplay_messages26mode3Dnew26location%3D.ee6e1fc

Q. Does anyone offer a managed IDS service using the Cisco IDS?

A. Yes, numerous managed service providers offer a managed IDS service using the Cisco IDS. These managed service providers include AT&T, Counterpane, IBM Emergency Response Services, NetSolve, Riptech, RedSiren, and Ubizen.

Sensors

Q. What are the new features of the Cisco IDS 4.0 Sensor software?

A. The Cisco IDS 4.0 Sensor software delivers a number of new features and enhancements to the network-based IDS portfolio. These features include:

- Re-architecture of communications protocol to enhance the efficiency of message transactions
- Common code base to allow feature parity between the appliance sensor and the switch sensor
- Delivery of a Layer 2 signature engine to mitigate issues such as man in the middle attacks and ARP spoofing in switched environments
- Introduction of an SMB engine to efficiently address attacks related to SMB
- Ability to capture the trigger packet that caused an alarm
- Enhanced shunning capabilities to allow shunning by port address
- Major enhancements to our existing protocol anomaly techniques
- Provision of Analysis Statistics Engine to deliver information of metrics such as bad checksums, bytes processed, data rates Mbps, TCP nodes per sec, and other analysis metrics
- Introduction of a full featured Cisco IOS-like CLI (command-line interface) for unprecedented sensor management over a secure SSH connection
- Capability of capture and display of the VLAN ID of the malicious traffic that was detected
- Enhancements to IP Fragmentation Reassembly
- Higher levels of granularity for the alarm information that is transmitted to the management console
- Support for ntp
- NAT support
- Logical signature groupings to allow global changes across the groupings
- Ability to implement exceptions to filter events to be displayed
- Tunability of IP session logging parameters

Q. What performance numbers (Mbps) are supported by the Cisco IDS Sensors?

A. The Cisco IDS 4215 supports 80 Mbps of performance and can be used to protect T1/E1/T3 environments.

At 250 Mbps, the Cisco IDS 4235 can be deployed to provide protection in switched environments, on multiple T3 subnets, and with the support of 10/100/1000 interfaces, it can also be deployed on partially utilized gigabit links.

The Cisco IDS 4250 supports superior performance at 500 Mbps and can be used to protect gigabit subnets and traffic traversing switches that are being used to aggregate traffic from numerous subnets.

Intrusion protection for fully saturated gigabit links is delivered by the Cisco IDS 4250-XL. Using customized hardware acceleration, the IDS-4250-XL can be used to protect gigabit subnets and multiple partially utilized gigabit links.

The Cisco Catalyst® 6500 Series Intrusion Detection System (IDSM-2) Services Module supports 600 Mbps. This module operates within the Catalyst 6500 Series and provides protection for traffic traversing the switch, which could be traffic from a single subnet or from numerous subnets that are being aggregated through the switch.

The Cisco IDS Network Module provides full-featured Intrusion Protection that is integrated into the Cisco 2600, 3600, and 3700 series routers. Each sensor addresses the bandwidth requirements of different routers up to 10 Mbps in the Cisco 2600XM, and up to 45 Mbps in the Cisco 3700 Series. By integrating IDS and branch office routing, Cisco reduces the complexity of securing WAN links and at the same time reduces operational costs. Additionally, by delivering full-featured intrusion protection to remote offices and branch offices, network administrators can now mitigate threats at these remote locations and effectively isolate them from the corporate network. The Network Module has the capability of inspecting GRE/IPsec encrypted packets that are traversing the router into which it integrates.

Q. How does the IDS sensor work?

A. Sensors monitor the network traffic by directly "tapping" the line (for example, via a shared-media hub) or by receiving copies of the traffic (for example, Switched Port Analyzer [SPAN] port on a switch) using a passive, promiscuous interface (the "monitoring interface"). The sensor analyzes the captured packets and compares them against a rule set of typical intrusion activity (that is, "signatures"). If the captured packets match a defined intrusion pattern in the rule set, the sensor sends an alarm to the management console and automatically responds (if configured to do so). The alarms are sent out a separate management interface so as not to impede continual packet capture by the monitoring interface.

Q. What kind of a performance impact does the sensor impose on the monitored network?

A. None. Sensors operate by "tapping" the network (for example, via a shared-media hub) or off copies of the packets (for example, via a switch SPAN port). The monitoring interfaces on the sensors are passive and do not source packets onto the network (the one exception is TCP reset packets for automatic response).

Q. How do you deploy sensors in a switched environment?

A. With most IDS products on the market today, sensors must be placed on the switch SPAN port to monitor network traffic. Although the SPAN port can provide access to network traffic, it does have certain limitations (for example, limited number of SPAN sessions). The Catalyst 6000 IDS Module was designed specifically to address switched environments by integrating the IDS functionality directly into the switch and taking traffic right off the switch backplane.

Q. What is the Cisco IDS Network Module for the Cisco 2600, 3600, and 3700 series routers?

A. The Cisco IDS Network Module is a network module that is installed in a Cisco 2600, 3600, or 3700 series chassis to provide full-featured intrusion protection services within the router. The Cisco 2600, 3600, and 3700 Series IDS Network Module provides the ability to inspect all traffic traversing the router, to identify unauthorized or malicious activity such as hacker attacks, worms, or denial-of-service attacks, and to terminate this traffic to suppress or contain threats.

Q. How does the Cisco IDS Network Module work?

A. The Cisco 2600, 3600, and 3700 Series IDS Network Module receives copies of packets directly from the router's backplane in a passive or promiscuous mode. The packets are passed through the internal monitoring interface for classification and processing. The Cisco 2600, 3600, and 3700 Series IDS Network Module analyzes the captured packets and compares them against a rule set of typical intrusion activity. If the captured packets match a defined intrusion pattern in the rule set, the IDS Network Module can take one of two actions. It can send a command to the router to either shut down the interface or it can send a TCP reset packet to the sender to stop the TCP session causing the attack.

Q. What is the rated performance of the Cisco 2600, 3600, and 3700 Series IDS Network Module?

A. The Cisco 2600, 3600, and 3700 Series IDS Network Module provides up to 10 Mbps for the 2600XM Series and up to 45 Mbps for the 3700 Series, depending on the platform in which the network module is inserted.

Q. Can the Cisco Network IDS Sensors monitor trunked traffic?

A. Both IDSM and the appliance sensors can monitior 802.1q traffic and, hence, are VLAN aware.

Q. What type of interfaces are supported on the appliance sensors?

A. Copper interfaces are supported on the IDS 4215 and IDS 4235. Both Copper and Fiber interfaces are supported on the IDS 4250 Sensor. The 4250-XL supports dual fiber interfaces with MTRJ connectors.

Q. Does Cisco IDS provide multi-interface support?

A. Yes. Dual sniffing interfaces are supported on the IDS 4250-XL. Up to 5 interfaces are supported on the IDS 4215, 4235, and 4250 Sensor appliances.

A configurable four Fast Ethernet interface card is provided for other models of the Cisco 4200 Series sensors to deliver a total of five sniffing interfaces for each sensor—one onboard sniffing interface plus four Fast Ethernet configurable interfaces.

The Cisco IDSM-2 can be used to monitor traffic from multiple interfaces. The network module for the Cisco access routers can monitor traffic from any of the router interfaces.

Q. Is the user notified when the sniffing interface of a sensor is disconnected?

A. Sensors are equipped with a monitoring interface for data packet capture and a command and control interface for transmitting alarms to the management console and receiving configuration information from the management console. When the sniffing interface is disconnected, an alarm is triggered. This setup provides the user with an alert mechanism when the interface is tampered with and, hence, assures persistent operation.

Q. Does the Cisco IDS Sensor provide an indication of when it is oversubscribed?

A. Yes. The sensor, IDSM, and network module issue an alarm when their respective performance ratings are exceeded.

Q. Where can I find more details on the IDS signature algorithms?

A. For more information on the signature algorithms, please refer to a white paper that may be downloaded at:

http://www.cisco.com/warp/public/cc/pd/sqsw/sqidsz/prodlit/idssa_wp.htm

Q. Does Cisco IDS protect against common IDS evasion techniques?

A. Cisco IDS also includes protection from a number of advanced, anti-IDS evasion techniques including:

- IP fragmentation reassembly
- TCP streams reassembly
- Unicode Web deobfuscation

Q. Can the sensor itself be attacked and compromised?

A. A properly configured and installed sensor cannot be compromised. The monitoring interface (connected to the production network) cannot be detected, and packets cannot be directed at it. The interface is in promiscuous mode, and has neither a protocol stack nor an IP address bound to it. It is not susceptible to "antisniff" detection techniques. The separate management interface does have an IP address, but Cisco recommends that a separate, isolated management subnet be used to provide connectivity from the management interface on the sensor to the IDS management console. In addition, only a very limited number of services are available from the management interface, and access controls can be configured to allow only designated management systems to connect to the sensor.

Q. What is Cisco Countermeasures Research Team (C-CRT)?

A. The core of the Cisco IDS solution—the advanced protection capabilities—is developed and maintained by C-CRT. This team of elite security professionals is dedicated to:

- Advancing countermeasures research
- Identifying and responding to new threats
- Distributing proactive signature files and signature micro-engines
- Maintaining our network security database (NSDB)
- Contributing research to the Cisco Security Encyclopedia (CSEC)
- Improving the state of threat mitigation science

The C-CRT is comprised of elite "white hat" personnel. C-CRT's esteemed credentials include:

- *Heritage and tenure*—most joined Cisco through the WheelGroup acquisition.
- *Government clearance*—greater than 65 percent have held Secret and Top Secret Department of Defense security clearances.
- *Military backgrounds*—experience logged from USAF Information Warfare Center, Department of Defense (DOD), Department of Energy (DOE), National Security Agency (NSA), Central Intelligence Agency (CIA), or other notable government organizations.
- *Security experience*—average member of the C-CRT has over six years of computer security experience, allowing Cisco to deliver the most mature, accurate, and industry-proven intrusion protection solutions.

Q. Can I create my own signatures?

A. Because the security objectives for each IDS deployment are unique, Cisco IDS adds granularity to the way in which sensors may be tuned to specifically suit the environment in which they are deployed. Using our innovative TAME (Threat Analysis Micro Engine) policy language, users can create new policies or modify existing policies to meet their unique security objectives. Since the TAME policies are decoupled from the sensing application, changes can be made without affecting sensor performance or reliability.

Q. Is it possible to record and replay the IP session of the source IP address that triggered an IDS alarm?

A. IP session logging provides extensive logging that is important for system troubleshooting as well as for reconstructing system events before and after attacks. Cisco IDS augments this capability by converting these logs to a standard TCP dump format that allows them to be viewed and replayed using public domain utilities, such as Ethereal and TCPReplay.

Q. Can the sensor detect attacks if the traffic is encrypted, for example IPsecurity (IPsec) or Secure Sockets Layer (SSL)?

A. The Cisco IDS Sensor analyzes both packet header information (context data) and packet data information (content data) to determine if suspicious activity is occurring. Encryption algorithms encrypt the data portion of the packet for confidentiality. Because it can process only what it can "see," the Sensor cannot detect attacks that require inspection of the payload or data fields within a packet. It will, however, still alarm and respond to attacks, which are detected from the unencrypted packet header information. All network-based IDSs suffer this problem. Therefore, in networks carrying encrypted traffic, Sensor placement is critical. To take advantage of their full intrusion-detection capability, the Cisco IDS Sensors should be installed where the traffic has already been decrypted. Otherwise, the Sensor can be placed on an encrypted segment and will detect all but the packet data or payload-based attacks.

Q. What techniques does Cisco use for mitigating threats?

A. Several techniques provide comprehensive protection against the latest cyber threats, including simple pattern matching, stateful pattern matching, protocol anomaly detection, heuristic-based detection, and anomaly detection.

Q. Does Cisco IDS deliver Peer to Peer signatures?

A. Yes. Cisco IDS delivers protection against file-sharing threats with support for advanced P2P attack mitigation techniques.

Q. How are the Cisco IDS signatures updated?

A. Cisco posts signature updates on Cisco Connection Online (CCO) approximately every 14 days. Cisco IDS provides a facility to automatically distribute new signature files and application upgrades to sensors without operator involvement. Utilizing a secure staging technique, new signature files are placed on a central server and passed to the sensor at scheduled intervals. After verifying the integrity of the package, the sensor automatically installs the update. This new capability significantly streamlines the process of regularly updating remote sensors, thereby lowering the recurring operational costs associated with this task. Additionally, users can subscribe to Cisco Active Update notification services to stay informed about breaking vulnerability news and posted countermeasures at:

http://www.cisco.com/warp/public/779/largeent/issues/security/idsnws/archive.html

Users may refer to the following site for a chronological listing of the Cisco IDS Active Update Notification Bulletins:

http://www.cisco.com/warp/public/779/largeent/issues/security/idsnws/archive.html

Q. How do the Cisco IDS Sensors and management consoles communicate with each other?

A. Communication between the Cisco IDS 4.0 Sensors and management consoles is provided by a secure (SSL) XML based messaging format. All alarm transmissions from the sensor to the management console are acknowledged.

If connectivity from the sensor to the management console is disrupted, the sensor will continue to monitor the network, and will queue alarms and retransmit until successful.

Q. How much additional network traffic does the Cisco IDS generate?

A. Because each alarm and acknowledgment is contained in a single UDP packet, there is negligible impact on network traffic.

Q. Is there a site that lists all the supported Cisco IDS signatures?

A. Yes. Users may access the latest Cisco IDS signatures at the Cisco Secure Encyclopedia site at:

http://www.cisco.com/pcgi-bin/front.x/csec/idsHome.pl

Q. Does Cisco support a centralized site that contains a compiled listing of the latest vulnerabilities?

A. Yes. Cisco's Security Encyclopedia is a one-of-a-kind clearinghouse of security and vulnerability information. Unlike other security databases that simply consolidate vulnerability information published on a number of public-source Web sites, the CSEC contains statistics on the vulnerabilities by industry or by sector. These statistics are compiled from over 400 actual Security Posture Assessments (SPA) performed by the Cisco Security Consulting team. CSEC is developed and maintained by the elite C-CRT. You may visit the CSEC site at:

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

Q. Where can I download the latest IDS software?

A. Both current and archived IDS Sensor software can be downloaded at the Software Center on CCO (CCO login required):

http://www.cisco.com/public/sw-center/ciscosecure/ids/crypto/

Q. Where can I access documentation on the Cisco IDS Sensor Software?

A. Documentation for sensor software updates are available at:

http://www.cisco.com/univercd/cc/td/doc/product/iaabu/csids/index.htm

Threat Response Technology

Q. Is Threat Response an event correlator?

A. Threat Response is not an event correlator. Event correlation involves analyzing data from NIDS sensor, firewalls, routers, and other sources. Instead of correlating this type of data, Threat Response investigates the actual target of an attack. This is the same process an expert network security specialist would use, and is the best way to determine if a system has been compromised.

Q. Does Threat Response conduct network vulnerability scans?

A. No, Threat Response does not conduct enterprise wide scans of your environment, nor does Threat Response inventory your network. The designers of Threat Response have been network administrators for large mission-critical enterprises such as the U.S. Pentagon and know that downtime is unacceptable. Because of this, Threat Response conducts a low-impact investigation of targeted systems only when needed. Threat Response is able to work in dynamic network environments (including DHCP and wireless) without the need to run regular vulnerability scans that can disrupt your enterprise.

Q. Does Threat Response require deployment of software across the enterprise?

A. No, Threat Response does not require the deployment of software across the enterprise. Threat Response accesses these systems in the same way a security network administrator would—with read access privileges.

Q. How does Threat Response stay up to date with the latest attacks?

A. Cisco releases updates to keep the Threat Response IDS signature database up to date with the IDS vendors, as well as corresponding forensic signature updates to investigate IDS events. When an update is available, the administrator will be notified via the Threat Response GUI and can use the integrated auto-update feature to keep the product current.

Q. What does Threat Response do once real attacks are identified?

A. Threat Response will provide the user with detailed information on how the event was investigated, as well as any forensic data gathered showing details on the actual attack. This information can then be used by an administrator to quickly remediate an intrusion.

Q. What type of systems can Threat Response investigate?

A. Threat Response can conduct a full active investigation of systems running Windows-based operating systems. For systems running Linux, Solaris, and other forms of UNIX, Threat Response will perform passive checks as a first line of investigation. Based on this initial analysis, Threat Response can eliminate many alarms that are not targeted to those specific platform types.

Q. How do I get Threat Response technology?

A. Threat Response technology is currently available as a full featured, 90-day free trial software solution. The trial version ships with every Cisco IDS sensor. Once the trial has expired, customers have the choice of:

- switching to a reduced capabilities free version (only conducts basic level investigation of the targeted system)
- purchasing the full featured version, which will be offered as part of a VMS bundle

Management

Q. What management console options are available for the Cisco IDS?

A. See Table 1 and Table 2.

Table 1 Event Management

	IEV	IEV with CTR Technology	VMS SecMon	VMS SecMon with CTR Technology
Deployment method	Dedicated system required	Dedicated system required	Dedicated system required	Dedicated system required
GUI type	Java desktop application	Browser-based GUI	Browser-based GUI	Browser-based GUI
# sensors	5	5	Unlimited	Unlimited
Event types	IDS	IDS	IDS, Firewall, Router	IDS, Firewall, Router

Table 2 Device Management

	IDM	CLI	VMS Management Center
Deployment method	Integrated on sensor	Integrated on sensor	Dedicated system required
GUI type	Browser-based GUI	Browser-based GUI	Browser-based GUI
# sensors	Unlimited, by sensor	Unlimited, by sensor	Unlimited, by sensor groups
Event types	IDS	IDS	IDS, Firewall, Router

IEV = Cisco IDS Event Viewer, included free of charge with IDS sensor
VMS SecMon = CiscoWorks Monitoring Center for IDS, part of the CiscoWorks VMS bundle
IDM = IDS Device Manager, included free of charge with the IDS sensor
CLI = Command-line interface, included free of charge with the IDS sensor
VMS Mgmt Center = CiscoWorks Management Center for IDS, part of the CiscoWorks VMS bundle

For More Information

More information on Cisco's VMS solutions can be found at:

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

In addition, augmentation to the alarm viewing, analysis, and reporting capabilities of the Cisco IDS Management solution are provided through third-party applications that are available from Cisco Security Associates partners.

For more details see:

http://www.cisco.com/warp/public/778/security/sap/management.html

Q. Are Cisco IDS communications encrypted?

A. IPsec functionality is included on the appliance Sensors to allow customers to encrypt traffic to management consoles with IPsec capabilities.

Q. If I lose connectivity to a remote sensor, can I tell from the management console?

A. The Cisco IDS management consoles monitor the health of a Sensor via a continuous heartbeat. If communications with the Sensor are lost for more than one minute (by default), a visual indicator is displayed on the management console, indicating a communications failure with the Sensor. If it is determined that a sensor has failed, it can be quickly replaced with another sensor and the configuration, stored on the management console, and can be quickly pushed to the new sensor.

Q. How many sensors can one Cisco IDS Management console manage?

A. Although the technical limit is very large (greater than 1000), Cisco typically recommends a ratio of 20 to 25 sensors per management console for practical reasons. With ratios greater than this, operators can be easily overwhelmed with the volume of information that they may be required to analyze, thereby diminishing the overall effectiveness of the IDS. For deployments larger than 25 sensors, multiple management consoles can be installed to scale the number of sensors.

Q. Can I have multiple Cisco IDS management consoles?

A. The Cisco IDS architecture supports the deployment of multiple management platforms. Sensors can send alarms to multiple management consoles simultaneously, and management consoles can forward alarms to other management consoles, allowing customers to build large, hierarchical management infrastructures.

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

Design Guide

Cisco IOS **Intrusion Detection** Systems

Executive Summary

Intrusion detection has become a critical component of Enterprise and Service Provider infrasturctures. Increasing complexity in public networks for data transport in light of new business applications, e-commerce, extranets and virtual private networks (VPNs) has created increased risks to the integrity and security of internal network.

In order to counter increasing security threats, Cisco IOS, Intrusion Detection Systems (IDS) offers added abilities for detection, logging, auditing and mitigation to a variety of existing security products. Cisco offers complementary technologies in firewall products (Cisco IOS Firewall, PIX, etc), encryption technologies (Cisco IOS IPSec VPNs, Cisco VPN-3000, Authentication, Authorization, and Accounting [AAA]) for a full-layered approach security.

Cisco IOS IDS includes intrusion detection technology for the full range of Cisco IOS routers. Cisco 1700, 2600, 3600, 7100, 7200, 7500, and RSM Series Routers support Cisco IOS IDS. The Cisco 830 Series router will support Cisco IOS IDS. It is targeted for November 2003 . These intrusion detection capabilities are ideal for monitoring intranet, extranet, and branch office Internet perimeters against network violations. Integrated into the routing path, Cisco IOS IDS uses signatures to identify common attacks, and to subsequently protect the network.

Cisco IOS IDS acts as an in-line intrusion detection sensor, watching packets as they traverse the router's interfaces and acting upon them in a definable fashion. When one or more packets in a session match a signature, Cisco IOS IDS may perform the following configurable actions:

- *Alarm*: sends an alarm to a syslog server or Net Ranger Director
- *Drop*: drops the packet
- *Reset*: resets the TCP connection

Through the use of syslog and integration with CiscoWorks VPN/Security Management Solution (VMS), security operations can quantify their security posture and determine any threats to the networks. These metrics provide a machanism to track unauthorized network activity over time and evaluate security policy effectiveness, security activities, and budgeting considerations from a quantifiable perspective.

The remainder of this guide provides a background of information for Cisco IOS IDS, design considerations and scenarios for deployment. Cisco IOS IDS is available in Cisco IOS Software Release 12.0.(5)T and later releases. Advanced performance improvements for Cisco IOS IDS were released in Release 12.2.(8)T.

Cisco Comprehensive Security Solution

Intrusion detection implementation requires planning. Intrusion detection technology is a complementary tool that should be utilized alongside traditional security products. Cisco IOS IDS is one part of the end-to-end security solution. Products such as Firewalls, Encryption and Authentication, and Access Control Lists should be part of an integrated approach to implementing any Corporate Security Policy.

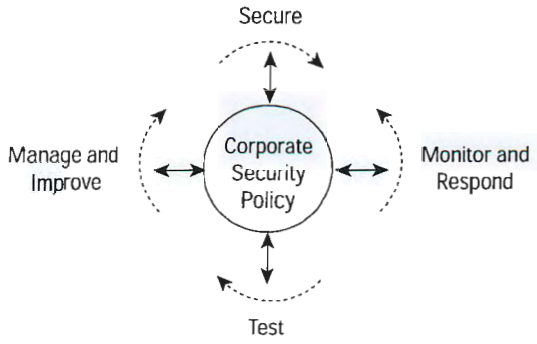
Considerations for the following should be taken into account to understand overall security concerns:

- Security Wheel
- Developing a Strong Security Policy
- Securing the Network
- Monitoring the Network
- Testing Security
- Improving Security

The Security Wheel

The Cisco security solution approach is one of an operational perspective rather than one of a products or policy approach. Like network management, the philosophy is one that addresses a dynamic, process towards security.

Figure 1. The Security Wheel



The Security Wheel is cylical, ensuring diligence and imporvement. The paradigm incorporates the following five step:

1. Develop a strong security policy
2. Secure the network
3. Monitor the network and respond to attacks
4. Test existing security safeguards
5. Manage and improve corporate security

Data gained from Steps 2 through 5 should always be reflected back to the corporate security policy in Step 1, so that high-level security expectations are being met.

Developing a Strong Security Policy

Consideration of the following is crucial in developing a strong security policy:

- What assets must be protected?
- What is the risk to those assets?
- What is the impact (in terms of reputation, revenues, profits, research) of a successful attack?
- How much sensitive information is available online? What is the impact if this information is damaged or stolen?
- Which users have access to those assets?
- What do users (including partners and customers) expect in terms of security control procedures and mechanisms?
- Should users be trusted?
- Are users accessing assets locally or remotely, or a mixture of both?
- Do distinct parts of the organization have different security requirements?
- What types of traffic exist on the network?
- Are the needs of security consistent with the business/operational needs of the organization?
- Is there a strong commitment from management to provide sufficient resources to implement security policies and technologies?
- Is there a strong commitment for security awareness training?

A strong security policy should be clearly defined, implemented, and documented, yet simple enough that users can easily conduct business within its parameters. A policy of strong password creation can only work if there is a system to validate password selection.

In many ways, the security policy is a risk management plan, as it documents the risk threshold an organization is willing to accept. Because no security technology provides one hundred percent protection, and in most cases organizations do not have the budget to implement all required security elements, the security policy rates assets and applies commensurable levels of security.

A critical element often overlooked is the policy on incident response. What is the official organization response if a policy is violated?

For additional information on the development and implementation of information security policies, refer to SANS Institute Resources: http://www.sans.org/newlook/resources/policies/policies.htm

Securing Your Network

Once the security policy is developing, the network must be secured with multiple technologies: firewalls, intrusion detection, AAA, etc. However, this cannot occur without complete understanding of the user, assets, and network topology.

Understand Your Network Topology

Careful inspection of the following will help to prevent possible miscalculations in deploying and configuring Cisco IOS IDS:

- Network size and complexity
- Locations of critical resources (file servers, hosts, etc.) on the network
- Connections with other networks, both Internet and extranets
- The amount and type of network traffic

Consideration of these placement points will help determine where Cisco IOS IDS can be enabled. All connections to the network that require protection should receive the same degree of consideration.

Monitoring the Network

Once the network has been secured, activity should be monitored, either via syslog or through the use CiscoWorks VMS. When a security violation does occur, an appropriate response is crucial:

- Logging the event
- Resetting the TCP connection
- Dropping the offending packets
- Possible reconfiguration of the ACLs on the router, in order to deny the attack

Specific responses should be detailed within the security policy.

Testing Security

Periodic scans of the network for new vulnerabilities are appropriate. Changes in the network and service/technology advancement can create new "security holes". These aspects are inevitable and should be considered normal operations within a growing network. New test procedures for testing security as well as testing the pre-established policy should be part of this review procedure for improvement.

Improving Security

Analyze all the metrics that are collected. Each part of the security cycle will produce different information, which can then be prioritized. When responding to a threat, consider:

A) Identify resources required to respond

B) Incident response policy

C) Chart ownership and monitoring of security

Keep abreast of any new network threats by improving on the established security policy. Continue to implement the Security Wheel cycle.

Technical Highlights

Cisco IOS IDS supports intrusion detection technology for midrange and high-end router platforms with firewall support. It is ideal for any network perimeter, and especially for locations in which a router is deployed, and additional security between network segments is required. It also can protect intranet and extranet connections where additional security is mandated, and branch-office sites connecting to the corporate office or Internet.

Intrusion detection systems provide a level of protection beyond the firewall by protecting the network from internal and external attacks and threats. Cisco IOS IDS enhances perimeter firewall protection by taking appropriate action on packets and flows that violate the security policy or represent malicious network activity.

Cisco IOS IDS acts as an in-line intrusion detection sensor, watching packets as they traverse the router's interfaces and acting upon them in a definable fashion. When one or more packets in a session match a signature, Cisco IOS IDS may perform the following configurable actions:

- *Alarm*: sends an alarm to a syslog server or Net Ranger Director
- *Drop*: drops the packet
- *Reset*: resets the TCP connection

Intrusion detection systems customers that have already deployed Cisco IDS "appliance sensors" can deploy Cisco IOS IDS signatures to complement their existing systems. This allows an intrusion detection system to be deployed in areas that may not support a Cisco IDS Sensor. Cisco IOS IDS signatures can be deployed alongside or independently of other Cisco IOS Firewall features.

Cisco IOS Firewall with intrusion detection can be added as an icon on the Cisco VMS Security Monitor screen, providing a consistent view of all intrusion detection sensors throughout a network. Cisco IOS Firewall intrusion detection capabilities have an enhanced reporting mechanism that permits event logging to the Security Monitor console via Cisco IOS syslog.

Cisco IOS IDS utilizes signatures to detect patters of misuse in the network. Each signature is categorized by severity and complexity. Signatures are classified by both severity and complexity:

Severity:

Informational signatures: detect information (ie: port sweep)

Attack signatures: detect malicious activity (ie: illegal ftp commands; Denial of Service (DoS attempt),

Complexity:

Atomic signatures: detect simple patterns (ie: attempt on a specific host or within a single packet)

Compound signatures: detect complex patterns (ie: attack on multiple hosts, over extended time periods with multiple packets)

Configuration Basics

1. Initialize Cisco IOS IDS—ip audit parameters (alarm, drop, and/or reset)

An audit rule specifies the signatures that should be applied to a packet traffic and the actions to be taken when a match is found. The signature list can include any number of signatures. Signatures can be disabled in case of false positives, or based on the needs of the network.

Note: it is generally recommended that drop and reset actions be used together.

Command Syntax:

```
   ip audit info {action [alarm] [drop] [reset]}        ! Sets the default actions for
info and attack signatures
   ip audit attack {action [alarm] [drop] [reset]}
   ip audit name audit-name {info | attack} [list standard-acl] [action [alarm] [drop]
[reset]] ! Creates audit rules, where audit-name is a user-defined name for an audit rule.
```

2. Determine logging Policy

Command Syntax:

```
ip audit notify log    ! Sends event notifications (alarms) to either a Cisco Secure
IDS Director, a syslog server, or both.
```

3. Configure and Apply Audit Rules—which interfaces, what routing path?

Audit rules can be applied to an interface on the router with a specific direction (*in* or *out*).

If the audit rule is applied to the in direction on the interface, packets passing through the interface are audited before the inbound ACL can to discard them. This alerts an administrator if an attack or information-gathering activity is underway. Because of this sequences of events, IDS can trigger even if the router would otherwise reject the activity.

Audit rules that are applied in the out direction on an interface are conversly auditing packets after they have entered the router through another interface. Inbound ACLs of other interfaces may discard packets before they are audited. As such, IDS alarms may be lost even though the attack or information-gathering activity was thwarted.

Command Syntax:

```
interface interface-number              ! Enters interface configuration mode.
ip audit audit-name {in | out}          ! Applies an audit rule at an interface. With this
command, audit-name is the name of an existing audit rule, and direction is either in or
out.
```

4. Verify the Configuration

```
show ip audit configuration
show ip audit interface
show ip audit statistics
```

5. Optionally Disabling Signatures

```
ip audit signature signature-id {disable | list acl-list}     ! Disables individual
signatures.
```

Cisco IOS IDS Deployment Scenarios

Cisco IOS IDS capabilities are ideal for providing additional visibility at intranet, extranet, and branch-office Internet perimeters. Network administrators enjoy more robust protection against attacks on the network and can automatically respond to threats from internal or external hosts.

Cisco IOS IDS is intended to satisfy the security goals of all of our customers, and is particularly appropriate for the following scenarios:

- *Enterprise*: interested in a cost-effective way to extend perimeter security across all network boundaries, specifically branch-office, intranet, and extranet perimeters.
- *Small and medium businesses*: need a cost-effective router that has an integrated firewall with intrusion-detection capabilities.
- *Service Providers*: may want to deploy this as the router/firewall for a managed service. They can set this at subscribers' sites to provide firewalling and intrusion detection within the necessary function of a router.

Commonly referred to as "perimeter protection" Cisco IOS IDS can be placed to monitor traffic between the network and the Internet. Companies generally also use a firewall to protect the perimter, which the most common deployment scenario. This enables the both incoming and outgoing traffic to be monitored.

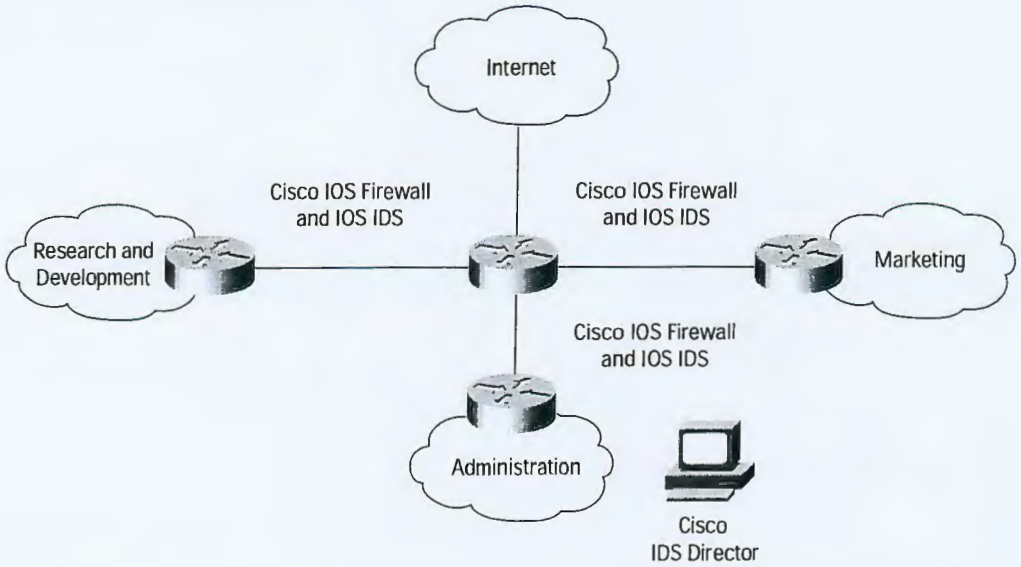
An internal attacker can additionally take advantagte of network services that otherwise go unprotected. For this reason, the perimeter protection offers little help. Placing Cisco IOS IDS on other segments, and in the routing path solves this problem and can shield from outside attacks, while addressing often overlooked networks: extranet, remote access, and less secure intranet networks.

Although partner companies generally have security policies of their own, there is often little reassurrance that these policies are adequately enforced. Outsiders often may enter a network through this type of connection, so it should also be protected and firewalled.

Remote access networks are also notorious for their vulnerability to attack. Although generally designated for employee use, external attackers often expliot vunerabilities in authorization, authentication and or wireless technologies. Cisco IOS IDS defends and monitors against such weaknesses in this area.

As mentioned earlier, intranet connections should also be monitored and protected with Cisco IOS IDS. Research and Development networks and Engineering resources, for example, often require additional security mesurements to protect proprietary information. For these areas, a robust security solution can be achieved by utilizing a combined approach of strong access control lists, Cisco IOS Firewall, and Cisco IOS IDS. (Figure 2).

Figure 2. Combined Security Approach



When Cisco IOS IDS is deployed, audit rules are applied specifying the direction of traffic through an interface (in or out).

Audit rules applied to the in direction on an interface will allow packets passing through the interface to be audited before inbound ACLs.

Audit rules applied to the out direction of an interface allow signature matching to occur against packets after they enter the router through another interface. In this case, inbound ACLs may discard packets before they are audited. Unintentional loss of Cisco IOS IDS alarms may result, despite the avoidance of an attack or information-gathering activity. Detection of such unsuccessful violations and attack attempts are often equally as important as detecting successful attacks.

Memory and Performance Impact

The performance impact of intrusion detection will depend on the configuration of the signatures, the level of traffic on the router, the router platform, and other individual features enabled on the router (ie: encryption, source route bridging). Enabling or disabling individual signatures will not alter performance significantly; however, signatures that are configured to use ACLs will have a significant performance impact.

The network only uses this router as a security device; therefore, no packet is allowed to bypass the security mechanisms. Cisco IOS IDS sits directly in the packet path, so it searches each packet for signature matches. In some cases, the entire packet will need to be searched, while the router must maintain state information, application state, and awareness.

There is no traffic-dependent memory requirement for auditing atomic signatures. For auditing compound signatures, CBAC allocates memory to maintain the state of each session for each connection. Memory is also allocated for the configuration database and for internal caching.

Differing Cisco IDS Products

- Cisco IOS IDS (Router Sensor): Cisco IOS IDS delivers in-line integrated intrusion protection in the routing path with a feature-rich set of networking services. It provides real-time monitoring, interception, and response to network misuse with a broad set of the most common attack and information-gathering intrusion detection signatures.
- Cisco IDS -4210, 4235, 4250 (Network Sensor Appliance): Network sensor provides a comprehensive dedicated appliance model to protect the network of observation from malicious activity.
- Cisco IDS Module (Integrated Switch sensor): Integrated Switch Sensor is designed to protect switched environments by integrating full-featured IDS functionality directly into the network infrastructure. This allows the user to monitor traffic directly off the switch backplane.
- Cisco IDS Host Sensor: The Host Sensor provides comprehensive protection for the server operating system and the applications running on the servers. It is installed on each server, guarding operating system and applications, as well as access to those applications. The system employs call interception techniques to provide the only proactive server security system.
- Firewall Sensor: Integration of IDS functionality into Cisco PIX Series Firewalls. This protects common network-based attacks.

Conclusion

Cisco IOS IDS supports intrusion detection technology for midrange and high-end router platforms with firewall support. It is ideal for any network perimeter, and especially for locations which a router is being deployed and additional security between network segments is required. It also can protect intranet and extranet connections where additional security is mandated, as well as branch-office sites connecting to the corporate office or Internet.

Intrusion detection should be considered an integral component when designing and implementing a layered approach towards security. Sensors may be placed on almost any network segment of the enterprise-wide network where security visibility is required. Perimeter placements, internal network segments where critical resources are located, extranet connections, and DMZs are the most minimal of locations to consider when implementing and maintaining a security policy.

The Security Wheel can help to attain the goal of security in an ever-changing environment. To ensure that a high percentage of security objectives are achived, always secure, monitor, test, and improve.

References

Cisco IOS IDS (Product Documentation)

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t5/iosfw2/ios_ids.htm

Improving Security on Cisco Routers

http://www.cisco.com/warp/public/707/21.html

Security Technical Tips

http://www.cisco.com/warp/customer/707/index.shtml#IOS

Configuring Context-Based Access Control

http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a00800ca7c5.html

Configuring Cisco IOS IDS

http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a00800ca7c6.html

Defining Strategies to Protect Against TCP SYN Denial of Service Attacks

http://www.cisco.com/warp/public/707/4.html

Cisco IOS IDS Signature List

http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a00800ca7c6.html

SANS Institute Resource Project—The SANS Security Policy Project

http://www.sans.org/newlook/resources/policies/policies.htm

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

Cisco Systems

Data Sheet

Cisco IOS **Intrusion** Detection Systems **Signature List**

The following is a complete list of Cisco IOS® Intrusion Detection Systems (IDS) signatures, listed sequentially, by signature number, which is documented in the Cisco Secure Encyclopedia and Cisco IDS Signature Database.

Cisco IOS IDS identifies one hundred of the most common attacks that use "signatures" to detect patterns of misuse in network traffic. Forty-two of these are new signatures that have been added, based on analyzed data from the Security Posture Assessment (SPA) Database, PIX signature database, and fifteen of the most dangerous HTTP signatures in the Network Security Database (NSDB).

Fifty-nine intrusion-detection signatures were provided in Cisco IOS Firewall in images prior to Cisco IOS Software Release 12.2(11)YU. Forty-two new signatures are included in this release, in addition to all images after the next release of Cisco IOS Software Release 12.2T. These signatures, which were chosen from a broad cross-section of intrusion-detection signatures, represent the most severe breaches of security, common network attacks and information-gathering scans that are commonly found in an operational network.

Cisco IOS IDS signatures can be categorized by severity and complexity:

- Severity
  - *Info signatures* (forty): detect information-gathering activities (ie: port sweep)
  - *Attack signatures* (sixty-one): detect malicious activity (ie: illegal ftp commands)
- Complexity
  - *Atomic signatures* (seventy-four): detect simple patterns (ie: attempt on a specific host)
  - *Compound signatures* (twenty-seven): detect complex patterns (ie: attack on multiple hosts, over extended time periods with multiple packets)

Cisco IOS IDS Signatures

To access Cisco Secure Encyclopedia information about each signature, click on the signature name, enter your CCO login/password, and accept the Terms & Conditions that are stated.

Signature	Severity	Complexity	Timeframe	Description
1000 IP Options-Bad Option List	Info	Atomic	Original 59 signatures	Triggers on receipt of an IP datagram where the list of IP options in the IP datagram header is incomplete or malformed. The IP options list contains one or more options that perform various network management or debugging tasks.
1001 IP Options-Record Packet Route	Info	Atomic	Original 59 signatures	Triggers on receipt of an IP datagram where the IP option list for the datagram includes option 7 (Record Packet Route).
1002 IP Options-Timestamp			Original 59 signatures	Triggers on receipt of an IP datagram where the IP option list for the datagram includes option 4 (Timestamp).
1003 IP Options-Provide s,c,h,tcc	Info	Atomic	Original 59 signatures	Triggers on receipt of an IP datagram where the IP option list for the datagram includes option 2 (Security options).
1004 IP Options-Loose Source Route	Info	Atomic	Original 59 signatures	Triggers on receipt of an IP datagram where the IP option list for the datagram includes option 3 (Loose Source Route).
1005 IP Options-SATNET ID	Info	Atomic	Original 59 signatures	Triggers on receipt of an IP datagram where the IP option list for the datagram includes option 8 (SATNET stream identifier).
1006 IP Options-Strict Source Route	Info	Atomic	Original 59 signatures	Triggers on receipt of an IP datagram in which the IP option list for the datagram includes option 2 (Strict Source Routing).
1100 IP Fragment Attack	Attack	Atomic	Original 59 signatures	Triggers when any IP datagram is received with an offset value less than 5 but greater than 0 indicated in the offset field.
1101 Unknown IP Protocol	Info	Atomic	Modified signature of the original	Triggers when an IP datagram is received with the protocol field set to 134 or greater. These protocol types are undefined or reserved and should not be used.
1102 Impossible IP Packet	Attack	Atomic	Original 59 signatures	This triggers when an IP packet arrives with source equal to destination address. This signature will catch the so-called Land Attack.
1104 IP Localhost Source Spoof	Attack	Atomic	41 additional signatures	This signature triggers when an IP packet with a address of 127.0.0.1 is detected.
1105 Broadcast Source Address	Attack	Atomic	41 additional signatures	This signature triggers when an IP packet with a source address of 255.255.255.255 is detected.

Signature	Severity	Complexity	Timeframe	Description
1106 Multicast Ip Source Address	Attack	Atomic	41 additional signatures	This signature triggers when an IP packet with a source address of 224.x.x.x is detected.
1107 RFC 1918 Addresses Seen	Info	Atomic	41 additional signatures	This signature fire when RFC 1918 addresses are detected.
1202 IP Fragment Overrun—Datagram Too Long	Attack	Atomic	41 additional signatures	Triggers when a reassembled fragmented datagram would exceed the declared IP data length or the maximum datagram length.
1206 IP Fragment Too Small	Attack	Atomic	41 additional signatures	Triggers when any fragment other than the final fragment is less than 400 bytes, indicating that the fragment is likely intentionally crafted.
2000 ICMP Echo Reply	Info	Atomic	Original 59 signatures	Triggers when a IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 0 (Echo Reply).
2001 ICMP Host Unreachable	Info	Atomic	Original 59 signatures	Triggers when an IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 3 (Host Unreachable).
2002 ICMP Source Quench	Info	Atomic	Original 59 signatures	Triggers when an IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 4 (Source Quench).
2003 ICMP Redirect	Info	Atomic	Original 59 signatures	Triggers when a IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 5 (Redirect).
2004 ICMP Echo Request	Info	Atomic	Original 59 signatures	Triggers when a IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 8 (Echo Request).
2005 ICMP Time Exceeded for a Datagram	Info	Atomic	Original 59 signatures	Triggers when a IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 11(Time Exceeded for a Datagram).
2006 ICMP Parameter Problem on Datagram	Info	Atomic	Original 59 signatures	Triggers when a IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 12 (Parameter Problem on Datagram).
2007 ICMP Timestamp Request	Info	Atomic	Original 59 signatures	Triggers when a IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 13 (Timestamp Request).

Signature	Severity	Complexity	Timeframe	Description
2008 ICMP Timestamp Reply	Info	Atomic	Original 59 signatures	Triggers when a IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 14 (Timestamp Reply).
2009 ICMP Information Request	Info	Atomic	Original 59 signatures	Triggers when a IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 15 (Information Request).
2010 ICMP Information Reply	Info	Atomic	Original 59 signatures	Triggers when a IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 16 (ICMP Information Reply).
2011 ICMP Address Mask Request	Info	Atomic	Original 59 signatures	Triggers when a IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 17 (Address Mask Request).
2012 ICMP Address Mask Reply	Info	Atomic	Original 59 signatures	Triggers when a IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 18 (Address Mask Reply).
2150 Fragmented ICMP Traffic	Attack	Atomic	Original 59 signatures	Triggers when a IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and either the more fragments flag is set to 1 (ICMP) or there is an offset indicated in the offset field.
2151 Large ICMP Traffic	Attack	Atomic	Original 59 signatures	Triggers when a IP datagram is received with the protocol field of the IP header set to 1(ICMP) and the IP length > 1024.
2154 Ping of Death Attack	Attack	Atomic	Original 59 signatures	Triggers when a IP datagram is received with the protocol field of the IP header set to 1(ICMP), the Last Fragment bit is set, and (IP offset * 8) + (IP data length) > 65535 that is to say, the IP offset (which represents the starting position of this fragment in the original packet, and which is in 8 byte units) plus the rest of the packet is greater than the maximum size for an IP packet.
3038 Fragmented NULL TCP Packet	Attack	Atomic	41 additional signatures	Triggers when a single fragmented TCP packet with none of the SYN, FIN, ACK, or RST flags set has been sent to a specific host.
3039 Fragmented Orphaned FIN Packet	Attack	Atomic	41 additional signatures	Triggers when a single fragmented orphaned TCP FIN packet is sent to a privileged port (having port number less than 1024) on a specific host.
3040 NULL TCP Packet	Attack	Atomic	Original 59 signatures	Triggers when a single TCP packet with none of the SYN, FIN, ACK, or RST flags set has been sent to a specific host.

Signature	Severity	Complexity	Timeframe	Description
3041 SYN/FIN Packet	Attack	Atomic	Original 59 signatures	Triggers when a single TCP packet with the SYN and FIN flags are set and is sent to a specific host.
3042 Orphaned Fin Packet	Attack	Atomic	Original 59 signatures	Triggers when a single orphaned TCP FIN packet is sent to a privileged port (having port number less than 1024) on a specific host.
3043 Fragmented SYN/ FIN Packet	Attack	Atomic	41 additional signatures	Triggers when a single fragmented TCP packet with the SYN and FIN flags are set and is sent to a specific host.
3050 Half-open SYN Attack	Attack	Compound	Original 59 signatures	Triggers when multiple TCP sessions have been improperly initiated on any of several well known service ports. Detection of this signature is currently limited to FTP, Telnet, WWW, SSH and E-mail servers (TCP ports 21, 23, 80, 22 and 25 respectively).
3100 Smail Attack	Attack	Compound	Original 59 signatures	Triggers on the very common smail attack against e-mail servers.
3101 Sendmail Invalid Recipient	Attack	Compound	Original 59 signatures	Triggers on any mail message with a pipe (|) symbol in the recipient field.
3102 Sendmail Invalid Sender	Attack	Compound	Original 59 signatures	Triggers on any mail message with a pipe (|) symbol in the From: field.
3103 Sendmail Reconnaissance	Attack	Compound	Original 59 signatures	Triggers when expn or vrfy commands are issued to the SMTP port.
3104 Archaic Sendmail Attacks	Attack	Compound	Original 59 signatures	Triggers when wiz or debug commands are sent to the SMTP port.
3105 Sendmail Decode Alias	Attack	Compound	Original 59 signatures	Triggers on any mail message with : decode@ in the header.
3106 Mail Spam	Attack	Compound	Original 59 signatures	Counts number of Rcpt to: lines in a single mail message and alarms after a user-definable maximum has been exceeded (default is 250).
3107 Majordomo Execute Attack	Attack	Compound	Original 59 signatures	A bug in the Majordomo program will allow remote users to execute arbitrary commands at the privilege level of the server.
3150 FTP Remote Command Execution	Attack	Compound	Original 59 signatures	Triggers when someone tries to execute the FTP SITE command.
3151 FTP SYST Command Attempt	Info	Compound	Original 59 signatures	Triggers when someone tries to execute the FTP SYST command.
3152 FTP CWD ~root	Info	Compound	Original 59 signatures	Triggers when someone tries to execute the CWD ~root command.
3153 FTP Improper Address Specified	Attack	Atomic	Original 59 signatures	Triggers if a port command is issued with an address that is not the same as the requesting host.

Signature	Severity	Complexity	Timeframe	Description
3154 FTP Improper Port Specified	Attack	Atomic	Original 59 signatures	Triggers if a port command is issued with a data port specified that is <1024 or >65535.
3215 IIS DOT DOT EXECUTE Attack	Attack	Compound	41 additional signatures	Triggers on any attempt to cause Microsoft's Internet Information Server to execute commands.
3229 Website Win-C-Sample Buffer Overflow	Attack	Compound	41 additional signatures	This signature triggers when an attempt is made to access the win-c-sample program distributed with WebSite servers.
3233 WWW count-cgi Overflow	Attack	Compound	41 additional signatures	This signature triggers when an attempt is made to overflow a buffer in the cgi Count program.
4050 UDP Bomb	Attack	Atomic	Original 59 signatures	Triggers when the UDP length specified is less than the IP length specified. This malformed packet type is associated with a denial of service attempt.
4051 Snork	Attack	Atomic	41 additional signatures	This signature triggers when a UDP packet with a source port of either 135, 7, or 19 and a destination port of 135 is detected.
4052 Chargen DoS	Attack	Atomic	41 additional signatures	This signature triggers when a UDP packet is detected with a source port of 7 and a destination port of 19.
4100 Tftp Passwd File	Attack	Compound	Original 59 signatures	Triggers on an attempt to access the passwd file via TFTP. Indicative of an attempt to gain unauthorized access to system resources.
4600 IOS UDP Bomb	Attack	Atomic	41 additional signatures	This signature triggers on receipt of improperly formed SYSLOG transmissions bound for UDP port 514.
5034 WWW IIS newdsn Attack	Attack	Compound	41 additional signatures	This signature triggers when an attempt is made to run the newdsn.exe command via the http server.
5035 HTTP cgi HylaFAX Faxsurvey	Attack	Compound	41 additional signatures	Triggers when an attempt is made to pass commands to the CGI program faxsurvey. A problem in the CGI program faxsurvey, included with the HylaFAX package from SGI, allows an attacker to execute commands on the host machine. These commands will execute at the privilege level of the HTTP server. There are no legitimate reasons to pass commands to the faxsurvey command.
5041 WWW Anyform Attack	Attack	Compound	41 additional signatures	This alarm triggers when an attacker attempts to execute arbitrary commands through the anyform cgi-bin script.
5043 WWW Cold Fusion Attack	Attack	Compound	41 additional signatures	This alarm triggers when an attempt is made to access example scripts shipped with Cold Fusion Servers.

Signature	Severity	Complexity	Timeframe	Description
5044 WWW Webcom.se Guestbook Attack	Attack	Compound	41 additional signatures	This alarm triggers when an attacker attempts to execute arbitrary commands through Webcom.se's rguest.exe or wguest.exe cgi-bin script.
5045 WWW xterm Display Attack	Attack	Compound	41 additional signatures	Triggers when any cgi-bin script attempts to execute the command xterm -display.
5050 WWW IIS .htr Overflow Attack	Attack	Compound	41 additional signatures	This signature triggers when an .htr buffer overrun attack is detected, indicating a possible attempt to execute remote commands, or cause a denial of service against the targeted Windows NT IIS server.
5055 HTTP Basic Authentication Overflow	Attack	Compound	41 additional signatures	A buffer overflow can occur on vulnerable web servers if a very large username and password combination is used with Basic Authentication.
5071 WWW msacds.dll Attack	Attack	Compound	41 additional signatures	An attempt has been made to execute commands or view secured filed, with privileged access.
5081 WWW WinNT cmd.exe Access	Attack	Atomic	41 additional signatures	Triggers when the use of the Windows NT cmd.exe is detected in a URL.
5090 WWW FrontPage htimage.exe Access	Attack	Atomic	41 additional signatures	Triggers when the FrontPage CGI program is accessed with a filename argument ending with "0,0".
5114 WWW IIS Unicode Attack	Attack	Atomic	41 additional signatures	Triggers when an attempt to exploit the Unicode ../ directory traversal vulnerability is detected.
5116 Endymion MailMan Remote Command Execution	Attack	Atomic	41 additional signatures	Endymion MailMan insecurely uses the perl function open(), which allows user-supplied input containing shell metacharacters to be executed as shell commands with the privilege level of the CGI script.
5117 phpGroupWare Remote Command Exec	Attack	Atomic	41 additional signatures	phpGroupWare is a multi-user groupware suite that is freely distributed. There exists a problem in the software could allow users to remotely execute malicious code by exploiting a vulnerable include() command.
5118 eWave ServletExec 3.0C File Upload	Attack	Atomic	41 additional signatures	UploadServlet is a servlet that ServletExec contains in its server side classes.
5123 WWW Host: Field Overflow	Attack	Atomic	41 additional signatures	This alarm will fire if web traffic is detected sending an abnormally large GET request with a large 'Host' field.
6050 DNS HINFO Request	Info	Atomic	41 additional signatures	Triggers on an attempt to access HINFO records from a DNS server.

Signature	Severity	Complexity	Timeframe	Description
6051 DNS Zone Transfer	Info	Atomic	41 additional signatures	Triggers on normal DNS zone transfers, in which the source port is 53.
6052 DNS Zone Transfer from High Port	Attack	Atomic	41 additional signatures	Triggers on an illegitimate DNS zone transfer, in which the source port is not equal to 53.
6053 DNS Request for All Records	Attack	Atomic	41 additional signatures	Triggers on a DNS request for all records.
6054 DNS Version Request	Attack	Atomic	41 additional signatures	Triggers when a request for the version of a DNS server is detected.
6055 DNS Inverse Query Buffer Overflow	Attack	Atomic	41 additional signatures	This alarm triggers when an IQUERY request arrives with a data section that is larger than 255 characters.
6056 DNS NXT Buffer Overflow	Attack	Compound	41 additional signatures	This alarm triggers when a DNS server response arrives that has a long NXT resource where the length of the resource data is > 2069 bytes OR the length of the TCP stream containing the NXT resource is > 3000 bytes.
6057 DNS SIG Buffer Overflow	Attack	Compound	41 additional signatures	This alarm triggers when a DNS server response arrives that has a long SIG resource where the length of the resource data is > 2069 bytes OR the length of the TCP stream containing the SIG resource is > 3000 bytes.
6062 DNS Authors Request	Info	Atomic	41 additional signatures	Alarms when a DNS query type TXT class CHAOS is detected with string "Authors.Bind" (case insensitive).
6063 DNS Incremental Zone Transfer	Info	Atomic	41 additional signatures	Alarms when a DNS query type of 251 is detected.
6100 RPC Port Registration	Info	Atomic[1]	Original 59 signatures	Triggers when attempts are made to register new RPC services on a target host.
6101 RPC Port Unregistration	Info	Atomic[1]	Original 59 signatures	Triggers when attempts are made to unregister existing RPC services on a target host.
6102 RPC Dump	Info	Atomic[1]	Original 59 signatures	Triggers when an RPC dump request is issued to a target host.
6103 Proxied RPC Request	Attack	Atomic[1]	Original 59 signatures	Triggers when a proxied RPC request is sent to the portmapper of a target host.
6150 ypserv Portmap Request	Info	Atomic[1]	Original 59 signatures	Triggers when a request is made to the portmapper for the YP server daemon (ypserv) port.
6151 ypbind Portmap Request	Info	Atomic[1]	Original 59 signatures	Triggers when a request is made to the portmapper for the YP bind daemon (ypbind) port.

Signature	Severity	Complexity	Timeframe	Description
6152 yppasswdd Portmap Request	Info	Atomic[1]	Original 59 signatures	Triggers when a request is made to the portmapper for the YP password daemon (yppasswdd) port.
6153 ypupdated Portmap Request	Info	Atomic[1]	Original 59 signatures	Triggers when a request is made to the portmapper for the YP update daemon (ypupdated) port.
6154 ypxfrd Portmap Request	Info	Atomic[1]	Original 59 signatures	Triggers when a request is made to the portmapper for the YP transfer daemon (ypxfrd) port.
6155 Mountd Portmap Request	Info	Atomic[1]	Original 59 signatures	Triggers when a request is made to the portmapper for the mount daemon (mountd) port.
6175 rexd Portmap Request	Info	Atomic[1]	Original 59 signatures	Triggers when a request is made to the portmapper for the remote execution daemon (rexd) port.
6180 rexd Attempt	Info	Atomic[1]	Original 59 signatures	Triggers when a call to the rexd program is made. The remote execution daemon is the server responsible for remote program execution. This may be indicative of an attempt to gain unauthorized access to system resources.
6190 statd Buffer Overflow	Attack	Atomic[1]	Original 59 signatures	Triggers when a large statd request is sent. This could be an attempt to overflow a buffer and gain access to system resources.
8000 FTP Retrieve Password File	Attack	Atomic[1]	Original 59 signatures	Triggers on string passwd issued during an FTP session. May indicate someone attempting to retrieve the password file from a machine in order to crack it and gain unauthorized access to system resources.

1. * Atomic signatures that are allocated memory for session states by Cisco IOS Firewall.

Glossary

Attack signature—A signature that detects attacks attempted into a protected network, such as denial of service attempts or the execution of illegal commands during an FTP session.

Atomic signature—Detect patterns as simple as an attempt to access a specific port on a specific host.

Compound signature—Can detect complex patterns, such as a sequence of operations distributed across multiple hosts over an arbitrary period of time.

Info signature—A signature that detects information-gathering activity, such as a port sweep.

Intrusion detection—Involves the ongoing monitoring of network traffic for potential misuse or policy violations. It matches network traffic against lists of signatures, which look for patterns of misuse.

NetRanger Director—The Director is NetRanger's graphical control interface. A single Director can manage and monitor a group of Sensors, which enables security personnel to secure a network from a centralized console.

NetRanger Sensor—The NetRanger Sensor is an intrusion detection appliance that analyzes network traffic, using signatures to search for signs of unauthorized activity.

Signature—A signature detects patterns of misuse in network traffic. In Cisco IOS IDS, signatures are categorized into four types: Info Atomic, Info Compound, Attack Atomic, or Attack Compound.

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

202822.0/ETMG 02/03

Hierarchical Navigation
Skip to Content
PRODUCTS & SERVICES
CISCO SECURITY AND VPN SOFTWARE
CISCO IDS SENSOR SOFTWARE VERSIONS AND OPTIONS
Cisco IDS Sensor Software Version 4.0
Cisco IDS Sensor Software Version 3.1
Cisco IDS Sensor Software Version 3.0
End-of-Sale Versions and Options

CISCO IDS SENSOR SOFTWARE VERSION 4.0

Partner Search: GO

Site To Search Search All Cisco.c

Toolkit: Roll over tools below
Email This Page
Glossary

Related Tools
Software Advisor
Dynamic Configuration Tool
Pricing Tool

Introduction

Cisco IDS Sensor Software Version 4.0 (Cisco IDS 4.0) is the core of the Cisco Intrusion Detection System, providing unprecedented security. It is designed to accurately identify and classify known and unknown threats targeting your network, including worms, Denial of Service, and application attacks. The first step in delivering an efficient and secure intrusion protection system is accurately detecting all possible threats. To achieve this goal, multiple detection methods are employed, thus ensuring comprehensive coverage. The methods include: stateful pattern recognition, protocol analysis, traffic anomaly detection, and protocol anomaly detection. In addition, Cisco IDS 4.0 provides the capability to prevent detected attacks from executing. And, several ease of use features are integrated to maximize efficiency.

Comprehensive Threat Protection

- **Multiple Detection Methods**--Cisco IDS uses an array of detection methods to accurately detect nearly all potential threats. Building on seven years of IDS experience, Cisco delivers a hybrid system using detection methods most appropriate for the threat including stateful pattern recognition, protocol analysis, traffic anomaly detection, and protocol anomaly detection. Cisco IDS 4.0 delivers enhancements to these detection methods, most notably in the area of protocol anomaly detection. Additionally, Cisco IDS delivers a Layer 2 signature engine to provide protection from ARP spoofing techniques in layer 2 environments. These advanced detection techniques, coupled with IP defragmentation, TCP streams reassembly, anti-IDS evasion protection, and deobfuscation techniques, provide comprehensive protection against an array to threats allowing users to quickly identify and mitigate potential damage to data or networked assets.
- **Extensive Protocol Monitoring**--Cisco IDS 4.0 can monitor all of the major TCP/IP protocols, including, but not limited to IP, Internet Control Message Protocol (ICMP), TCP, and User Datagram Protocol (UDP). It can also statefully decode application-layer protocols such as FTP, Simple Mail Transfer Protocol (SMTP), HTTP, Domain Name System (DNS), remote procedure call (RPC), NetBIOS, NNTP and Telnet.
- **Comprehensive Attack Detection**--The Cisco IDS 4.0 has the most extensive and comprehensive capability to detect attacks in all of the following categories:

- ExploitsActivity indicative of someone attempting to gain access or compromise systems on your network, such as Back Orifice, failed login attempts, and TCP hijacking
- DoSActivity indicative of someone attempting to consume bandwidth or computing resources to disrupt normal operations, such as Trinoo, TFN, and SYN floods
- ReconnaissanceActivity indicative of someone probing or mapping your network to identify "targets of opportunity," such as ping sweeps and port sweeps; usually a precursor to an actual exploit attempt
- MisuseActivity indicative of someone attempting to violate corporate policy; this can be detected by configuring the sensor to look for custom text strings in the network traffic; for example, XYZ Corporation could easily configure the Cisco IDS to send an alarm on and eliminate any connection that transmits the phrase "XYZ Confidential" in e-mail or File Transfer Protocol (FTP).

Damage Prevention

Cisco IDS uses multi-layer protection options to prevent an attack from successfully reaching the target. After the attack is accurately identified and classified, the system can stop the attack before damage occurs. Whether dropping the packet, terminating the session, reconfiguring ACLs on routers and switches, or dynamically modifying the firewall policy to "shun" the intruder, Cisco IDS offers an array of immediate response actions to stop attacks that can cost you time and money. Cisco IDS 4.0 enhances these techniques by providing added levels of granularity to the way in which these response actions can be configured by extending its capability to include shunning by source/destination port number in addition to source/destination IP address.

Ease of Use

- **Flexible Policy Language**--Because the security objectives for each IDS deployment are unique, Cisco IDS allows users to create and modify policies to specifically suit the environment in which they are deployed. Using our innovative T.A.M.E. (Threat Analysis Micro Engine) policy language, users have the flexibility to create new policies or modify existing policies to meet their unique security objectives. Since T.A.M.E. policies are decoupled from the sensing application, changes do not effect the sensor performance or reliability. Unlike other security languages that rely on simple pattern matching, Cisco T.A.M.E language allows user to leverage the underlying protocol analysis capabilities. Cisco IDS 4.0 simplifies the policy management with improved navigation allowing global changes to be implemented across categories. Additionally, Cisco IDS 4.0 now provides detailed information about the alarm trigger providing the user with forensics data and advanced

analysis data to speed the decision support process.

- **Automated Updates Streamlines Management**-- Cisco IDS Active Update technology automates the process of updating deployed sensors thus reducing the operating costs. This process provides a facility to automatically distribute new signature files and application upgrades to sensors without operator involvement. Utilizing a secure staging technique, new signature files are placed on a central server and passed to the sensor at scheduled intervals. After verifying the integrity of the package, the sensor automatically installs the update. This new capability significantly streamlines the process of regularly updating remote sensors, thereby lowering the recurring operational costs associated with this task. Additionally, users can subscribe to Cisco Active Update notification services to stay informed about breaking vulnerability news and posted countermeasures. These policy updates are developed and maintained by Cisco's Countermeasures Research Team (C-CRT). This elite team of "white hat" security professionals is dedicated to rapid response to new and evolving threats.

13.301

Technical Documentation

Quick Start

(All Cisco IDS Sensor Software Quick Start)

Quick Start Guide for the Cisco Intrusion Detection System Version 4.0

Release Notes

(All Cisco IDS Sensor Software Release Notes)

Release Notes for the Cisco Intrusion Detection System Version 4.0

CISCO INTRUSION DETECTION SYSTEM

Ease of Management

Ease of Management

Cisco provides effective security monitoring and configuration regardless of deployment size using a range of management options. All management tools are designed with an intuitive user interface, and easy navigation enabling rapid installation, configuration, and management of security events and devices.

Intuitive Event Display

- **Secure, browser-based GUI**--Alarms can be easily viewed from practically any desktop, no matter which operating system is being used on the desktop. The result is rapid access to data from systems throughout the enterprise. The familiar browser interface enhances usability. And with Secure Sockets Layer (SSL), security of data is maintained.
- **Unified, scalable view of all security events**--With the CiscoWorks VPN/Security Management Solution (CiscoWorks VMS), events from all types of security devices, including firewall, VPN, and IDS can be viewed from a single console. Multiple data sources can be supported and managed. This enhances the ability to view security across the enterprise.

Easy Alarm Processing

- **Forensic data**--With Cisco Threat Response technology, the GUI provides a view into the steps taken to investigate and confirm intrusion events. To aid in remediation of intrusions, forensic data collected by the Threat Response technology is accessible. Examples include Web logs, system logs, and other relevant data. (This capability is available only as part of a CiscoWorks VMS technology bundle.)
- **Correlation of events**--CiscoWorks VMS provides event correlation to enable improved confidence in alarm data by corroborating data from multiple security devices.
- **Network security database**--The network security database (NSDB) provides instant access to specific information about the attacks, hot links, potential countermeasures, and related vulnerabilities. Because the NSDB is an HTML database, it can be personalized for each user to include operation-specific information such as response and escalation procedures for specific attacks.

Flexible Reporting and Notification

- **Default reports**--Reporting allows the creation and viewing of reports about network activities monitored by sensors on your network. The reports include summary reports based on alarms, sources, or destinations. Because these reports are HTML based, they can be sent in e-mail messages to key administration personnel.
- **Custom reporting**--Custom reports can be created to meet the specific needs of your environment.

Simple Configuration

- **Wizard-based configuration**--Wizards guide the user through the configuration process, allowing sensors to be configured quickly and easily.
- **Automatic updates**--Automatic update capabilities maintain the effectiveness of the intrusion protection system, and simplify the regular maintenance.
- **Remote management**--Because you are not always at the same computer, or where the IDS system is located, remote access capabilities using a secure Web browser connection allow for easy remote connectivity.

Scalable Enterprise Management

- **Multi-tiered architecture**--CiscoWorks VMS promotes a three-tiered architecture providing enhanced scalability needs to enterprise security deployments.
- **Flexible device grouping**--Easily manage large IDS deployments by grouping devices by function, location, or by configuration to perform mass configuration changes.
- **Roles-based access control**--Control administrative access to ensure proper device authorization.
- **Tiered approval model (optional)**--Separate configuration definition and deployment authorities to provide proper audit and control.

For more details on the CiscoWorks VMS solution go to: http://www.cisco.com/en/US/products/sw/cscowork/ps2330/.

CHAPTER 3

IDS Device Manager Configuration Tasks

After configuring system information, you are ready to configure signatures, set up blocking, set up automatic signature updates, and restore defaults.

The following sections describe how to configure these options through the Configuration tab:

Configuring Signatures

You can create system variables, create event filters, and tune signatures through the Sensing Engine.

The following sections describe how to configure signatures through the Sensing Engine:

Explaining Signatures

Attacks or other misuses of network resources can be defined as network intrusions. Network intrusions can be detected by sensors that use a signature-based technology. A signature is a set of rules that your sensor uses to detect typical intrusive activity, such as denial of service (DoS) attacks. As sensors scan network packets, they use signatures to detect known attacks and respond with actions that you define.

The sensor compares the list of signatures with network activity. When a match is found, the sensor takes an action, such as logging the event or sending an alarm to IDS Event Viewer. Sensors allow you to modify existing signatures and define new ones.

Signature-based intrusion detection can produce false positives because certain normal network activity can be misinterpreted as malicious activity. For example, some network applications or operating systems may send out numerous ICMP messages, which a signature-based detection system might interpret as an attempt by an attacker to map out a network segment. You can minimize false positives by tuning your sensors.

To configure a sensor to monitor network traffic for a particular signature, you must enable the signature. By default, the most critical signatures are enabled when you install IDS Device Manager. When an attack is detected that matches an enabled signature, the sensor generates an alert event (formerly known as an alarm), which is stored in the sensor's event store. The alert events, as well as other events, may be retrieved from the event store by web-based clients. By

default the sensor logs all Informational alarms or higher. If you have added IDS Event Viewer as a destination, the alarm is sent to the IDS Event Viewer database and you can view the alarm in IDS Event Viewer.

Some signatures have subsignatures, that is, the signature is divided into subcategories. When you configure a subsignature, changes made to the parameters of one subsignature apply only to that subsignature. For example, if you edit signature 3050 subsignature 1 and change the severity, the severity change applies to only subsignature 1 and not to 3050 2, 3050 3, and 3050 4.

Built-in signatures are known attack signatures that are included in the sensor software and are enabled by default. You cannot add to or delete from the list of built-in attack signatures. You also cannot rename them. You can tune built-in signatures by adjusting several signature parameters. Built-in signatures that have been modified are called *tuned* signatures.

You can create new signatures, which are called *custom* signatures. Custom signature IDs begin at 20000. You can configure them for any number of things, such as matching of strings on UDP connections, tracking of network floods, and scans. Each signature is created using a signature engine specifically designed for the type of traffic being monitored.

Configuring Alarm Channel System Variables

Alarms are sent to the alarm channel, where they are filtered and aggregated. You cannot select the alarm channel, because there is only one alarm channel in version 4.0.

You can change the value of an alarm channel system variable, but you cannot add variables or delete variables. You also cannot change the name, type, or constraints of a variable.

For all the Sensing Engine panels, you must click the **Save Changes** icon on the Activity bar to apply your new configuration.

You use the system variables when configuring alarm channel event filters. When you want to use the same value within multiple filters, use a variable. When you change the value of a variable, the variables in all the filters are updated. This saves you from having to change the variable repeatedly as you configure alarm filters. See Configuring Alarm Channel Event Filters, page 3-6, for more information.

For example, if you had an IP address space that applied to your engineering group and there were no Windows systems in that group, and you were not worried about any Windows-based attacks, you could set up a USER-ADDR1 to be the engineering group's IP address space. You could then use this variable on the Event Filters page to set up the filter to ignore all Windows-based attacks for USER-ADDR1.

To define alarm channel system variables, follow these steps:

Step 1 Select **Configuration > Sensing Engine > Alarm Channel Configuration > System Variables**.

The System Variables page appears.

Figure 3-1 System Variables Page

Step 2 Select the check box next to the system variable you want to edit, and then click **Edit**.

The Editing page appears for the variable that you chose.

Note You can edit only one variable at a time. You can adjust the page view using the Rows per page list box at the bottom of the page, or you can move to additional pages of variables by selecting a page from the Page list box.

Figure 3-2 Editing Page

Step 3 Fill in the following values for the following system variables (according to the one that you are editing):

- OUT

  OUT is defined as anything that is not included in IN. You cannot edit this variable. The default is 0–255.255.255.255.

- IN

  IN is a list of all internal IP address spaces. Enter your internal IP addresses.

- DMZ1, DMZ2, and DMZ3

  You can use DMZ to define any valid IP address. These are named DMZ for you to use with filtering signatures that pertain to firewalls.

- USER-ADDRS1, USER-ADDRS2, USER-ADDRS3, USER-ADDRS4, and USER-ADDRS5

  You can use USER-ADDR to define any valid IP address. You can set up a USER-ADDR variable to apply to any group of IP addresses that you want to use a filter on.

- SIG1, SIG2, SIG3, SIG4, and SIG5

  You can use SIG to define popular signatures that you like to exclude for certain addresses.

Note To reset the form, click **Reset**.

Step 4 Click **Ok**.

Note To undo your changes, click the **Undo Changes** icon on the Activity bar.

Step 5 Click the **Save Changes** icon in the Activity bar to save your system variables.

Note A message displays "Configuration update in progress. This page will be unavailable for a few minutes." In a few minutes, click **Alarm Channel Configuration > System Variables** again to see the edited variable in the list.

The new value appears in the Value column.

Step 6 Repeat Steps 2 though 5 to edit additional system variables.

Configuring Alarm Channel Event Filters

You can configure event filters that are based on source and destination addresses for specified signatures. You can use the alarm channel system variables that you defined on the Alarm Channel System Variables page to group addresses for your filters.

For all the Sensing Engine panels, you must click the **Save Changes** icon on the Activity bar to apply your new configuration.

To configure alarm channel event filters, follow these steps:

Step 1 Select **Configuration > Sensing Engine > Alarm Channel Configuration > Event Filters**.

The Event Filters page appears.

Figure 3-3 Event Filters Page

Step 2 Click **Add** to add an event filter.

The Adding page appears.

Figure 3-4 Adding Page

Step 3 In the SIGID field, enter the signature IDs of the events to which this filter should be applied.

You can use a list (2001, 2004), or a range (2001–2004), an asterisk (*) for all signatures, or one of the SIG variables if you defined them on the Alarm Channel System Variables page.

Step 4 In the SubSig field, enter the subsignature IDs of the events to which this filter should be applied.

Step 5 In the Exception field, enter the exception (Boolean) to the event filter.

Note If the filter describes an exception to an event filter, you can create a "general case" exclusion rather than adding more specific information.

Step 6 In the SrcAddrs field, enter the source addresses of events to which this filter should be applied.

You can use one of the DMZ or USER-ADDR variables if you defined them on the Alarm Channel System Variables page.

Step 7 In the DestAddrs field, enter the destination addresses of events to which this filter should be applied.

You can use one of the DMZ or USER-ADDR variables if you defined them on the Alarm Channel System Variables page.

Note To reset the form, click **Reset**.

Step 8 Click **Apply to Sensor**.

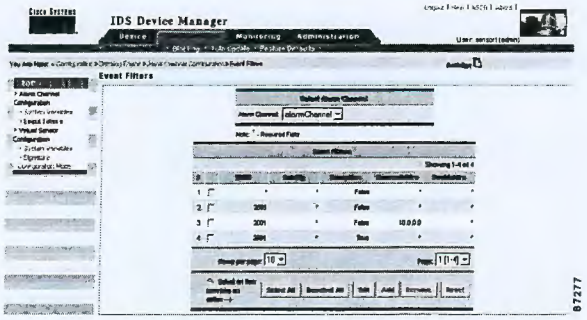
Note To undo your changes, click the **Undo Changes** icon on the Activity bar.

Step 9 Click **Saves Changes** on the Activity bar to save your changes.

Note A message displays "Configuration information is not available at this time. Try again in a few minutes." After a few minutes, click **Event Filters** again to see the filter you added.

The filtered signature appears on the Event Filters page.

Figure 3-5 Added Event Filters Page



Step 10 To remove the filter, select the check box next to the signature and click **Remove**.

Configuring Virtual Sensor System Variables

You can change the value of a system variable but you cannot add variables or delete variables. You cannot change the name or type of a variable. You cannot select the virtual sensor, because there is only one virtual sensor in version 4.0.

To configure the virtual sensor system variables, follow these steps:

Step 1 Select **Configuration > Sensing Engine > Virtual Sensor Configuration > System Variables**.

The System Variables page appears.

Figure 3-6 System Variables Page

Step 2 Select the system variable that you want to edit and click **Edit**.

The Editing page appears.

Figure 3-7 Editing Page

Step 3 Fill in the value of the system variable that you want to edit:

Note You can edit only one system variable at a time. You can adjust the page view using the Rows per page list box at the bottom of the page, or you can move to additional pages of variables by selecting a page from the Page list box.

- WEBPORTS

  WEBPORTS has a predefined set of ports where web servers are running, but you can edit the value. This variable affects all signatures that have web ports. The default is 80, 3128, 8000, 8010, 8080, 8888, 24326.

- Ports1, Ports2, Ports3, Ports4

  You can set up a list of ports to apply to particular signatures.

- ADDRS1, ADDRS2, ADDRS3, ADDRS4

  You can set up this variable with a list of addresses to use anywhere you can use IP addresses.

- IPReassembleMaxFrags

  You can define the total number of fragments you want the system to queue. You can define a number between 1000 and 50,000. The default is 10,000.

Note To reset the form, click **Reset**.

Step 4 Click **OK**.

Note To undo your changes, click the **Undo Changes** icon on the Activity bar.

Step 5 Click the **Save Changes** icon on the Activity bar to save your system variables.

Note A message displays "Configuration update in progress. This page will be unavailable for a few minutes." After a few minutes, click **Virtual Sensor Configuration > System Variables** to see the edited variable.

The new value appears in the Value column.

Step 6 Repeat Steps 2 though 5 to edit additional system variables.

Working with Virtual Sensor Signature Configuration Mode

The Signature Configuration Mode page displays a list of top level categories of signature groups for the virtual sensor. You can see all the signatures in the list or you can see signatures that are grouped according to their signature engine type. Certain signatures are enabled by default to provide you immediately with a certain level of security. When you modify a built-in signature, it becomes a tuned signature. You can also create signatures, which are called custom signatures.

You cannot select the virtual sensor, because there is only one virtual sensor in version 4.0.

You can display all individual signatures at once by clicking **All Signatures**. If you are looking for a particular signature, click **All Signatures**, and use the browser's search option to find the string you are looking for—the signature ID or the signature name.

You can display the signature list within a group by clicking the group name. Each group displays its enable level (the disabled, partially enabled, or enabled icon). You can enable or disable one, some, or all signatures within the group. To select the signature for enabling or disabling, select the signature check box.

You can tune built-in signatures. To tune a signature, select the check box and click **Edit**. Some signatures have subsignatures, which you can edit individually to have more control over the signature. You can create custom signatures, and then delete one, some, or all custom signatures. To create a custom signature, choose the correct signature engine, and then click Add and configure the signature parameters. For more information on signature engines and their parameters, see Appendix A, "Working With Signature Engines."

A signature can be in multiple groups. Editing a signature in one group, affects it in all groups. For example, if you enable all general attack signatures in the Attack category, it will enable 7107. If you disable the ATOMIC.ARP signature in the Engine category, 7107 will be disabled. Whichever action is the last one, is the one that is applied.

To configure virtual sensor signature groups, follow these steps:

Step 1 Select **Configuration > Sensing Engine > Virtual Sensor Configuration > Signature Configuration Mode**.

The Signature Groups page appears.

Figure 3-8 Signature Groups Page

Step 2 To enable or disable all signatures in a group, select the check box next to the signature group, and then click **Enable** or **Disable**.

Note A clear circle indicates that no signatures in that signature group are enabled. A solid circle indicates that all signatures are enabled. A partial circle indicates that at least one signature in that group is enabled.

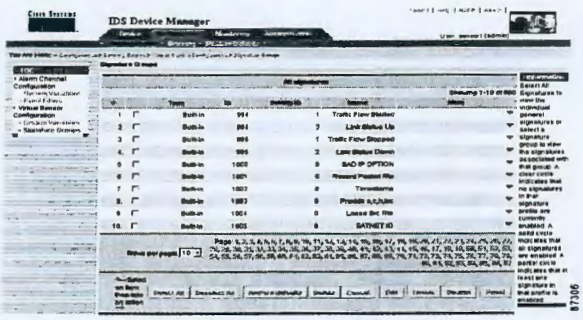
Note Click **Restore Defaults** to return the signature group to its default settings.

Step 3 You can click **All Signatures** to display all the IDS signatures or you can click a signature group name.

The All Signatures page appears.

Note If you select **All** in the Rows per page list box, it can take some time for all signatures to display.

Figure 3-9 All Signatures Page



The All Signatures page contains the following:

- Enabled or Disabled icon
- Signature ID
- Subsignature ID
- Signature name
- Type (built-in, tuned, custom)
- Severity level (Informational, Low, Medium, High)
- Action
- More (lists all the signature parameters; these appear when you edit the signature)

Step 4 Select the check box(es) next to the signatures that you want to perform an action on:

Note You can edit only one signature at a time. You can adjust the page view using the Rows per page list box at the bottom of the page, or you can move to additional pages of variables by selecting a page from the Page list box.

- To enable or disable the signature(s), click **Enable** or **Disable**.

Caution Signatures can belong to more than one group. Enabling or disabling signatures in one group also affects those signatures that belong to other groups.

- To restore the defaults to a signature(s), click **Restore Defaults**.
- To delete a signature(s), click **Delete**.

Note You cannot delete built-in or tuned signatures, only custom signatures.

- To edit the signature(s), click **Edit**.

The Editing page appears.

This is where you tune built-in signatures. You can see the definition of each parameter by passing your mouse over the parameter. Some parameters are required (red asterisk), others have menu lists you can choose from, for others you must add text. For a detailed description of signature engines and parameters, see Appendix A, "Working With Signature Engines."

Figure 3-10 Editing Page

Step 5 Click **Ok** to save the changes you made to the built-in signature.

The Type has changed from Built-in to Tuned on the All Signatures page.

Note Use the **Back** button at the bottom of the page as you tune or create multiple signatures.

Note To undo your changes, click the **Undo Changes** icon on the Activity bar.

Step 6 To create a custom signature, click the Engines category on the Signature Groups page.

Figure 3-11 Signature Groups Page

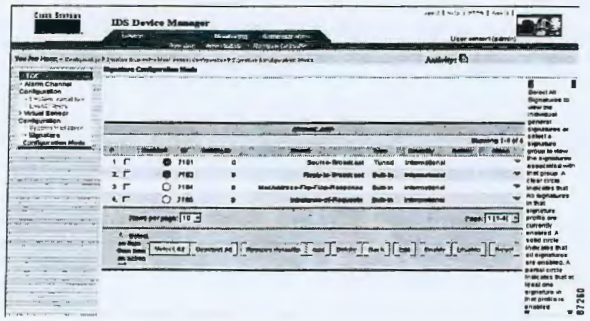
The Engines page appears.

Figure 3-12 Engines Page

Step 7 Click the engine you want to use to create a custom signature, for example, **ATOMIC.ARP**.

The ATOMIC.ARP page appears.

Figure 3-13 ATOMIC.ARP Page



Step 8 Click **Add**.

The Adding page appears.

Figure 3-14 Adding ATOMIC.ARP Page

Step 9 Fill in the parameters that you want, and then click **OK**.

Note For a detailed description of signature engines and parameters, see Appendix A, "Working With Signature Engines."

A note tells you that to add the signature you must click **Save Changes** on the Activity bar (see Step 10). The ATOMIC.ARP page appears with the custom signature in the list.

Figure 3-15 ATOMIC.ARP Page with Custom Signature

Step 10 Click the **Save Changes** icon on the Activity bar to save your changes.

Note A message displays "Configuration update in progress. This page will be unavailable for a few minutes." Click **Virtual Sensor Configuration > Signature Configuration Mode** to return to the Signature Configuration Mode page. Click **All Signatures** or the relevant signature group to see the tuned signature in the list.

The built-in signature that you edited now shows Tuned in the Type column.

Identifying Traffic Oversubscription

Signature 993 alarms tell you if the sensor is dropping packets and the percentage dropped to help you tune the traffic level you are sending to the sensor. For example, if the alarms show that there is zero or a very small percentage of dropped packets, the sensor is able to monitor the quantity of traffic being sent.

If you are seeing 993 alarms with a higher percentage of dropped packets, your sensor is oversubscribed. When a sensor gets oversubscribed, it can have difficulty in detecting alarms in TCP streams in a nonlinear fashion. The percentage of streams that are affected by the dropped packets is not easy to predict. If you find that you are operating your sensor in an environment where it is oversaturated and you need to continue operating it in that environment, we recommend disabling the TCP3WayHandshake and setting TCPReassemblyMode to loose so that best security is ensured.

Signature 993, which is part of the signature engine OTHER, has the following configuration parameters:

- MpcInterval in seconds 5 <= MpcInterval <= 2500 (default = 30).

  MpcInterval is the interval between alarms.

- MpcPercentThreshold in percent 0 <= MpcPercentThreshold <= 100 (default = 0).

  MpcPercentThreshold is the percentage of missed packets that must be exceeded to trigger an alarm. A value of 100 percent disables this threshold.

- MpcAbsThreshold in packets 0 <= MpcAbsThreshold <= 65535 (default = 0).

  MpcAbsThreshold is the absolute number of missed packets that must be exceeded to trigger an alarm. A value of 65535 disables this threshold.

If either the MpcPercentThreshold or the MpcAbsThreshold is exceeded, the alarm is triggered.

Note If signature 993 is firing with 100 percent packet loss, the sensor is not generating alarms and there is a problem. Make sure that you have the most recent version of the sensor. If you have the most recent version, contact TAC to report the problem.

See OTHER Engine, page A-30, for more information on the OTHER signature engine.

Configuring Blocking

You can configure a sensor to block an attack by generating ACL rules for publication to a Cisco IOS router, or a Catalyst 6500 family switch, or by generating shun rules on a PIX Firewall.

The following sections describe how to set up blocking:

Configuring Blocking Properties

You set up global blocking properties for the Network Access Controller (NAC) on this page. NAC is responsible for controlling blocking actions on managed devices.

To configure blocking on the sensor, follow these steps:

Step 1 Select **Configuration > Blocking Properties**.

The Blocking Properties page appears.

Figure 3-16 Blocking Properties Page

Step 2 Do not select the Allow the Sensor IP to be Blocked check box unless necessary.

Caution We suggest that you do not allow the sensor to block itself, because it will stop communicating with the managed device. You can select this option if you can ensure that if the sensor creates a rule to block its own IP address, it will not prevent the sensor from accessing the blocking device.

Step 3 In the Maximum Block Entries field, enter how many blocks are to be maintained simultaneously (0 to 250).

Note We do not recommend or support setting the maximum block entries higher than 250.

The default value is 100.

Note The number of blocks will not exceed the maximum block entries. If the maximum is reached, new blocks will not occur until existing blocks time out and are removed.

Note To reset the form, click **Reset**.

Step 4 Click **Apply to Sensor** to save your changes.

Configuring Addresses Never To Block

You must tune your sensor to identify hosts and networks that should never be blocked, not even manually, because you may have a trusted network device whose normal, expected behavior appears to be an attack. But such a device should never be blocked, and trusted, internal networks should never be blocked. Properly tuning signatures reduces the number of false positives and helps ensure proper network operations. Tuning and filtering signatures prevents alarms from being generated. If an alarm is not generated, the associated block does not occur.

If you specify a netmask, this is the netmask of the network that should never be blocked. If no netmask is specified, only the IP address you specify will never be blocked.

To set up addresses never to be blocked by blocking devices, follow these steps:

Step 1 Select **Configuration > Never Block Addresses**.

The Never Block Addresses page appears.

Figure 3-17 Never Block Addresses Page

Step 2 Click **Add** to add addresses that should never be blocked.

The Adding page appears.

Figure 3-18 Adding Page

Step 3 In the IP Address field, enter the IP address of the host that should never be blocked.

Step 4 In the Network Mask field, enter the network mask of the network that should never be blocked.

Note To reset the form, click **Reset**.

Step 5 Click **Apply to Sensor** to save your changes.

Setting Up Logical Devices

You can add logical devices that the senor will manage. For example, routers that all share the same passwords and usernames can be under one logical device name.

To set up logical devices, follow these steps:

Step 1 Select **Configuration > Logical Devices**.

The Logical Devices Configuration page appears.

Figure 3-19 Logical Device Configuration Page

Step 2 Click **Add** to add the logical devices that the sensor will manage.

The Adding page appears.

Figure 3-20 Adding Page

Step 3 In the Name field, enter the name of the logical device.

Step 4 In the Enable Password field, enter the enable password for the logical device (1 to 16 characters).

Note If there is no enable password, enter **none**.

Step 5 In the Password field, enter the Telnet or SSH password for the logical device (1 to 16 characters).

Note If there is no password, enter **none**.

Step 6 In the Username field, enter the username for the logical device.

Note If there is no username, enter **none**.

Note To reset the form, click **Reset**.

Step 7 Click **Apply to Sensor** to save your changes.

Configuring Blocking Devices

You can configure your sensor to block an attack by generating ACL rules for publication to a Cisco IOS router, or a Catalyst 6500 switch, or by generating shun rules on a PIX Firewall. The router, switch, or firewall is called a blocking device.

To configure blocking devices, follow these steps:

Step 1 Select **Configuration > Blocking Devices**.

The Blocking Devices page appears.

Caution A single sensor can manage multiple devices, but multiple sensors cannot be used to control a single device. In this case, use a master blocking sensor. See Configuring a Master Blocking Sensor, page 3-31, for more information.

Figure 3-21 Blocking Devices Page

Step 2 Click **Add** to add a blocking device.

The Adding page appears.

Figure 3-22 Adding Page

Step 3 In the IP Address field, enter the IP address of the blocking device.

Step 4 In the NAT Address field, enter the NAT address of the blocking sensor.

Step 5 Select an option from the Apply Logical Device list box.

Note The same logical device can be used for multiple blocking devices. If you do not have logical devices set up, the only option is None.

Step 6 In the Device Type field, enter the type of device that will do the blocking:

- Cisco Router
- Catalyst 6000 VACL
- PIX Firewall

Step 7 In the Enable SSH field, select the type of secure communications you want to enable between the sensor and the blocking device:

- SSH 3DES
- SSH DES
- Telnet

Note Before you can use SSH 3DES or SSH DES, you have to use the **ssh host-key** *ipaddress* to obtain the public key in the correct format so that you can add the host to the known hosts list. Refer to the *Cisco Intrusion Detection System Appliance and Module Installation and Configuration Guide Version 4.0* for the procedure.

Note To reset the form, click **Reset**.

Step 8 Click **Apply to Sensor** to save your changes.

Configuring Router Blocking Device Interfaces

You must configure the blocking interfaces on the router and specify the direction of traffic you want blocked.

To configure the blocking interfaces on a router, follow these steps:

Step 1 Select **Configuration > Router Blocking Device Interfaces**.

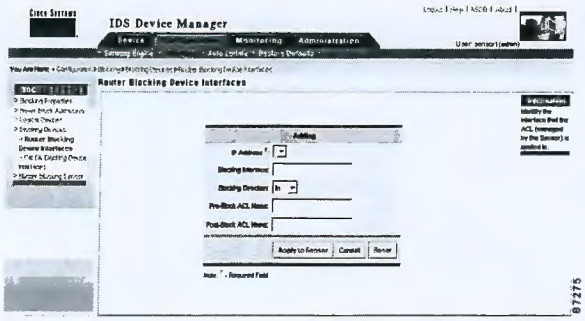
The Router Blocking Device Interfaces page appears.

Figure 3-23 Router Blocking Device Interfaces Page

Step 2 Click **Add** to configure the blocking interfaces on the router.

The Adding page appears.

Figure 3-24 Adding Panel



Step 3 In the IP Address field, enter the IP address of the router that will be used to block.

Step 4 In the Blocking Interface field, enter the interface on the router that will be used for blocking (1 to 32 characters).

Step 5 From the Blocking Direction list box, select the direction of the traffic through the interface that should be blocked (In, Out).

Step 6 In the Pre-Block ACL Name field, enter the name of the Pre-Block ACL (1 to 64 characters).

Step 7 In the Post-Block ACL Name field, enter the name of the Post-Block ACL (1 to 64 characters).

Note To reset the form, click **Reset**.

Step 8 Click **Apply to Sensor** to save your changes.

Configuring Catalyst 6K Blocking Device Interfaces

You must configure the blocking interfaces on the Catalyst switch and specify which VLAN you want blocked.

To configure the blocking interfaces on a Catalyst switch, follow these steps:

Step 1 Select **Configuration > CAT 6K Blocking Device Interfaces**.

The CAT 6K Blocking Device Interfaces page appears.

Figure 3-25 CAT 6K Blocking Device Interfaces Page

Step 2 Click **Add** to configure the blocking interfaces on the router.

The Adding page appears.

Figure 3-26 Adding Page

Step 3 In the IP Address field, enter the IP address of the Catalyst switch that will be used to block.

Step 4 In the VLAN field, enter the VLAN number that the sensor will configure for blocking.

Step 5 In the Pre-Block VACL Name field, enter the name of the Pre-Block VACL (1 to 64 characters).

Step 6 In the Post-Block VACL Name field, enter the name of the Post-Block VACL (1 to 64 characters).

Note To reset the form, click **Reset**.

Step 7 Click **Apply to Sensor** to save your changes.

Configuring a Master Blocking Sensor

Multiple sensors can forward blocking requests to a specified master blocking sensor, which controls one or more devices. The sensor that is sending its block requests to the master blocking sensor is referred to as a "blocking forwarding sensor." On the blocking forwarding sensor, you must specify which remote host serves as the master blocking sensor; on the master blocking sensor you must add the blocking forwarding sensors to its remote host configuration.

Note Only the master blocking sensor is configured to manage the network devices. The blocking forwarding sensor should not be configured to manage network devices.

See Setting Up a Blocking Forwarding Sensors, page 3-33, for the procedure to configure the blocking forwarding sensor.

To configure blocking forwarding sensors to a master blocking sensor, follow these steps:

Step 1 Select **Device > Sensor Setup > Allowed Hosts**.

The Allowed Hosts page appears.

Figure 3-27 Allowed Hosts Page

Step 2 Click **Add** to add a sensor as a blocking forwarding sensor.

The Adding page appears.

Figure 3-28 Adding Page

Step 3 In the IP Addressfield, enter the IP address of the blocking forwarding sensor.

Step 4 If you are using SSH, the port number is the same port number that the master blocking sensor is using for IDM connections.

Note For example, if you are connecting using https, it is port 443 by default.

Step 5 In the User Name field, enter your IDS Device Manager administrator username.

Step 6 In the Password field, enter your IDS Device Manager administrator password.

Step 7 If you select Use SSH, you have to use the **tls trusted-host ip-address** *ipaddress* command.

Note To reset the form, click **Reset**.

Step 8 Click **Apply to Sensor** to save your changes.

Note Repeat this procedure for each sensor you want to identify as a blocking forwarding sensor.

Setting Up a Blocking Forwarding Sensors

The blocking forwarding sensor sends block requests to the master blocking sensor. On the blocking forwarding sensor, you must specify which remote host serves as the master blocking sensor.

See Configuring a Master Blocking Sensor, page 3-31, for more information on how to set up a master blocking sensor.

To set up a blocking forwarding sensor, follow these steps:

Step 1 Select **Device > Sensor Setup > Allowed Hosts**.

The Allowed Hosts page appears.

Figure 3-29 Allowed Hosts Page

Step 2 Click **Add** to add a sensor as a master blocking sensor.

The Adding page appears.

Figure 3-30 Adding Page

Step 3 In the IP Address field, enter the IP address of the master blocking sensor.

Step 4 In the Netmask field, enter the netmask of the master blocking sensor.

Note To reset the form, click **Reset**.

Step 5 Click **Apply to Sensor** to save your changes.

The master blocking sensor is added to both the Allowed Hosts page and to the Master Blocking Sensor page.

Configuring Automatic Updates

You can configure automatic service pack and signature updates, so that when service pack and signature updates are loaded on a central FTP or SCP server, they will be downloaded and applied to your sensor. The timeout default is 5 minutes.

Note The sensor cannot automatically download service pack and signature updates from Cisco.com. You must download the service pack and signature updates from Cisco.com to your FTP or SCP server, and then configure the sensor to download them from the FTP or SCP server.

See Supported FTP Servers, page 3-37, for a list of supported servers.

To configure automatic updates, follow these steps:

Step 1 Select **Configuration > Auto Update**.

The Auto Update page appears.

Figure 3-31 Auto Update Page

Step 2 Select the Enable Auto Update check box to enable automatic updates.

Step 3 In the IP Address field, enter the IP address of the server to poll for updates.

Step 4 In the Directory field, enter the path to the directory on the server where the updates are located (1 to 128 characters).

Step 5 In the Username field, enter the username to use when logging in to the server (1 to 16 characters).

Step 6 In the Password field, enter the username password on the server (1 to 16 characters).

Step 7 In the File Copy Protocol list box, select either **SCP** or **FTP**.

Step 8 For hourly updates, select **Hourly**, and follow these steps:

a. In the Start Time field, enter the time you want the updates to start (hh:mm:ss).

b. In the Frequency field, enter the hour interval at which you want every update to occur (1 to 8760).

For example, if you enter 5, every 5 hours the sensor looks at the directory of files on the server. If there is an available update candidate, it is downloaded and installed. Only one update is installed per cycle even if there are multiple available candidates.

Step 9 For calendar updates, select **Calendar**, and follow these steps:

a. In the Start Time field, enter the time you want the updates to start (hh:mm:ss).

b. In the Day field, select the day(s) you want to download updates.

Note To reset the form, click **Reset**.

Step 10 Click **Apply to Sensor** to save your changes.

Supported FTP Servers

The following FTP servers are supported for service pack and signature updates:

- Sambar FTP Server Version 5.0 (win32).
- Web-mail Microsoft FTP Service Version 5.0 (win32).
- Serv-U FTP-Server v2.5h for WinSock (win32).
- Solaris 2.8.
- HP-UX (HP-UX qdir-5 B.10.20 A 9000/715).
- Windows 2000 (Microsoft ftp server version 5.0).
- Windows NT 4.0 (Microsoft ftp server version 3.0).

Note The sensor cannot download service pack and signature updates from Cisco.com. You must download the service pack and signature updates from Cisco.com to your FTP server, and then configure the sensor to download them from your FTP server.

Restoring Default Settings

You can restore the default configuration to your sensor.

Warning **Clicking Apply to Sensor removes the current application settings and restores the default settings. Your network settings also return to the defaults and you immediately lose connection to IDS Device Manager and the CLI.**

To restore the default configuration, follow these steps:

Step 1 Select **Device > Configuration > Restore Defaults**.

The Restore Defaults page appears.

Figure 3-32 Restore Defaults Page

Step 2 Click **Apply to Sensor** to restore the default configuration.

The IP address, netmask, default gateway, allowed hosts, password, and time will not be reset. Manual and automatic blocks also remain in effect.

CHAPTER 4

IDS Device Manager Monitoring Tasks

This chapter describes how to set up monitoring from the Monitoring tab.

This chapter contains the following sections:

Downloading IP Logs

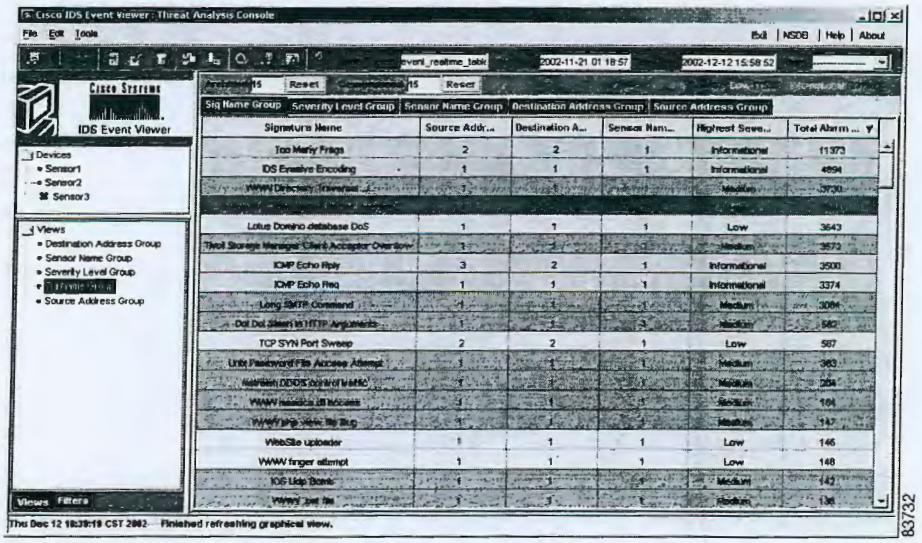
The Ip Logs page displays all IP logs that are available for downloading on the system. There is a hyperlink to each log file that is available for download. First, you have to turn on IP logging from Administration > IP Logging. The results of what you configure on that page show up in the list on the Ip Logs page. See Configuring IP Logging, page 5-5, for the procedure. You can also generate IP logs by setting a signature's EventAction to log. When the sensor detects an attack based on this signature, it automatically creates an IP log. See Configuring Signatures, page 3-1, for more information.

CHAPTER 6

IDS Event Viewer Introduction

IDS Event Viewer is a Java-based application that enables you to view and manage alarms for up to five sensors. With IDS Event Viewer you can connect to and view alarms in real time or in imported log files. You can configure filters and views to help you manage the alarms. You can also import and export event data for further analysis. IDS Event Viewer also provides access to the Network Security Database (NSDB) for signature descriptions.

Figure 6-1 IDS Event Viewer



System Requirements

IDS Event Viewer can be installed on the following platforms (English version only):

- Windows NT 4 Service Pack 6.
- Windows 2000 Service Pack 2.

IDS Event Viewer installs and uses the following support applications:

- Java 2 Runtime Environment Version 1.3.1.
- MySQL server Version 3.23.

IDS Event Viewer can be installed on a system that meets or exceeds the following minimum hardware requirements:

- Pentium III 800 Mhz or greater.
- 256 MB Ram.
- 500 MB free disk space.

Working with IDS Event Viewer

IDS Event Viewer enables you to view and manage alarm feeds from up to five sensors. The following task flow outlines the high-level tasks for configuring and working with IDS Event Viewer.

Step 1 Install and start IDS Event Viewer.

Warning **You cannot upgrade from version 3.1 to version 4.0. If you have IDS Event Viewer 3.1, you must uninstall that version before installing version 4.0.**

For more information, see the following references:

1. Installing IDS Event Viewer, page 6-4
2. Uninstalling IDS Event Viewer, page 6-5
3. Starting IDS Event Viewer, page 6-6

Step 2 Specify the devices you will monitor with IDS Event Viewer.

For more information, see the following references:

1. Adding a Device, page 6-7
2. Reviewing Device Status, page 6-10
3. Accessing the IDS Device Manager, page 6-12

Step 3 Configure filters and views to specify the alarms you want to view.

For more information, see the following references:

1. Creating a Filter, page 6-13
2. Creating a View, page 6-18

Step 4 Configure refresh cycle settings and database archival settings and verify application settings.

For more information, see the following references:

1. Configuring Refresh Cycle Settings, page 6-21
2. Configuring Data Archival Settings, page 6-23
3. Specifying Web Browser Application Location, page 6-25
4. Specifying Ethereal Application Location, page 6-27
5. Specifying NSDB Folder Location, page 6-28
6. Changing the Auto Refresh View Setting, page 6-29

Step 5 View the events and individual alarms.

For more information, see the following references:

1. Viewing Event Data, page 6-30
2. Working with Alarms, page 6-41

Step 6 Maintain the database by importing, exporting, and deleting event data.

For more information, see Database Administration, page 6-44

Installing IDS Event Viewer

The following procedure assumes that you have downloaded the IDS Event Viewer executable file to the appropriate host.

Warning **You cannot upgrade from version 3.1 to version 4.0. If you have IDS Event Viewer 3.1, you must uninstall that version before installing version 4.0. Refer to Uninstalling IDS Event Viewer, page 6-5, for more information.**

Before You Begin

You must be logged in to the host as a user with administrative privileges to install IDS Event Viewer.

To install IDS Event Viewer, follow these steps:

Step 1 Locate and double-click the IDS Event Viewer executable to start the setup program.

The Welcome panel of the IDS Event Viewer setup program appears.

Step 2 Click **Next** to proceed with the setup program.

The Select Destination Location panel appears.

Step 3 To accept the default location for the IDS Event Viewer files, click **Next**. Otherwise, click **Browse** to locate a different folder, and then click **Next**.

The Select Program Manager Group panel appears.

Step 4 Click **Next** to proceed with the setup program.

The Start Installation panel appears.

Step 5 Click **Next** to proceed with the setup program.

The Installing panel appears.

Step 6 Click **Next** to proceed with the setup program.

The Installation Complete panel appears.

Step 7 Click **Finish** to complete the IDS Event Viewer setup program.

The Install popup window appears.

Step 8 You must reboot this host to complete the IDS Event Viewer installation. Click **OK** to reboot the host.

Uninstalling IDS Event Viewer

You cannot upgrade from version 3.1 to version 4.0. Instead, you must uninstall 3.1 before installing version 4.0.

To uninstall IDS Event Viewer, follow these steps:

Step 1 Choose **Start > Programs > Cisco Systems > Cisco IDS Event Viewer > Uninstall Cisco IDS Event Viewer**.

The Select Uninstall Method panel appears.

Step 2 Select **Automatic**, and then click **Next**.

The Perform Uninstall panel appears.

Step 3 Click **Finish** to continue with the uninstallation.

If you are uninstalling 3.1, the uninstallation program does not remove the paths that were created when 3.1 was installed. To complete the uninstallation of 3.1, you must manually remove the following paths from the Windows system PATH variable:

- [*drive letter:*\...]Cisco IDS Event Viewer\MySQL\bin
- [*drive letter:*\...]Cisco IDS Event Viewer\JRE\bin
- [*drive letter:*\...]Cisco IDS Event Viewer\DataFeed\bin
- [*drive letter:*\...]Cisco IDS Event Viewer\IEV\bin
- [*drive letter:*\...]Cisco IDS Event Viewer\MySQL\lib\opt

The Cisco IDS Event Viewer and MySQL services are stopped and removed along with the entire Cisco IDS Event Viewer directory.

Starting IDS Event Viewer

Tip Ensure the Windows NT services for IDS Event Viewer are running. You can review the status of the Cisco IDS Event Viewer and MySQL services by selecting Start > Settings > Control Panel > Services.

To start IDS Event Viewer, follow these steps:

Step 1 Double-click the Cisco IDS Event Viewer shortcut on your desktop, or

Step 2 From the Windows Start menu, select **Programs > Cisco Systems > Cisco IDS Event Viewer > Cisco IDS Event Viewer**.

Specifying Devices to Monitor

IDS Event Viewer enables you to view alarms for up to five sensors at a time. To specify which five sensors IDS Event Viewer should monitor, you have to add each sensor to the Devices folder. You can later change the properties associated with a device or delete a device from IDS Event Viewer. This section includes the following procedures:

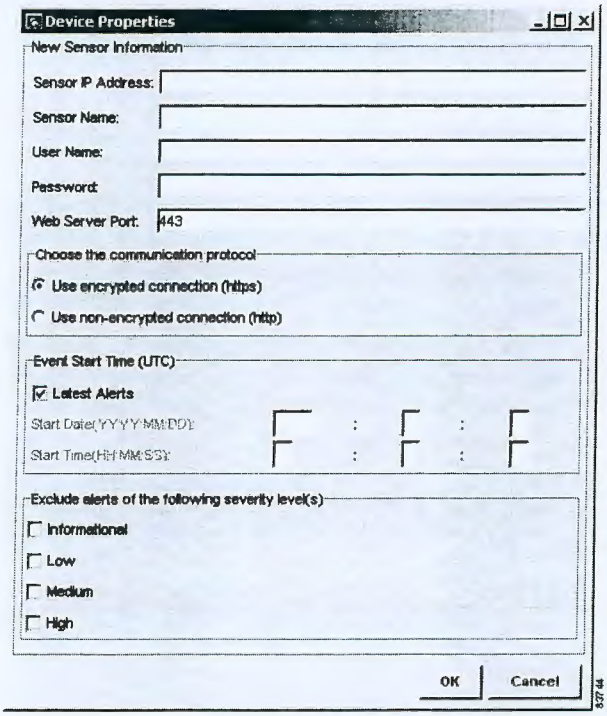
- Adding a Device, page 6-7
- Editing Device Properties, page 6-10
- Deleting a Device, page 6-10
- Reviewing Device Status, page 6-10

Adding a Device

To add a sensor to the IDS Event Viewer Devices folder, follow these steps:

Step 1 From the IDS Event Viewer main menu, select **File > New > Device.**
The Device Properties panel appears.

Figure 6-2 Device Properties



Step 2 Complete the following fields in the Device Properties panel:

- Sensor IP Address
- Sensor Name
- User Name

- Password
- Web Server Port

Note The information you provide in the Device Properties panel should match the settings you entered during initial configuration of the sensor. If you have set up a user account with Viewer access for IDS Event Viewer, specify the username and password for that account.

Step 3 To specify the communication protocol IDS Event Viewer should use when connecting to the sensor, select the **Use encrypted connection (https)** or **Use non-encrypted connection** radio button.

Step 4 To specify what alerts to pull from the sensor, follow these steps:

a. To pull the latest alerts from the sensor, select the **Latest Alerts** check box.

IDS Event Viewer will receive alerts from the sensor, beginning with the first alert the sensor receives after connecting with IDS Event Viewer.

b. To pull alerts from the sensor eventStore, deselect the **Latest Alerts** check box and specify the following:

- Start Date
- Start Time

IDS Event Viewer will receive alerts from the sensor, beginning with the first alert that matches the criteria you specified.

Step 5 To exclude alarms of a certain severity level, select one or more of the following:

- Informational
- Low
- Medium
- High

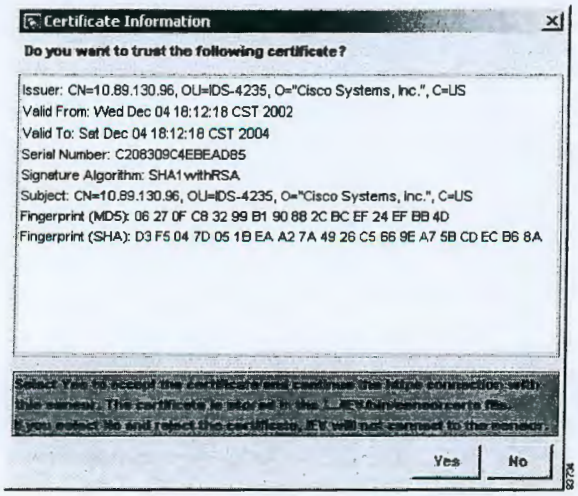
Alarms that match the severity level(s) you selected are not pulled from the sensor event store and will not appear in the Statistical Graph.

Step 6 Click **OK** to close the Device Properties panel.

IDS Event Viewer sends a subscription request to the sensor. This request remains open until you modify the device properties or delete the device.

Note If you specified https as the communication protocol, IDS Event Viewer retrieves the certificate information from the sensor and displays the Certificate Information dialog box. You must click Yes to accept the certificate and continue the https connection between IDS Event Viewer and the sensor.

Figure 6-3 Certificate Information



Step 7 Repeat Steps 1 through 3 for any additional sensors you want to monitor (up to 5).

Note If IDS Event Viewer cannot connect to the sensor, a red X appears next to the device name to indicate that no connection is present. IDS Event Viewer continues trying to connect to the sensor every 20 seconds until a connection is established or you delete the device from IDS Event Viewer.

Editing Device Properties

To edit properties for an existing device in the Devices folder, follow these steps:

Step 1 Expand the **Devices** folder to view the list of devices.

Step 2 Right-click the device you want to edit, and then click **Properties**.

The Device Properties panel appears.

Step 3 Select and edit the properties you want change, and then click **Update** to save your changes.

Deleting a Device

To delete a device from the Devices folder, follow these steps:

Step 1 Expand the **Devices** folder to view the list of devices.

Step 2 Right-click the device you want to delete, and then click **Delete Device**.

The Device Deletion Confirmation dialog box appears.

Step 3 Click **Yes** to delete the device from the Devices folder.

Reviewing Device Status

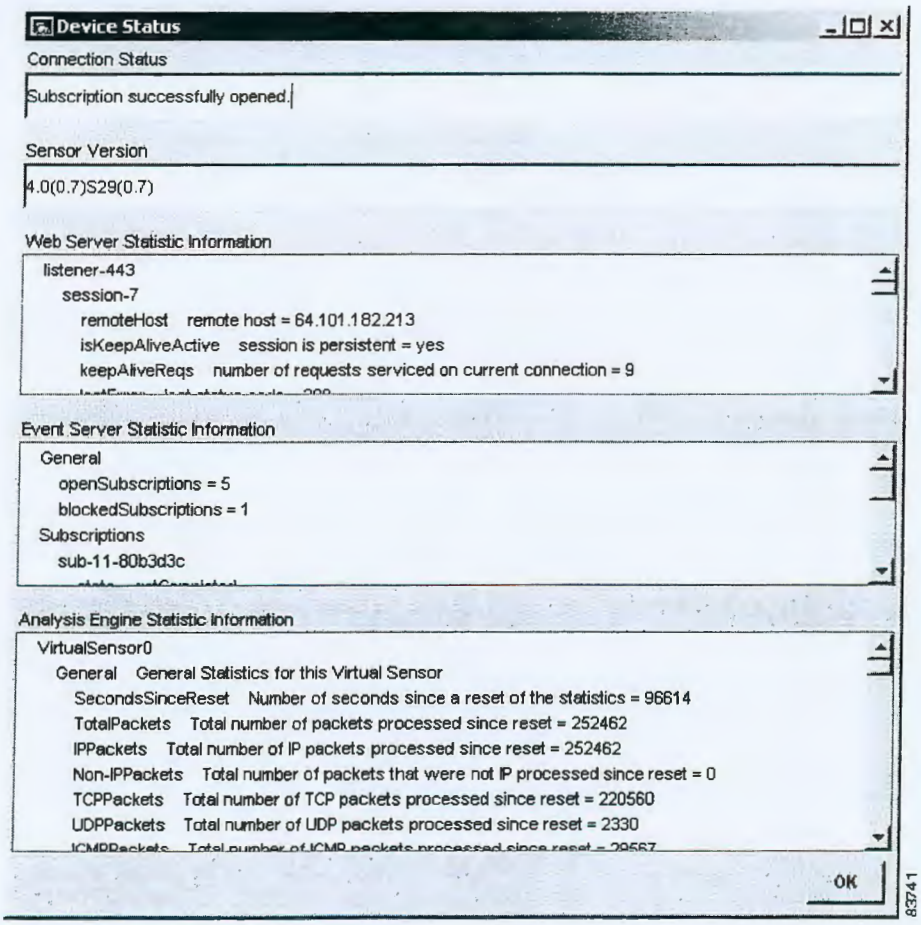
To review the version information and connection status for a device, follow these steps:

Step 1 Expand the **Devices** folder to view the list of sensors.

Step 2 Right-click the sensor for which you want to review status information, and then click **Device Status**.

The Device Status dialog box displays the Sensor Version, Device Status, Web Server Statistic Information, Event Server Statistic Information, and Analysis Engine Statistic Information.

Figure 6-4 Device Status



IDS Event Viewer will return one of the following connection status responses:

- `Subscription not open yet.`
- `Subscription successfully opened.`

- `Failed to open subscription. Check communication parameters.`
- `Network connection error. Is the web server running?`
- `Status unknown. IEV server program may not be running.`

Step 3 To close the Device Status dialog box, click **OK**.

Accessing the IDS Device Manager

You can access IDS Device Manager for a particular sensor from IDS Event Viewer.

To access IDS Device Manager, follow these steps:

Step 1 Expand the **Devices** folder to view the list of sensors.

Step 2 Double-click the sensor you want to manage.

The browser application opens and connects to the IP address for this sensor, using the port number and encryption specified in the Device Properties panel.

Configuring Filters

Filters enable you to customize and refine your view of event data by specifying alarms to exclude from your view. IDS Event Viewer ships with a default filter; however, you can create and store user-defined filters in the Filters folder. These filters can later be applied to any default or user-defined view. This section includes the following procedures:

- Creating a Filter, page 6-13
- Editing Filter Properties, page 6-16
- Deleting a Filter, page 6-17

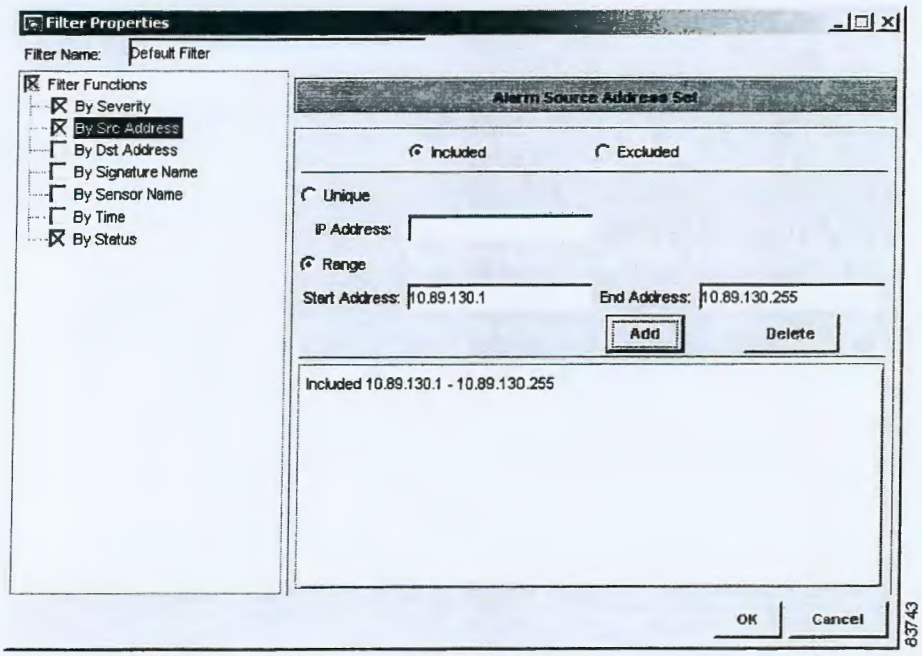
Creating a Filter

To create a filter, follow these steps:

Step 1 From the IDS Event Viewer main menu, select **File > New > Filter.**

The Filter Properties panel appears.

Figure 6-5 Filter Properties



Step 2 To name the filter, type an alpha or numeric text string (up to 64 characters) in the Filter Name field.

Step 3 To filter alarms by severity, select the **By Severity** check box under Filter Functions and select one or more of the following severity level check boxes: **Informational**, **Low**, **Medium**, or **High**.

Step 4 To filter alarms by source address or destination address, select the **By Src Address** or **By Dst Address** check box, respectively, under Filter Functions and perform the following steps:

a. To include an IP address or range, select the **Included** radio button. To exclude an IP address or range, select the **Excluded** radio button.

b. To specify a single IP address, select the **Unique** radio button, enter a valid IP address in the IP Address field, and then click **Add**.

   The IP address is added to the group of addresses excluded or included (depending on what you selected) by this filter.

c. To specify a range of IP addresses, select the **Range** radio button, enter a valid starting IP address in the Start Address field and a valid ending IP address in the End Address field, and then click **Add**.

   The IP address range is added to the group of addresses excluded or included (depending on what you selected) by this filter.

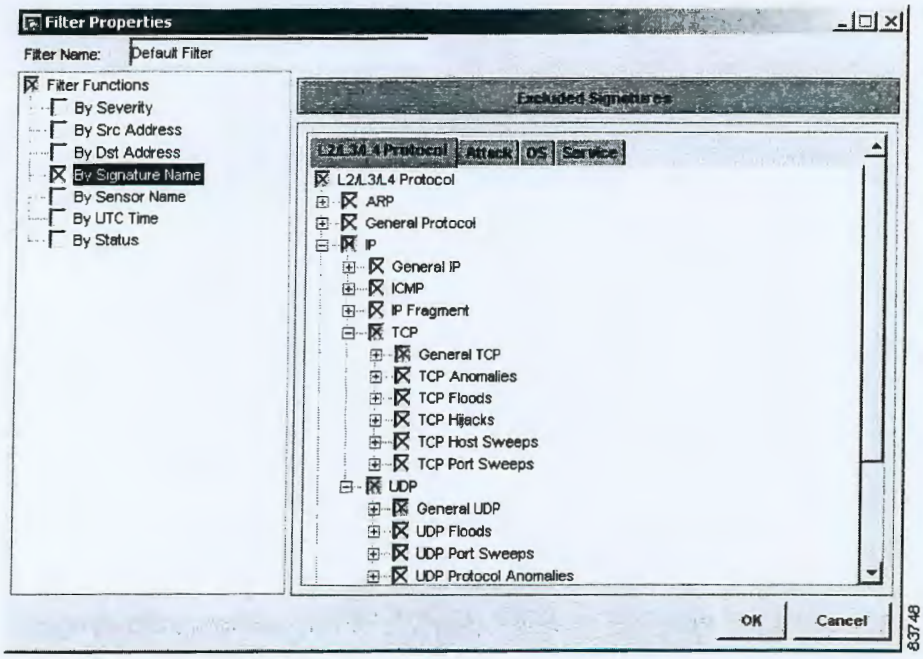
d. Repeat Step 4 to continue adding IP addresses or ranges of IP addresses.

Step 5 To filter alarms by signature name, select the **By Signature Name** check box under Filter Functions and follow these steps:

a. To locate a signature, click one of the following tabs:

- **Attack**—Identifies the attack classification categories. You can select an attack category, such as Denial of Service, to exclude all signatures contained in that category.
- **L2/L3/L4 Protocol**—Identifies the Layer 2, 3, and 4 protocol categories. You can expand each protocol category to view the individual signatures contained in that category. You can select an entire protocol category, such as UDP signatures, to exclude all signatures contained in that category.
- **OS**—Identifies the operating system categories. You can expand each operating system category to view the individual signatures contained in that category. You can select an entire operating system category, such as Windows NT, to exclude all signatures contained in that category.
- **Service**—Identifies the service categories. You can expand each service category to view the individual signatures contained in that category. You can select an entire service category, such as DNS, to exclude all signatures contained in that category.

Figure 6-6 Filter Properties



b. To exclude individual signatures, expand the appropriate signature category and select the desired signatures.

The signatures you select are excluded by this filter.

Step 6 To exclude alarms by sensor, select the **By Sensor Name** check box under Filter Functions and choose a sensor from the Devices folder.

Step 7 To exclude alarms by time and date, select the **By UTC Time** check box under Filter Functions and follow these steps:

a. Enter a valid numerical start date, beginning with the 4-digit year, and then the 2-digit month and day in the Start Date field.

b. Enter a valid start time, beginning with the 2-digit hour, and then minute and seconds in the Start Time field.

Tip 16:00:00 is the equivalent to 4:00 p.m.

c. Enter a valid numerical end date, beginning with the 4-digit year, and then the 2-digit month and day in the End Date field.

d. Enter a valid end time, beginning with the 2-digit hour, and then minute and seconds in the End Time field.

Tip 22:30:00 is the equivalent to 10:30 p.m.

e. Repeat Step 7 to add additional time periods.

Step 8 To exclude alarms by status, select the **By Status** check box under Filter Functions and select one or more of the following status level check boxes:

- New
- Acknowledged
- Assigned
- Closed
- Deleted

Step 9 To save the filter, click **OK**.

The filter is added to the Filters folder and can now be used in a view.

Editing Filter Properties

To edit the properties for an existing filter in the Filters folder, follow these steps:

Step 1 Expand the **Filters** folder to view the list of defined filters.

The Filter Properties panel appears.

Step 2 Right-click the filter you want to edit, and then click **Properties**.

Step 3 Select and edit the properties, as appropriate, listed under Filter Functions, and then click **OK**.

A dialog box appears and warns you that you are about to overwrite the existing filter with the edited filter.

Step 4 Click **Yes** to overwrite the existing filter and save your changes.

Deleting a Filter

To delete a filter from the Filters folder, follow these steps:

Step 1 Expand the **Filters** folder to view the list of defined filters.

The Filter Deletion Confirmation dialog box appears.

Step 2 Right-click the filter you want to delete, and then click **Delete Filter**.

Step 3 Click **Yes** to delete the filter from the Filters folder.

Configuring Views

Views enable you to analyze filtered event data from a specified source. IDS Event Viewer ships with five default views; however, you can use the View Wizard to create and store user-defined views in the Views folder. This section includes the following procedures:

- Creating a View, page 6-18
- Editing View Properties, page 6-20
- Deleting a View, page 6-21

Creating a View

To create a view, follow these steps:

Step 1 From the IDS Event Viewer main menu, select **File > New > View**.

The View Wizard appears.

Step 2 To name the view, enter an alpha or numeric text string (up to 64 characters) in the View Name field.

Step 3 To specify a filter, select the **Use Filter** check box and choose a filter from the list.

Step 4 To specify how alarms are grouped in the table, select a grouping style under Select the grouping style on alarm aggregation table.

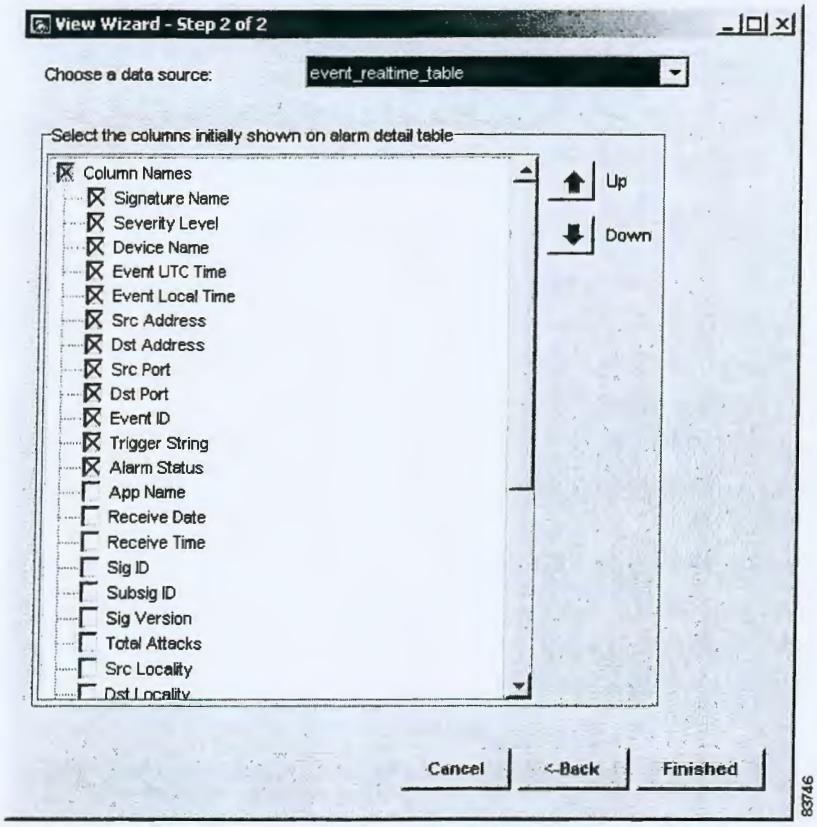
Step 5 To specify the columns that should appear in the table, select one or more check boxes under Select the columns initially shown on alarm aggregation table.

Step 6 To specify sort order for the columns, select an option from the Column Secondary Sort Order list.

Step 7 Click **Next** to advance to the final panel of the View Wizard.

The final panel of the View Wizard appears.

Figure 6-7 View Wizard



Step 8 To specify the alarms that should populate this view, select a source from the Choose a data source list box.

Note To view alarms in real time, select **event_realtime_table**. IDS Event Viewer also comes with a demo table. If the data source you want to use has not yet been established, you can select the default source (event_realtime_table) and later edit the view to associate a different data source.

Step 9 To specify the columns that should appear in the alarm detail, select one or more columns from the Select the columns initially shown on alarm detail table list. You can rearrange the order of these columns by using the Up or Down buttons.

Step 10 To save your changes and create the view, click **Finish**.

The view is added to the Views folder.

Editing View Properties

Tip If you only need to change the data source associated with this view, right-click the view and select Data Source. From the Change Data Source panel you can select a new source for the current view. For more information, see Specifying a Data Source, page 6-31.

To edit the properties for an existing view in the Views folder, follow these steps:

Step 1 Expand the **Views** folder to view the list of defined views.

The View Wizard appears.

Step 2 Right-click the view you want to edit, and then click **Properties**.

Step 3 Select and edit the view name, associated filter, grouping style, columns, or sort order. Or, click **Next** to advance to the final panel from which you can edit the data source and columns for the alarm detail.

Step 4 Click **Finish** to accept your changes.

A dialog box appears and warns you that you are about to overwrite the existing view with the edited view.

Step 5 Click **Yes** to overwrite the existing view and save your changes.

Deleting a View

To delete a view from the Views folder, follow these steps:

Step 1 Expand the **Views** folder to view the list of defined views.

The View Deletion Confirmation dialog box appears.

Step 2 Right-click the view you want to delete, and then click **Delete View**.

Step 3 Click **Yes** to delete the view from the Views folder.

Configuring Preferences

From the Edit menu, you can specify how often contents in a graph or table view are refreshed. You can also configure archival settings to optimize performance. This section includes the following procedures:

- Configuring Refresh Cycle Settings, page 6-21
- Configuring Data Archival Settings, page 6-23

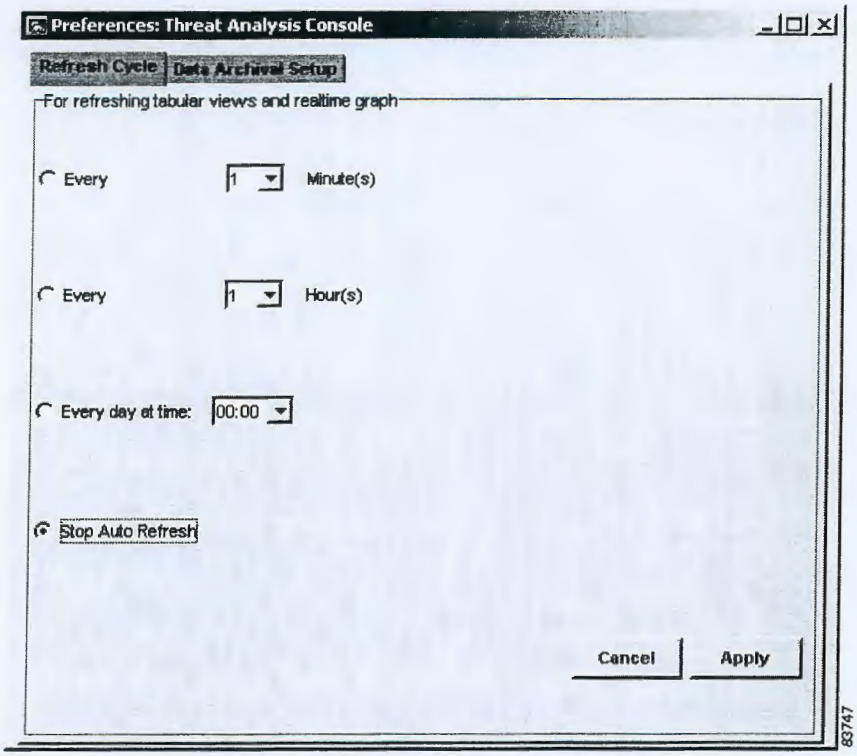
Configuring Refresh Cycle Settings

To configure the Refresh Cycle settings, follow these steps:

Step 1 From the IDS Event Viewer main menu, select **Edit > Preferences > Refresh Cycle**.

The Refresh Cycle tab of the Preferences panel appears.

Figure 6-8 Refresh Cycle



Step 2 To set the automatic refresh, perform one of the following steps:

a. To set the automatic refresh to occur every 1 to 59 minutes, select the **Every _ Minute(s)** radio button, select a time interval from the list, and then click **Apply**.

b. To set the automatic refresh to occur every 1 to 23 hours, select the **Every_ Hour(s)** radio button, select a time interval from the list, and then click **Apply**.

c. To set the automatic refresh to occur once a day, select the **Every day at time** radio button, select a specific time from the list, and then click **Apply**.

d. To stop the automatic refresh, select the **Stop Auto Refresh** radio button, and then click **Apply**.

Step 3 To close the Preferences panel, click the **Close** button.

Configuring Data Archival Settings

IDS Event Viewer includes a database archival feature that enables you to archive real-time events and ensure available disk space for incoming events. Two thresholds control the archival process. The first is a time interval and the second is a maximum number of records. Crossing either threshold triggers the archival processes.

If the time interval threshold is crossed, all records with a status matching the archival settings are moved from event_realtime_table to archive_table.timestamp. Any alarms with a status set to Deleted are deleted.

If the maximum records threshold is crossed, any alarms with a status set to Deleted are deleted from the event_realtime_table. Then, all records with a status matching the archival settings are moved from event_realtime_table to archive_table.timestamp. If, after the initial archival process, the event_realtime_table still contains more than half of the maximum number of records allowed, the archival process continues to archive and remove records (except those with a status set to New). If the number of records remaining exceeds the maximum number of records allowed, all remaining records are archived, including those with a status set to New.

To configure data archival settings, follow these steps:

Step 1 From the IDS Event Viewer main menu, select **Edit > Preferences > Data Archival Setup**.

The Data Archival Setup tab of the Preferences panel appears.

Step 2 To specify the alarms that you want to archive, select one or more of the following alarm status check boxes:

- New
- Acknowledged

- Assigned
- Closed

Step 3 To enable a time interval threshold, select **Enable time schedule for archiving events** and follow these steps:

a. To set the archival to occur every 1 to 59 minutes, select the **Every _ Minute(s)** radio button and select a time interval from the list.

b. To set the archival to occur every 1 to 23 hours, select the **Every _ Hour(s)** radio button and select a time interval from the list.

c. To set the archival to occur once a day, select the **Every day at time** radio button and select a specific time from the list.

Step 4 To specify the maximum number of real-time events to allow in the event_realtime_table, enter a numerical value (from 1000 to 1,000,000) in the **Maximum number of events in 'event_realtime_table'** field. When this threshold is met, IDS Event Viewer begins to archive events to make room for new events in the event_realtime_table.

Step 5 To specify the maximum number of archived files, enter a numerical value (from 10 to 400) in the **Maximum number of archived files** field. When this threshold is met, IDS Event Viewer begins to compress half of the oldest archived files and moves them to the compressed directory.

Step 6 To specify the maximum number of compressed archived files, enter a numerical value (from 10 to 400) in the **Maximum number of compressed archived files** field. When this threshold is met, IDS Event Viewer begins to purge half of the oldest compressed archived files.

Note To maintain available disk space for a full event_realtime_table, IDS Event Viewer purges compressed and archived files on a first-in, first-out basis until the available disk space is greater than three times the space needed.

Step 7 To save your changes, click **Apply**.

Step 8 To close the Preferences panel, click the **Close** button.

Configuring Application Settings

IDS Event Viewer relies on supporting applications to carry out database, retrieval, and communication functions. From the Edit menu, you can specify the location of these supporting applications. This section includes the following procedures:

Specifying Web Browser Application Location

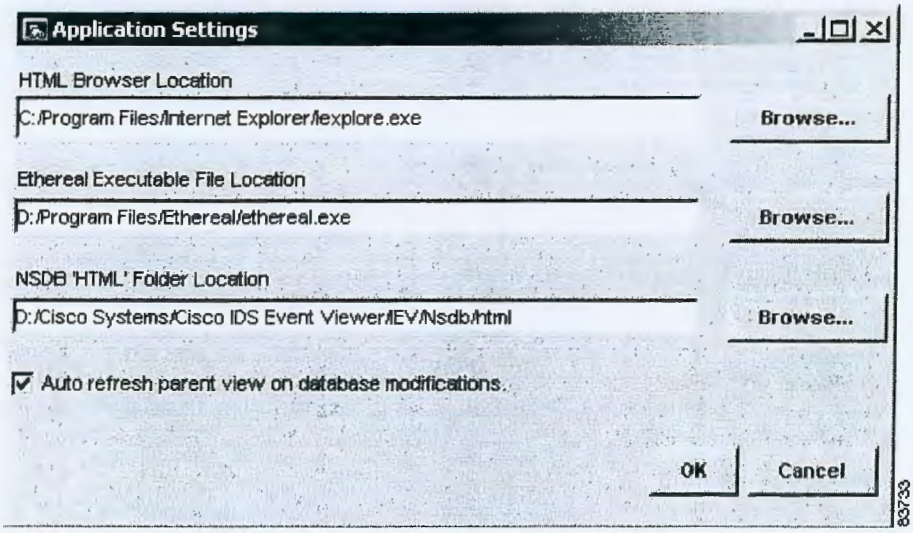
Note IDS Event Viewer detects the location of your web browser when you install IDS Event Viewer. You only need to specify the location of the browser application if you later move the Internet Explorer or Netscape executable file to a different directory.

Note IDS Event Viewer version 4.0 supports Internet Explorer versions 5.5 and later and Netscape versions 4.7 and later.

To specify the location of your browser, follow these steps:

Step 1 From the IDS Event Viewer main menu, select **Edit > Applications Settings**. The Application Settings panel appears.

Figure 6-9 Application Settings



Step 2 Enter the path, beginning with the drive letter, to the Internet Explorer or Netscape executable file in the HTML Browser Location field, or click **Browse** to locate the file.

Step 3 Click **OK** to accept your changes and close the Application Settings panel.

Specifying Ethereal Application Location

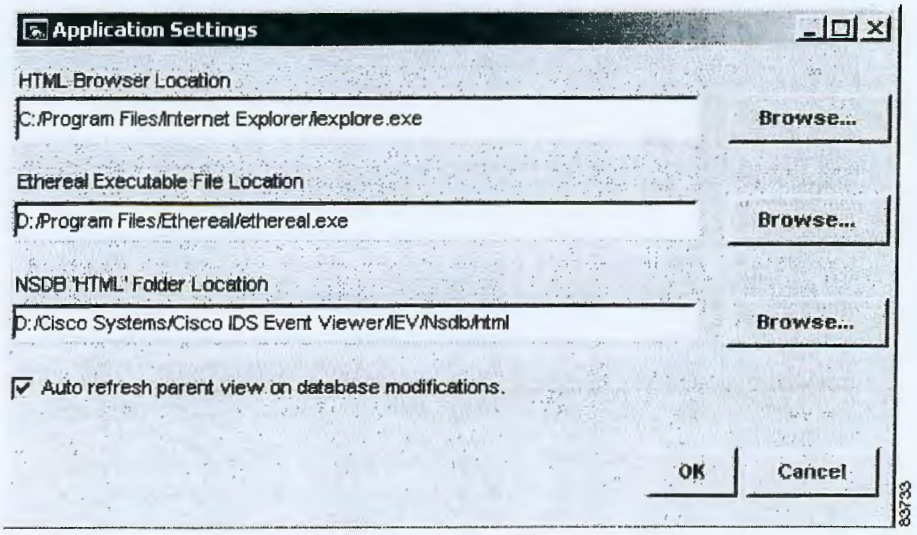
Note If Ethereal is installed on your system when you install IDS Event Viewer, IDS Event Viewer detects the location. You only need to specify the location of Ethereal if you later move the Ethereal executable file to a different directory or if you decide to install Ethereal after installing IDS Event Viewer.

To specify the location of Ethereal, follow these steps:

Step 1 From the IDS Event Viewer main menu, select **Edit > Applications Settings**.

The Application Settings panel appears.

Figure 6-10 Application Settings



Step 2 Enter the path, beginning with the drive letter, to the Ethereal executable file in the Ethereal Executable File Location field, or click **Browse** to locate the file.

Step 3 Click **OK** to accept your changes and close the Application Settings panel.

Specifying NSDB Folder Location

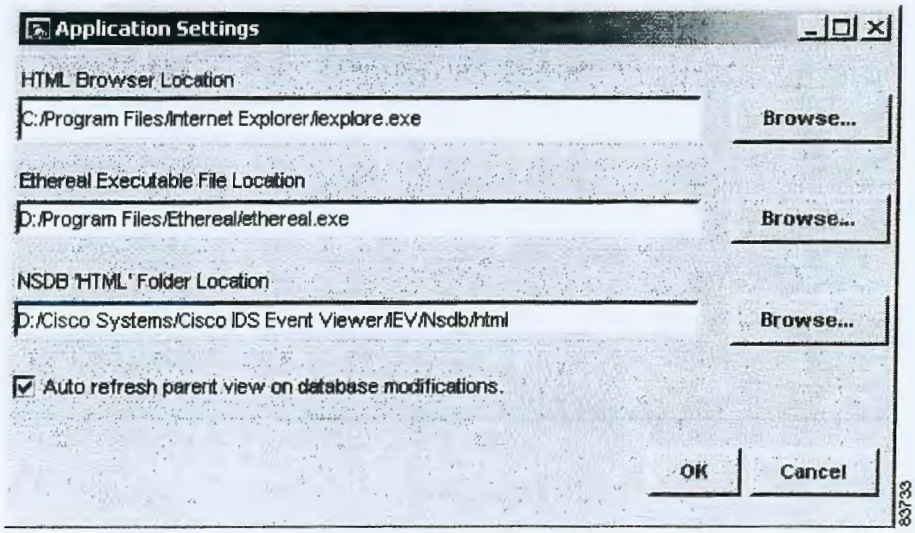
Note The NSDB is installed during IDS Event Viewer installation. You only need to specify the location of the NSDB if you have moved the NSDB HTML folder to a different directory since installing IDS Event Viewer.

To specify the location of the NSDB, follow these steps:

Step 1 From the IDS Event Viewer main menu, select **Edit > Applications Settings**.

The Application Settings panel appears.

Figure 6-11 Application Settings



Step 2 Enter the path, beginning with the drive letter, to the NSDB HTML folder in the NSDB HTML Folder Location field, or click **Browse** to locate the folder.

Step 3 Click **OK** to accept your changes and close the Application Settings panel.

Changing the Auto Refresh View Setting

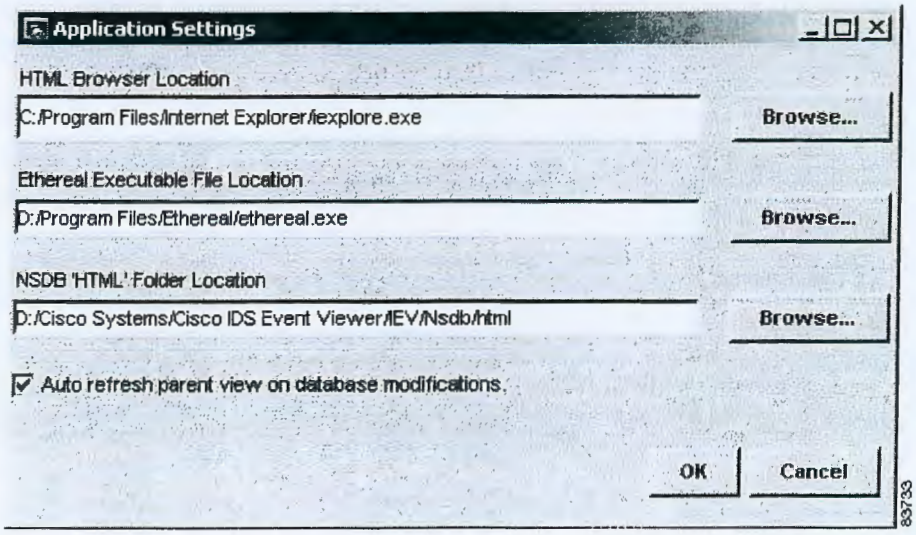
By default, if you delete a row in the Drill Down Dialog table or Expanded Details Dialog table, the aggregation table for that view is automatically refreshed to reflect the changes. However, you can change the default setting so that a change in a subordinate view is not reflected in the parent view until the next refresh cycle.

To change the auto refresh database setting, follow these steps:

Step 1 From the IDS Event Viewer main menu, select **Edit > Applications Settings**.

The Application Settings panel appears.

Figure 6-12 Application Settings



Step 2 To change the default auto refresh view setting, deselect the **Auto refresh parent view on database modifications** check box.

Step 3 Click **OK** to accept your changes and close the Application Settings panel.

Viewing Event Data

After you configure IDS Event Viewer, you can manipulate the views and tables to display event data from the sensors you are monitoring. This section includes the following introduction and procedures:

Introduction to Tables and Graphs

IDS Event Viewer enables you to access various tables and graphs that provide specialized views into the event data you are analyzing. Before you create a view and begin working with the individual tables and graphs, you should review the following descriptions.

The following tables and graph organize the events for a view. The events shown in these tables and graph differ depending on the data source you select for the view. The data source can be the event_realtime_table, archived tables, or imported log files.

- Alarm Aggregation table—The first table displayed for any view. You access an alarm aggregation table by double-clicking the view name in the Views folder.
- Expanded Details Dialog table—Displays the details of a particular event listed in an alarm aggregation table. You access the Expanded Details Dialog table by right-clicking a row in the first column of an alarm aggregation table.

- Drill Down Dialog table—Displays the individual entries for a particular column in the alarm aggregation table, such as the individual source addresses associated with a UDP Bomb event. You access the Drill Down Dialog table by double-clicking a column (except first or Total Alarm Count) in an alarm aggregation table.
- Alarm Information Dialog table—Displays the individual alarms for a particular event. You access the Alarm Information Dialog table by double-clicking the Total Alarm Count column in the alarm aggregation table, or by right-clicking the first column of the Expanded Details Dialog table.
- Statistical Graph—Displays the average number of alarms received by IDS Event Viewer, based on the filter that is applied to the data source. Therefore, depending on the filter, the Statistical Graph may not reflect the true average number of alarms. The time stamp for these events reflects the time the sensor generated the alarm.

The following table and graph organize events from a continuously running thread in IDS Event Viewer. This thread continuously monitors and aggregates the total number of alarms IDS Event Viewer receives.

- Realtime Dashboard—Displays the events, in real time, as IDS Event Viewer receives these events from the sensor(s). The most recent events appear at the top of the table. By default, the Realtime Dashboard displays the most recent events received from every device configured in IDS Event Viewer. You can configure the Realtime Dashboard to display only events from a particular device or only events of a particular severity level. You can also configure how often IDS Event Viewer should retrieve events from the sensor(s) and the maximum number of events to display.
- Realtime Graph—Displays the average number of alarms received by IDS Event Viewer. The time stamp for these events reflects the time IDS Event Viewer received the alarm, not necessarily the time the sensor generated the alarm.

Specifying a Data Source

You must associate a data source with a view to indicate the events that view should display.

To specify or change the data source associated with a view, follow these steps:

Step 1 Expand the **Views** folder to view the list of defined views.

Step 2 Right-click the view for which you want to specify a data source, and then click **Data Source**.

The Change Data Source dialog box appears.

Step 3 Select a data source from the Select the data source for current view(s) list, and then click **OK**.

If the view is open, the table automatically refreshes with events from the new data source. Otherwise, to reset the view with events from the new data source, double-click the view in the Views folder.

Viewing All Columns

You can right-click a column to hide it from the current view. You can later display all columns, including those hidden from view.

To view all columns, follow these steps:

Step 1 To view all columns for the current view, right-click a column heading and select **Show All Columns**.

The columns configured for this view are displayed.

Step 2 To hide a single column, right-click the column heading and select **Hide Column**.

Note You cannot hide the first or last column in an alarm aggregation table.

The column is hidden from the current view only. The next time you open this particular view, the column appears. If you want to permanently remove the column, edit the view properties.

Step 3 For columns that display an ellipses (...) after the column heading, click and drag the split bar that separates the columns to expand the column.

Step 4 For all columns, except the first, double-click a cell in that column to drill down and view the contents of the column.

The Drill Down Dialog appears, unless you double-click the Total Alarm Count column, in which case the Alarm Information Dialog appears.

Step 5 For cells that display an arrow (—>) after the number of occurrences, double-click that cell to display the contents of the cell.

A second table appears in the Drill Down Dialog and displays the contents of the cell. Double-clicking a cell containing an arrow (—>) in this second table displays the Alarm Information Dialog.

Sorting Data in Columns

You can sort the table data in ascending or descending order by column.

To sort data in columns, follow these steps:

Step 1 To view all columns for the current view, right-click a column heading, and then select **Show All Columns**.

Step 2 Double-click the column heading to select the column containing the data you want to sort.

An Up Arrow or Down Arrow appears, indicating the possible sort order for the column data.

Step 3 Click the arrow to sort the data in the order indicated.

Note You can only sort the table by one column at a time. Therefore, when you double-click an additional column heading, the arrow is removed from the previous column and appears next to the selected column heading.

Displaying Multiple Views

You can display multiple views at the same time. IDS Event Viewer places one view behind the other and displays a tab for each view.

To display multiple views, follow these steps:

Step 1 Expand the **Views** folder to view the list of defined views.

Step 2 To open a view, double-click the view name.

The view appears in the right view pane and displays an alarm aggregation table.

Step 3 Repeat Step 2 for each additional view that you want to open.

Step 4 To close a single view, right-click the tab for that view and select **Close***X*, where *X* stands for the name of the view.

Step 5 To close all views, right-click the tab for any view and select **Close All Views**.

All open views close.

Viewing Event Details

You can expand an event to view the details, such as signature name and severity level, associated with that event.

To view event details, follow these steps:

Step 1 Right-click a cell in the first column in an alarm aggregation table associated with the event you want to expand, and then select **Expand Whole Details**.

The Expanded Details Dialog appears with the Whole Address panel displayed.

Step 2 To view the events by address category, click the **Class A Level**, **Class B Level**, or **Class C Level** tab.

Viewing Events in a Graph

You can view events in a Realtime Graph or Statistical Graph. Each graph provides a view of the average number of alarms per minute, based on severity level. However, each graph represents a different data source and therefore a different view into the events.

The Realtime Graph is populated with events from a continuously running thread in IDS Event Viewer. This thread continuously monitors and aggregates the total number of alarms IDS Event Viewer receives. The events displayed in the Realtime Graph reflect the average number of alarms received by IDS Event Viewer. The time stamp for these events reflects the time IDS Event Viewer received the alarm, not necessarily the time the sensor generated the alarm.

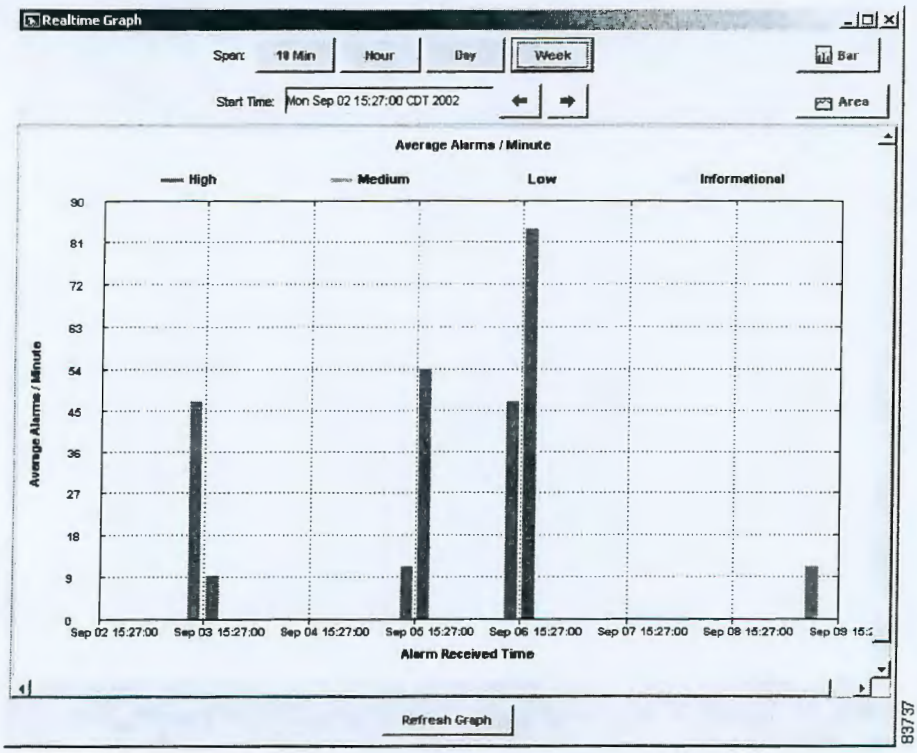
The Statistical Graph is populated with events from the data source you select. Valid data sources include the event_realtime_table, any archived table, or any imported table. The events displayed in the Statistical Graph reflect the average number of alarms received by IDS Event Viewer, based on the filter that is applied to the data source. Therefore, depending on the filter, the Statistical Graph may not reflect the true average number of alarms. The time stamp for these events reflects the time the sensor generated the alarm.

To view a graph, follow these steps:

Step 1 To view the Realtime Graph, select **Tools > Realtime Graph**.

The Realtime Graph appears.

Figure 6-13 Realtime Graph



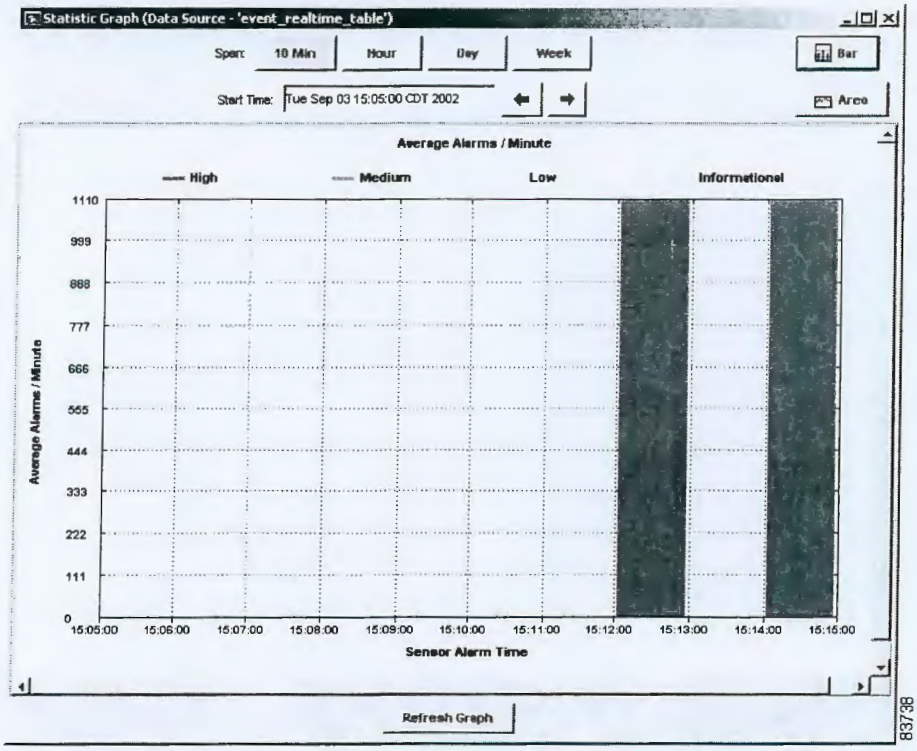
Step 2 To view the Statistical Graph, follow these steps:

a. Expand the **Views** folder and locate the view that contains the alarm data you want to display in a graph.

b. Right-click the view and select **Statistical Graph**.

IDS Event Viewer queries the data source for the selected view and calculates the average alarms per minute. The Statistical Graph appears and displays the result.

Figure 6-14 Statistical Graph



Step 3 To change the range of events displayed in the graph, follow these steps:

a. Specify the time span by which you want to advance the view.

b. To adjust the start time by the interval selected in SPAN, use the forward and backward arrows.

Step 4 To change the presentation to a bar or area graph, click **Bar** or **Area**.

Viewing Events in the Realtime Dashboard

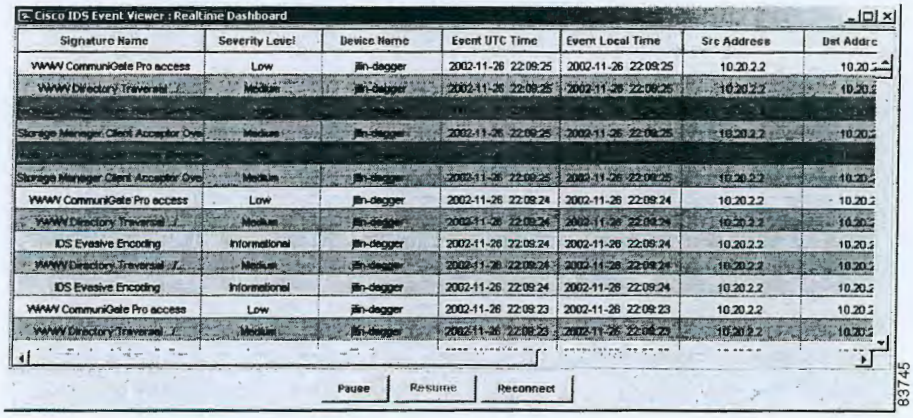
You can use the Realtime Dashboard to view a continuous stream of real-time events from the sensor.

To view events in the Realtime Dashboard, follow these steps:

Step 1 Select **Tools > Realtime Dashboard > Launch Dashboard**.

IDS Event Viewer opens a subscription request with the sensor. If the connection is successful, the Realtime Dashboard appears and displays the most recent events received by the sensor since the request was opened.

Figure 6-15 Realtime Dashboard



Step 2 To pause the stream of real-time events, click **Pause**.

IDS Event Viewer stops populating the Realtime Dashboard with events.

Step 3 To resume the stream of real-time events, click **Resume**.

IDS Event Viewer populates the Realtime Dashboard with events, beginning with the first event that was received after the stream was paused.

Step 4 To clear all existing events from the Realtime Dashboard, click **Reconnect**.

All existing events are removed from the Realtime Dashboard and IDS Event Viewer opens a new subscription with the sensor.

Configuring the Realtime Dashboard Settings

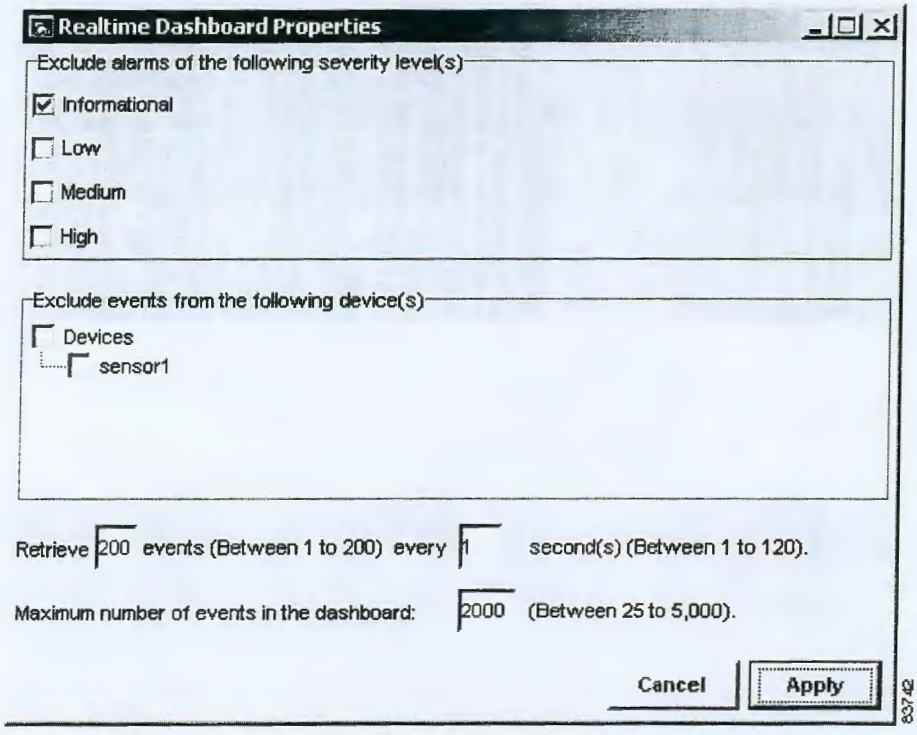
By default, the Realtime Dashboard displays the most recent events received from every device configured in IDS Event Viewer. You can configure the Realtime Dashboard to display only events from a particular device or only events of a particular severity level. You can also configure how often the Realtime Dashboard should retrieve events from the sensor(s) and the maximum number of events to display.

To configure the Realtime Dashboard settings, follow these steps:

Step 1 Select **Tools > Realtime Dashboard > Properties**.

The Realtime Dashboard Properties panel appears.

Figure 6-16 Realtime Dashboard Properties



Step 2 To exclude alarms by severity level, select one or more of the following severity levels:

- Informational
- Low
- Medium
- High

Alarms that match the severity level(s) you selected will not appear in the Realtime Dashboard.

Step 3 To exclude events from a particular device, select that device under Exclude events from the following sensor(s).

IDS Event Viewer closes any open subscriptions to this device and no events are received from the sensor.

Step 4 To configure the number of events IDS Event Viewer retrieves each second, follow these steps:

a. Specify the number of events (between 1 and 200) IDS Event Viewer should retrieve during each request.

b. Specify the number of seconds (between 1 and 120) that should elapse before IDS Event Viewer retrieves more events.

Step 5 Specify the maximum number of events to display in the Realtime Dashboard (between 25 and 5,000).

If the maximum number is reached, the oldest alarm will be removed from the Realtime Dashboard. This process will continue until the number of alarms in the Realtime Dashboard is less than the maximum number you specified.

Step 6 Click **Apply** to save your changes and close the Realtime Dashboard Properties panel.

Using Ethereal

Ethereal is a network protocol analyzer for Windows that enables you to examine data from a live network or from a captured file. You can interactively browse the captured data and view summary and detail information for each packet, including

the reconstructed stream of a TCP session. If you have Ethereal installed on the same host as IDS Event Viewer, you can start the Ethereal application from IDS Event Viewer Tools menu and view IP log files.

Working with Alarms

After you know how to manipulate views and tables to display the event data you are interested in, you can begin to manage individual alarms within those events. This task includes setting a status for alarms you have reviewed, adding notes to an alarm you want to track, or reviewing detailed alarm and signature information.

Viewing Individual Alarms

You can view individual alarms associated with an event.

To view individual alarms, follow these steps:

Step 1 To view alarms from an alarm aggregation table, follow these steps:

a. Expand the event details for the event containing the alarm you want to view.

The Expanded Details Dialog appears.

b. Right-click a row in the Expanded Details Dialog, and then select **View Alarms**.

The Alarm Information Dialog appears.

Step 2 To view alarms from any table, follow these steps:

a. Scroll to locate the Total Alarm Count column.

b. Double-click the cell containing the alarms you want to view in the Total Alarm Count column.

The Alarm Information Dialog appears.

Setting the Alarm Status

You can associate a status with the alarm, indicating what action should be taken by IDS Event Viewer (for alarms marked Deleted or during alarm archival) or by someone else in your organization.

Tip You can right-click a cell in the first column of an alarm aggregation table and change the status for all alarms in that cell. This is useful for deleting several alarms at the same time.

To set the status for an alarm, follow these steps:

Step 1 Locate the alarm for which you want to set a status.

Step 2 To set the status for that alarm, follow these steps:

a. Right-click the alarm and select **Set Status To**.

b. Select one of the following:

- New
- Acknowledged
- Assigned
- Closed
- Deleted

c. Select the status in the Alarm Status column and select a status from the list.

Adding Notes to an Alarm

You can add notes (up to 255 characters) to an alarm entry and store these notes as part of the alarm entry in the database.

To add notes to an alarm, follow these steps:

Step 1 Locate the alarm to which you want to add notes.

Step 2 Scroll to the Notes column.

Step 3 Double-click the cell in the Notes column for the alarm you want to add notes to.

The cell becomes active and a cursor appears.

Step 4 Type the notes you want to store with this particular alarm, and then press **Enter**.

Show Alarm Context

Certain alarms may have context data associated with them. Context data provides a snapshot of the incoming and outgoing binary TCP traffic (up to 256 bytes in both directions) that preceded the triggering of the signature.

To view the context for an alarm, follow these steps:

Step 1 From the Alarm Information Dialog or Realtime Dashboard, right-click a cell in the Context column, and then select **Show Context**.

The Decoded Alarm Context panel appears.

Show Attack Details

Certain attacks, such as sweep attacks, affect multiple victims or are the result of multiple attackers. The alarms generated from these attacks contain summary details of the attack.

To view the attack details for an alarm, follow these steps:

Step 1 From the Alarm Information Dialog or Realtime Dashboard, right-click the alarm, and then select **Show Attack Details**.

The Summary Attack Details panel appears.

Accessing the NSDB

The NSDB is a repository of information for individual signatures, including signature id, type, structure, and description.

To access the NSDB, perform one of the following steps:

Step 1 From the Expanded Details Dialog, right-click any column and then select **NSDB Link**.

or

Step 2 From the Alarm Information Dialog, right-click any column and then select **NSDB Link**.

or

Step 3 From the Drill Down Dialog, right-click a cell in the first column and then select **NSDB Link**.

or

Step 4 Select **Tools > NSDB Link**.

Database Administration

Database administration is essential to maintaining the integrity of IDS Event Viewer. Database administration includes routinely importing, exporting, and deleting event data. This section includes the following procedures:

- Importing Log Files, page 6-45
- Exporting Tables, page 6-47

- Deleting Tables from Data Source, page 6-48
- Deleting Alarms, page 6-49

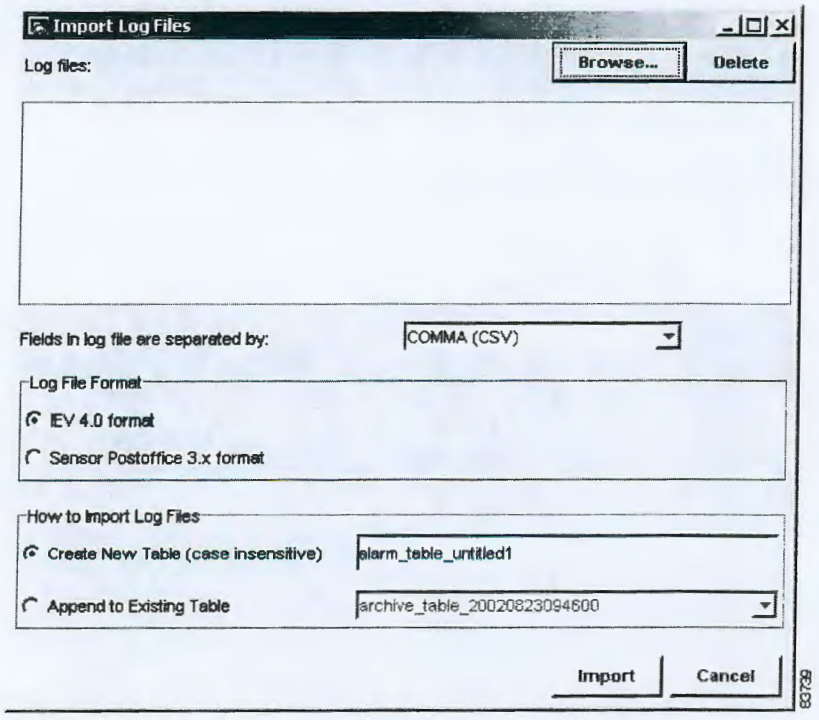
Importing Log Files

To import a log file, follow these steps:

Step 1 From the IDS Event Viewer main menu, select **File > Database Administration > Import Log Files.**

The Import Log Files panel appears.

Figure 6-17 Import Log Files



Step 2 Click **Browse** to locate the file you want to import.

Step 3 To specify how the data fields are separated, select **Comma (CSV)** or **Tab** from the Fields in log file are separated by list box.

Step 4 To specify the format of the file you want to import, select the **IEV 4.0 format** or **Sensor Postoffice 3.x format** radio button under Log File Format.

Note Log files with the Sensor Postoffice 3.x format are converted to IEV 4.0 format upon import.

Step 5 To import the log file information into a new table, follow these steps:

a. Select the **Create New Table** radio button under How to Import Log Files.

b. Type a valid name for the table.

Step 6 To import the log file information into an existing table, follow these steps:

a. Select the **Append to Existing Table** radio button under How to Import Log Files.

b. Select an existing table from the list box.

Step 7 To import the log file, click **Import**.

Depending on the option you chose, either the log file is appended to an existing table or a table is created. You can then select this table as the data source for a particular view and view the alarms in the log file.

Exporting Tables

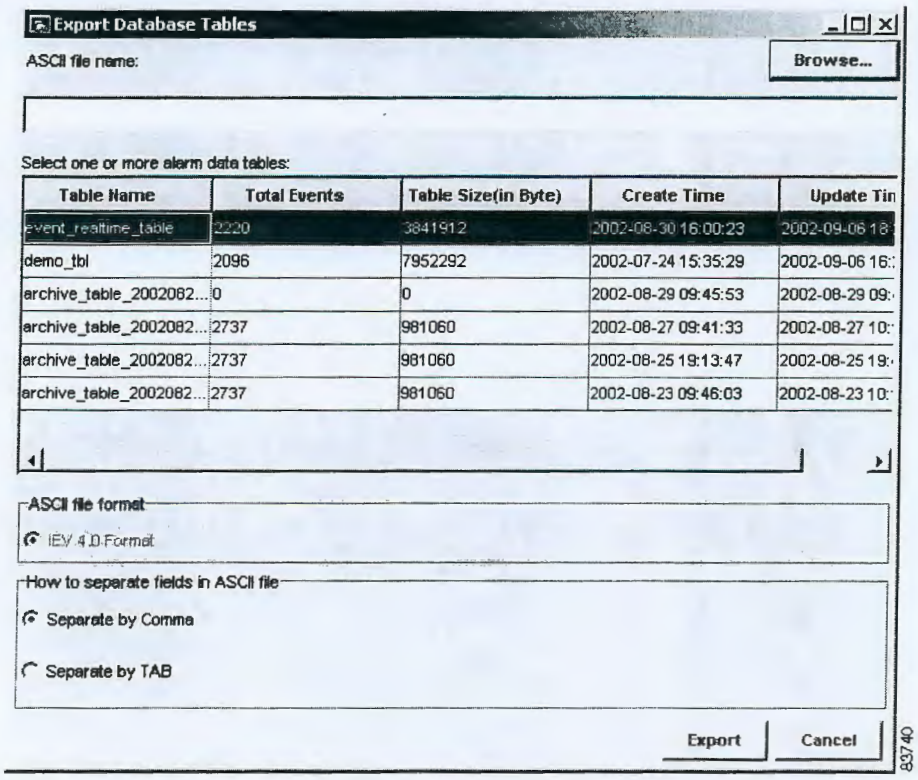
You can export data from the IDS Event Viewer tables to an ASCII file.

To export a table, follow these steps:

Step 1 From the IDS Event Viewer main menu, select **File > Database Administration > Export Tables**.

The Export Database Tables panel appears.

Figure 6-18 Export Database Tables



Step 2 To specify where to store the exported table, click **Browse** and choose a directory for the file.

Step 3 To name the exported file, enter a name in the ASCII file name field.

Step 4 Select the tables to export to the ASCII file. To select multiple tables, hold down the **Ctrl** key and click the names of the tables you want to include.

Note By default, tables are exported in the IEV 4.0 Format. This option appears dimmed.

Step 5 To specify how the table fields should be separated in ASCII format, select the **Separate by Comma** or **Separate by TAB** radio button under How to separate fields in ASCII file.

Step 6 To export the tables, click **Export**.

Deleting Tables from Data Source

You can delete an existing table from the list of available data sources for a view.

To delete a table from the data source repository, follow these steps:

Step 1 From the IDS Event Viewer main menu, select **File > Database Administration > Data Source Information**.

The Data Source Information panel appears.

Step 2 Select the row corresponding to the table you want to delete, and then click **Delete Tables**.

The Table Deletion Confirmation dialog box appears.

Step 3 Click **Yes** to remove the table from the data source repository.

Deleting Alarms

To delete alarms from a data source, follow these steps:

Step 1 To delete alarms with a status set to Deleted, follow these steps:

a. Verify that you have set the status of all the alarms you want to delete to Deleted.

b. From the IDS Event Viewer main menu, select **File > Database Administration > Data Source Information**.

The Data Source Information panel appears.

c. Select the row corresponding to the table containing the alarms you want to delete, and then click **Purge Tables**.

Alarms with a status set to Deleted are removed from the table.

Step 2 To delete all alarms from a table associated with an open view, right-click the tab for the view and select **Set All Status to Deleted and Purge**.

The status of all alarms in that table is set to Deleted and the table content is purged.

Step 3 To delete a single row from a table associated with an open view, select the row(s) you want to delete and then right-click the first column of the table and select **Delete Row (s) from Database**.

Note You can delete a single row from an Alarm Aggregation table, the Expanded Details Dialog table, or the Drill Down Dialog table.

CHAPTER 1

Overview

This quick start guide presents the requirements and procedures for installing and configuring select components of the CiscoWorks VPN/Security Management Solution (VMS) 2.1. This guide focuses on three components:

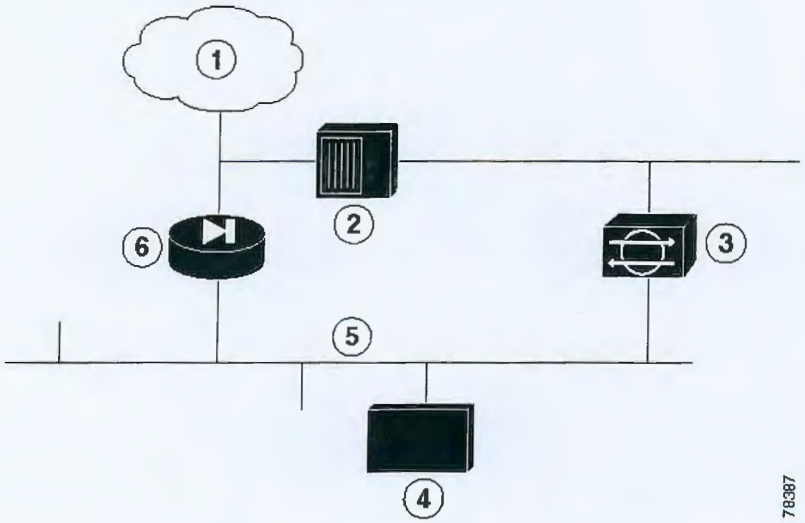
- Management Center for PIX Firewalls (PIX MC)
- Management Center for IDS Sensors (IDS MC)
- Monitoring Center for Security (Security Monitor)

Note This guide contains quick start installation instructions for evaluating these three components on a lab or small network. For custom installation instructions, see the installation guides available in PDF in the Documentation directory on the product CDs. To read the PDF files, you must have Adobe Acrobat Reader 4.0 installed.

For deployment guidelines in a larger production environment, see the *CiscoWorks VPN/Security Management Solution Deployment Guide*.

This guide assumes you are working with a simple lab or small network that includes a PIX Firewall and IDS Sensor, and one CiscoWorks2000 Server running the Management Centers, as depicted in Figure 1-1.

Figure 1-1 Simple Lab Network Example



1	*Outside network*, or untrusted network, from which you are protecting the inside network.
2	*Hub* to which the monitoring interface of the IDS Sensor is attached.
3	*Cisco Secure IDS Sensor* that monitors the traffic on the outside network.
4	*CiscoWorks2000 Server* running the PIX MC, IDS MC, and Security Monitor, which are used to manage and monitor the IDS Sensor and PIX Firewall.
5	*Inside network*, or trusted network, that you are protecting from users on the outside network.
6	*PIX Firewall* that filters traffic between the inside and outside networks.

This chapter contains the following sections:

About the VMS Bundle

CiscoWorks VPN/Security Management Solution (VMS), an integral part of the SAFE Blueprint, combines web-based tools for configuring, monitoring and troubleshooting enterprise Virtual Private Networks (VPNs), firewalls, and network-based and host-based intrusion detection systems (IDS). VMS delivers the industry's first robust and scalable architecture and feature set that addresses the needs of small and large-scale VPN and security deployments.

What's New?

VMS 2.1 includes four new security management and monitoring center modules:

- Management Center for PIX Firewalls (PIX MC)
- Management Center for IDS Sensors (IDS MC)
- Monitoring Center for Security (Security Monitor)
- Management Center for VPN Routers (Router MC)

In addition, the CSPM, Cisco IDS Host Sensor and Console, VPN Monitor, CD One, and Essentials modules include updates.

The following VMS 2.1 features improve scalability and ease-of-use for security management and monitoring center modules:

- A common architecture that provides a consistent user experience—including common user interfaces, workflows, user roles, platforms, installation, and administer authentication based on a common Cisco Secure ACS server.
- A new scalability feature, Auto Update, that allows numerous PIX Firewalls to be updated easily and quickly. Auto Update enables devices, even those remote devices with dynamic IP addresses, to check periodically with an update server and download the most up-to-date security policies.
- Smart Rules Hierarchy enables administrators to define device groups and to implement policy inheritance, which enables policies to be replicated quickly to across multiple devices.

- Command and Control Workflow enables separate groups control over network and security operations and provides distinct audit trails.
- Role-Based Access Control enables organizations to offer different groups unique access rights to different devices and applications.

VMS 2.1 Bundle Contents

VMS 2.1 contains the *VPN/Security Management Solution 2.1 Bundle Update*, the *Quick Start Guide for the VPN/Security Management Solution 2.1*, and the following seven sub-boxes:

- **Cisco Secure Policy Manager**—Contains the Cisco Secure Policy Manager for Firewalls and VPNs 3.1 CD.
- **Cisco IDS Host Sensor and Console**—Contains the IDS Host Sensor and Console 2.5 CD.
- **CiscoWorks Common Services**—Contains the Common Services 1.0 CD.
- **CiscoWorks Security Management Centers**—Contains the Management Center for PIX Firewalls 1.0, Auto Update Server 1.0, Monitoring Center for Security and Management Center for IDS Sensors 1.0, and Management Center for VPN Routers 1.0 CDs.
- **CiscoWorks VPN Monitor**—Contains the VPN Monitor 1.2 for Windows and Solaris CDs.
- **CiscoWorks CD One**—Contains the CD One 5th Edition for Windows and Solaris CDs.
- **CiscoWorks Resource Manger Essentials**—Contains the Resource Manager Essentials 3.4 for Windows and Solaris CDs.

The following table provides information about the product CDs and lists the associated content for each CD. For the complete list of paper and online documentation, see Documentation Roadmap, page xiii.

Product CD	Enables you to....	Associated content....
Management Center for PIX Firewalls 1.0	Configure PIX Firewalls.	• PIX MC product CD • Printed documentation – Release Notes
Management Center for IDS Sensors 1.0 and Monitoring Center for Security 1.0	• Configure network-based IDS Sensors. • Monitor network-based and host-based IDS events and IOS and PIX Firewall syslogs.	• IDS MC and Security Monitor product CDs • Printed documentation – Release Notes
Management Center for VPN Routers 1.0	Configure VPN routers.	• Router MC product CD • Printed documentation – Release Notes
Auto Update Server 1.0	Pull configurations from update server.	• AUS product CD • Printed Documentation – Release Notes
CiscoWorks Common Services 1.0	Provide common software and services for the Management Centers.	• CiscoWorks Common Services product CD • Printed Documentation – *Registration and Licensing Notes for Common Services* – Release Notes
Cisco Secure Policy Manager 3.1	Configure PIX Firewalls, IOS firewalls, and VPNs.	• CSPM product CD • Printed Documentation – Release Notes • CSPM License Disk—Provides the license to use CSPM. For information about the number of supported devices, see the device license label on the disk.

Product CD	Enables you to....	Associated content....
IDS Host Sensor and Console 2.5	Configure host-based IDS to protect critical servers.	• Cisco IDS Host Sensor product CD • Printed documentation – *Cisco Intrusion Detection System Host Sensor Registration* – Release Notes
VPN Monitor 1.2	Monitor IPSec-based, site-to-site and remote access VPNs.	• VPN Monitor product CD • Printed documentation – Release Notes
Resource Manager Essentials 3.4	Use operational management, such as software distribution, change audit, and syslog analysis.	• Essentials product CD • Printed documentation – Release Notes
CD One, 5th Edition (CiscoView)	Use CiscoView for graphical device management.	• CD One product CD • Printed documentation – Release Notes

Note CiscoWorks Common Services, CSPM, IDS MC, Security Monitor, Router MC, AUS, and PIX MC can be installed only on Windows 2000. The Cisco IDS Host Sensor Console can be installed on Windows 2000 and Windows NT servers. The Cisco IDS Host evaluation Agents can be installed on Windows 2000, Windows NT, and Solaris.

CHAPTER 2

VMS Bundle Component Installation

This chapter describes the system requirements and procedures for installing CiscoWorks Common Services, Management Center for PIX Firewalls (PIX MC), Management Center for IDS Sensors (IDS MC), and Monitoring Center for Security (Security Monitor). It also includes procedures to verify that you successfully installed the components.

System Requirements

CiscoWorks Common Services, PIX MC, IDS MC, and Security Monitor are components of the VPN/Security Management Solution (VMS).

You can install VMS CDs on Windows 2000. Table 2-1 shows VMS server requirements for Windows 2000 systems.

Table 2-1 Server Requirements

System Component	Requirement
Hardware	• IBM PC-compatible with a CD-ROM drive • Color monitor with video card capable of 16-bit colors
Processor	Pentium, 1 GHz, minimum

Table 2-1 Server Requirements (continued)

System Component	Requirement
Operating System	You must have one of the following operating systems: • Windows 2000 Server, Service Pack 2 or Service Pack 3 • Windows 2000 Professional, Service Pack 2 or Service Pack 3 **Note** CiscoWorks Common Services has not been tested with any other Windows or Windows 2000 operating system or service pack; therefore, installing CiscoWorks Common Services on any other operating system is not supported.
File System	NTFS
Memory	1 Gigabyte, minimum
Virtual Memory	2 Gigabytes, minimum
Hard Drive Space	9 Gigabytes of free hard drive space, minimum **Note** The actual amount of hard drive space required depends upon the number of CiscoWorks Common Services client applications you are installing and the number of devices you are managing with the client applications.

Additionally, you should not install CiscoWorks Common Services on a Windows server that is running any of the following services:

- Primary domain controller
- Backup domain controller
- Terminal server

You can access all product features from a client that fulfills the hardware, software, and browser requirements. Table 2-2 shows client hardware and software requirements.

Table 2-2 Client Hardware and Software Requirements

System Component	Requirement
Hardware/Software	IBM PC-compatible computer with 300 MHz or faster Pentium processor running one of the following: • Windows 98 • Windows NT 4.0 Workstation • Windows NT 4.0 Server • Windows 2000 Advanced Server • Windows 2000 Server or Professional Edition with Service Pack 2 or Service Pack 3 • Solaris SPARCstation or Sun Ultra 10 with a 333MHz processor running one of the following operating systems: – Solaris 2.7 – Solaris 2.8
Hard Drive Space	• 400 MB virtual memory (for Windows) • 512 MB swap space (for Solaris)
Memory	256 MB, minimum
Web Browser	You must also install one of the following HTML browsers: • Microsoft Internet Explorer 6.0 or 5.5 with Service Pack 2, and Java Virtual Machine (JVM) 5.00.3186 or later. **Note** PIX MC, Auto Update Server, and Router MC run only on Internet Explorer version 6.0 or 5.5 with Service Pack 2, and Java Virtual Machine (JVM) 5.00.3186 or later. • Netscape Navigator 4.79 (for Windows). • Netscape Navigator 4.76 (for Solaris).

Note CiscoWorks Common Services requires the Java Plugin from Sun Microsystems Java Runtime Environment (JRE) 1.3.1. CiscoWorks Common Services is not compatible with Java Plugin from JRE versions 1.2.x, 1.4.x, or any maintenance releases of JRE 1.3.1 (such as 1.3.1_01, 1.3.1_02, and so on). If the required JRE is not present on the client system, CiscoWorks Common Services downloads and installs it automatically; you do not need to install the JRE before accessing CiscoWorks Common Services. However, if an incompatible version of the JRE is present on the client system, you must remove it before accessing CiscoWorks Common Services. If you do not, some features of CiscoWorks Common Services may not function properly.

Installation Sequence

Complete the following tasks to install CiscoWorks Common Services, PIX MC, IDS MC, and/or Security Monitor.

Step 1 Bootstrap the managed devices.

Ensure that any supported devices you plan to manage, including PIX Firewalls and sensors, are installed on your network and that you can Telnet from the server to the managed device.

For more information, see Appendix A, "Network Device Preparation."

Step 2 Prepare the server and client systems.

Ensure that the server(s) on which you plan to install VMS components meet the minimum server system requirements. Additionally, ensure that any clients you will use to access the VMS components meet the minimum client system requirements.

For more information, see System Requirements, page 2-1.

Step 3 Install CiscoWorks Common Services.

Before you can install PIX MC, IDS MC, or Security Monitor, you must install CiscoWorks Common Services.

For more information, see Installing CiscoWorks Common Services as a Standalone Server, page 2-5.

Step 4 Install PIX MC.

PIX MC allows you to manage PIX Firewalls. You must install PIX MC on a server where CiscoWorks Common Services is installed.

For more information, see Installing PIX MC, page 2-11.

Step 5 Install IDS MC.

IDS MC allows you to manage IDS Sensors. You must install IDS MC on a server where CiscoWorks Common Services is installed.

For more information, see Installing IDS MC, page 2-12.

Step 6 Install Security Monitor.

Security Monitor allows you to collect, monitor, and view IDS Sensor postoffice events and PIX Firewall syslog messages. You must install Security Monitor on a server where CiscoWorks Common Services is installed.

Note For deployments in your production network and optimal performance, we recommend that you install Security Monitor on a server separate from the one running your Management Centers.

For more information, see Installing Security Monitor, page 2-14.

Step 7 Verify your installations.

Ensure that you successfully installed CiscoWorks Common Services, PIX MC, IDS MC, and Security Monitor.

For more information, see Verifying Your Installations, page 2-16.

Installing CiscoWorks Common Services as a Standalone Server

This section describes how to install CiscoWorks Common Services without first installing CiscoWorks. CiscoWorks Common Services contains the desktop and user authentication and authorization components found in CiscoWorks. However, you cannot run CiscoWorks applications, such as Resource Management Essentials, on a standalone installation of CiscoWorks Common Services.

Note For information about installing CiscoWorks Common Services on a server where CiscoWorks is already installed, see *Installing CiscoWorks Common Services 1.0 on Windows 2000*.

Before You Begin

- Obtain a license for CiscoWorks Common Services and make it available on the target server or floppy disk.
- Disable any virus scanning or intrusion detection software that may be running in the background on the server. These types of software can interfere with the installation.
- Close all other running programs.
- If you are reinstalling CiscoWorks Common Services, make sure the target directory is empty or does not exist before beginning the installation.

To install CiscoWorks Common Services in a standalone configuration, follow these steps:

Step 1 Put the Common Services 1.0 CD-ROM in the server CD-ROM drive, and then click **Install** on the Installer page that appears.

The CiscoWorks Common Services installation program starts. The Welcome page of the installation application appears.

If the installation program does not start, select **Start > Run** from the Windows taskbar, and then enter *d*:`/setup` in the Run dialog box, where *d* is the drive letter of the CD-ROM drive. Press **Enter** to start the installation program.

Step 2 Click **Next**.

The Software License Agreement page appears.

Step 3 To accept the terms of the license agreement, click **Yes**.

Note If you do not accept the terms of the license agreement, click **No**. The install wizard closes.

If you accepted the terms of the license agreement, the Choose Destination Location page appears. The default installation directory, `C:\Program Files\CSCOpx`, appears in the Destination Folder area.

Step 4 To change the default installation directory, click **Browse** and perform one of the following steps:

- Enter a new path in the Path field. If the directory specified does not exist, the installation program creates it.
- Use the Directories and Drives fields to navigate to an existing directory.

Step 5 Click **Next** to continue.

The System Requirements page appears.

Step 6 Review the requirements to ensure that the drive specified has enough free space for the installation. If the selected drive does not have enough free space, perform one of the following steps:

- Click **Back** to return to the Choose Destination Location screen and select a drive that meets the drive space requirements.
- Click **Cancel** to terminate the installation. You need to either install additional drive space on the target system or install CiscoWorks Common Services on a system that has the drive space requirements.

Verify that the system has enough memory. If the system does not have enough memory, click **Cancel** to terminate the installation. You should either install additional memory in the target system or install CiscoWorks Common Services on a system that meets the minimum memory requirements.

If your system meets all of the system requirements, click **Next**.

The Select License File screen appears.

Step 7 Enter the path to the license file in the License file location field. You can also use the Browse button to navigate to the correct license file. Click **Next** to continue.

Note You can bypass this step by clicking **Skip**. However, some of the client applications will not function if you do not enter a valid license. Refer to your client application documentation to note the licensing requirements for the applications you plan to install.

The Account Information page appears.

Step 8 Enter the password used to log in to Windows in the Password and Confirm Password fields. Click **Next** to continue.

If the two passwords do not match, the system prompts you to enter them again. If the passwords match, the Ports Configuration page appears.

Step 9 To change the external port numbers used by the Lock Manager (lm.exe) and database (fms.exe) services, enter the new information in the following fields:

- **LM Port**—The port used by Lock Manager. The default value is 1272. Use the default value unless it conflicts with another application on the server.
- **FMS Port**—The port used by the CiscoWorks Common Services database. The default value is 9652. Use the default value unless it conflicts with another application on the server.

Click **Next** to continue.

The Database Configuration page appears.

Step 10 Enter the information used by the SQL database component of CiscoWorks Common Services:

- **Server Port**—The port used by the SQL database. The default value is 10033. Use the default value unless it conflicts with another application on the server.
- **Password**—The password used by the SQL database. The password must be at least 4 characters long.
- **Confirm Password**—The same value you entered in the Password field.

Click **Next** to continue.

The Apache Server Configuration page appears.

Step 11 Enter the information used by the Apache server component of CiscoWorks Common Services:

- **HTTPS Port**—The port used by Apache for Secure Socket Layer (SSL) requests. Use the default value, 443, unless it conflicts with another application on the server.
- **Email Address**—The e-mail address of the system administrator (required).
- **SMTP Server**—The DNS name or IP address of your SMTP server.

Click **Next** to continue.

The Certificate Generation page displays.

Step 12 Enter the following information required to generate the local certificate. The local certificate is used for authentication and authorization when you login to the CiscoWorks desktop:

- **Country Code**—A two-character code for the country where the CiscoWorks Common Services server is located.
- **State**—The name of the state or province where the CiscoWorks Common Services server is located.
- **City**—The name of the city where the CiscoWorks Common Services server is located.
- **Company**—Your company name.
- **Organization**—The name of the organization or division you work in.
- **Domain**—The name of the domain the server resides in.
- **Certificate Password**—A password for the certificate. The password must have a minimum of 4 and a maximum of 10 alphanumeric characters.
- **Confirm Password**—The same value you entered in the Certificate Password field.

Note You cannot leave any of the fields blank. If one of the above fields does not apply to you, enter any text of your choosing in the field.

Click **Next** to continue.

The Create Shortcuts page appears.

Step 13 To create a shortcut on the Windows desktop, select the **Create a shortcut...** check box, and then click **Next** to continue.

The Verification page appears.

Step 14 Review your settings. If you need to change any settings, click **Back** to return to the setting you need to change. Click **Next** to continue.

The Start Copying Files page appears. During the file copy, the system prompts you four different times to change passwords for the following components:

- The casuser account (the user created by CiscoWorks Common Services to run the desktop services)
- The "admin" account

- The "guest" account
- The CMF database

Note If you abort the installation during the file copy stage, you must run the uninstall program before you attempt to install CiscoWorks Common Services again.

Step 15 To accept the default passwords, click **No**.

Note The default password for the admin account is "admin". The default password for the "guest" account is none (blank). You can change these passwords at a later time. The default passwords for causer and the database are generated by the system; you cannot change them later.

To change a password, follow these steps:

a. Click **Yes**.

b. Enter the password in the Password field.

c. Re-enter the password in the Confirm field.

d. Click **OK**.

The installation may take a few minutes to complete while the components are installed and the services are configured. When the installation is complete, the Restart page appears.

Step 16 Select **Yes** and click **Finish** to restart the computer. Select **No** and click **Finish** to restart the computer at a later time.

Note You must restart the computer before you use CiscoWorks Common Services.

Installing PIX MC

This section describes how to install PIX MC. This procedure assumes that you have already installed CiscoWorks Common Services.

To install PIX MC, follow these steps:

Step 1 Log in as the local administrator on the system on which you installed CiscoWorks Common Services.

This user account *must* be the same one used to install CiscoWorks Common Services.

Step 2 Insert the PIX MC CD into the CD-ROM drive, and then click **Install** on the Installer page that appears.

If the installation program does not start, select **Start > Run** from the Windows taskbar, and then enter *d*:/setup in the Run dialog box, where *d* is the drive letter of the CD-ROM drive. Press **Enter** to start the installation program.

The Welcome page appears.

Step 3 Click **Next**.

The Software License Agreement page appears.

Step 4 To accept the terms of the license agreement, click **Yes**.

Note If you do not accept the terms of the license agreement, click **No**. The install wizard closes.

The System Requirements page lists the details of your available system resources compared with the requirements of PIX MC.

Caution If your system does not meet the system requirements, we recommend that you exit the installation and see your system administrator for assistance installing the application.

Step 5 Click **Next**.

The Verification page lists the details of the installation and asks you to confirm that you want to proceed.

Step 6 Click **Next**.

Installation progress is displayed while files are copied and tools are configured. PIX MC is installed by default in the same location where CiscoWorks Common Services is installed. That default location is `C:\Program files\CSCOpx`. When the installation is complete, the Setup Complete page appears.

Step 7 Click **Finish**.

Installing IDS MC

This section describes how to install IDS MC.

This procedure assumes that you have already installed CiscoWorks Common Services.

Tip For enhanced performance, we recommend that you install IDS MC and Security Monitor on separate servers. If you are installing IDS MC and Security Monitor on the same server, follow the installation procedure in *Installing Management Center for IDS Sensors 1.0 and Monitoring Center for Security 1.0 on Windows 2000*.

To install IDS MC, follow these steps:

Step 1 Log in as the local administrator on the system on which you installed CiscoWorks Common Services.

Step 2 Insert the Monitoring Center for Security and Management Center for IDS Sensors CD into the CD-ROM drive, and then click **Install** on the Installer page that appears.

If the installation program does not start, select **Start > Run** from the Windows taskbar, and then enter *d*:/setup in the Run dialog box, where *d* is the drive letter of the CD-ROM drive. Press **Enter** to start the installation program.

The Welcome page appears.

Step 3 Click **Next** to begin the installation.

The Software License Agreement page appears.

Step 4 To accept the terms of the license agreement, click **Yes**.

Note If you do not accept the terms of the license agreement click **No**. The install wizard closes.

Step 5 Select the **Custom installation** radio button. Then, click **Next**.

Step 6 To install IDS MC, select the **IDS MC only** radio button. Then, click **Next**.

The System Requirements page appears.

Step 7 Verify that your system meets the minimum disk space and memory requirements. Then, click **Next**.

The Verification page appears.

Step 8 Verify the selected components. Then, click **Next**.

The Select Database Location page appears.

Step 9 By default, the database is located in the directory where CiscoWorks Common Services is installed. To specify a different directory for the IDS database, enter a file path in the Database file location field. Then, click **Next**.

The Select Database Password page appears.

Step 10 Enter the database password in the **Password** field. Then, to confirm the password, reenter it in the **Confirm Password** field. Then, click **Next**.

The Restart page appears.

Step 11 Select **Yes, I want to restart my computer now** and click **Finish** to restart the computer. Select **No, I will restart my computer later** and click **Finish** to restart the computer at a later time.

Note You must restart the computer before you use IDS MC.

Installing Security Monitor

This section describes how to install Security Monitor.

This procedure assumes that you have already installed CiscoWorks Common Services.

Tip For enhanced performance, we recommend that you install IDS MC and Security Monitor on separate servers. If you are installing IDS MC and Security Monitor on the same server, follow the installation procedure in *Installing Management Center for IDS Sensors 1.0 and Monitoring Center for Security 1.0 on Windows 2000*.

To install Security Monitor, follow these steps:

Step 1 Log in as the local administrator on the system on which you installed CiscoWorks Common Services.

Step 2 Insert the Monitoring Center for Security and Management Center for IDS Sensors disc into the CD-ROM drive, and then click **Install** on the Installer page that appears.

If the installation program does not start, select **Start > Run** from the Windows taskbar, and then enter *d*:/setup in the Run dialog box, where *d* is the drive letter of the CD-ROM drive. Press **Enter** to start the installation program.

The Welcome page appears.

Step 3 Click **Next** to begin the installation.

The Software License Agreement page appears.

Step 4 To accept the terms of the license agreement, click **Yes**.

Note If you do not accept the terms of the license agreement click **No**. The install wizard closes.

Step 5 Select the **Custom installation** radio button. Then, click **Next**.

Step 6 To install Security Monitor, select the **Security Monitor only** radio button. Then, click **Next**.

The System Requirements page appears.

Step 7 Verify that your system meets the minimum disk space and memory requirements. Then, click **Next**.

The Verification page appears.

Step 8 Verify the selected components. Then, click **Next**.

The Select Database Location page appears.

Step 9 By default, the database is located in the directory where CiscoWorks Common Services is installed. To specify a different directory for the IDS database, enter a file path in the Database file location field. Then, click **Next**.

The Select Database Password page appears.

Step 10 Enter the database password in the **Password** field. To confirm the password, reenter it in the **Confirm Password** field. Then, click **Next**.

The Select CW2000 Syslog Port page appears.

Step 11 Specify which UDP port CiscoWorks uses. The value can be between 1 and 65,535. By default, CiscoWorks uses UDP port 52514. We recommend that you use the default port value. Then, click **Next**.

The Configure Communication Properties page appears.

Step 12 To submit the communication properties for this host, enter the appropriate values in the Host ID, Organization ID, IP Address, Host Name, and Organization Name fields. Then, click **Next**.

The properties are used to establish the communication infrastructure for this host and the IDS sensor. The Restart page appears.

Step 13 Select **Yes, I want to restart my computer now** and click **Finish** to restart the computer. Select **No, I will restart my computer later** and click **Finish** to restart the computer at a later time.

Note You must restart the computer before you use Security Monitor.

Verifying Your Installations

This section describes how to log in to CiscoWorks and how to verify installation of CiscoWorks Common Services, PIX MC, Security Monitor, and Security Monitor. It contains the following sections:

Verifying the CiscoWorks Common Services Installation

You can verify the success of the installation before you log in to CiscoWorks Common Services.

To verify the CiscoWorks Common Services installation, follow these steps:

Step 1 Open a DOS prompt, enter **net start**, and press **Enter**.

A list of Windows 2000 services appears.

Step 2 Verify that the following services are running:

- Apache WebServer
- CMF rsh/rcp service
- CMF syslog service
- CMF tftp service
- CW2000 Daemon Manager
- CW2000 Device Agent Framework
- CW2000 KRS Database
- CW2000 Lock Manager
- CW2000 Sybase Server
- CW2000 Tomcat Servlet Engine
- CW2000 Web Server
- JRun Proxy Server for CW2000

If any of these services is not present, reboot the system to start the services. If the missing services do not appear after rebooting the server, the installation was unsuccessful.

Logging in to CiscoWorks2000

The CiscoWorks2000 Server desktop is the interface for the CiscoWorks network management applications, including Security Monitor, IDS MC, and PIX MC. The desktop is a graphical user interface that runs in a browser. For additional information about the CiscoWorks2000 Server desktop, see *Getting Started with the CiscoWorks2000 Server Desktop*.

Before you log in, make sure that your browser is configured correctly for CiscoWorks. For more information, see *Installing CiscoWorks Common Services 1.0 on Windows 2000*.

If you have installed CiscoWorks and are logging in for the first time, you can use the reserved "admin" username and password.

To log in to CiscoWorks, follow these steps:

Step 1 Access the CiscoWorks2000 Server from your web browser.

Step 2 Enter **admin** in both the Name and Password fields of the Login Manager.

Note If you changed the default password for the **admin** account during the install, use that new password. If you did not change the default password when you installed CiscoWorks Common Services, we strongly recommend that you perform Step 4 to change it.

Step 3 Click **Connect** or press **Enter**. You are now logged in.

Step 4 Select **Server Configuration > Setup > Security > Modify My Profile** to change the admin password.

Verifying Installation by Checking Package Options

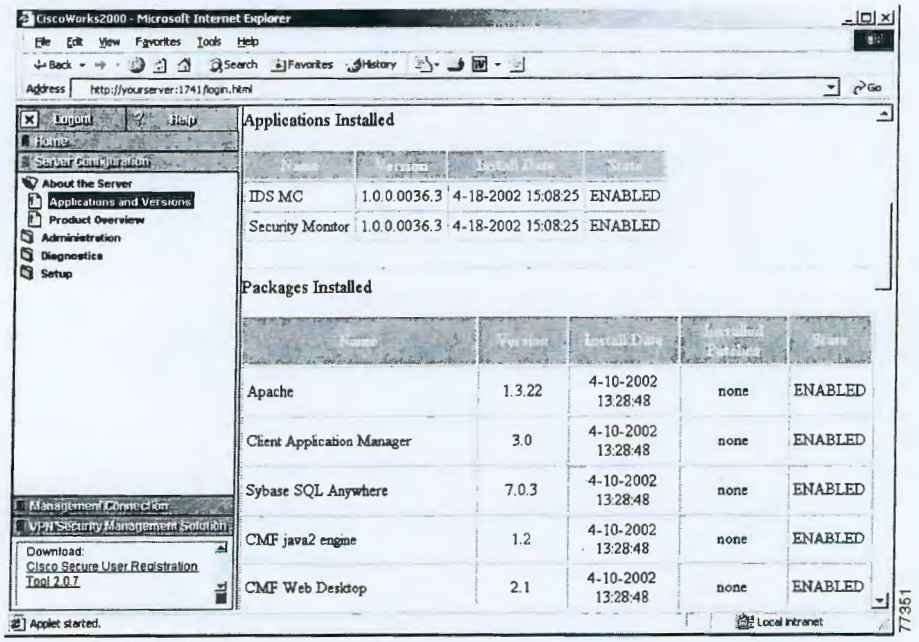
You can verify the installation of PIX MC, IDS MC, and Security Monitor in the Packages Installed section of the About the Server page from the CiscoWorks2000 desktop.

To verify installation from the About the Server page, follow these steps:

Step 1 Select **Server Configuration > About the Server > Applications and Versions**.

The About the Server page appears.

Step 2 Verify that IDS MC and Security Monitor are listed in the Applications Installed list of the About the Server page and that Management Center for PIX Firewalls is listed in the Packages Installed list.



13183
A.

CHAPTER 3

Introducing the Cisco IDS Director

This chapter introduces the Cisco IDS Director, and includes the following sections:

- The Director's Graphical Display
- Alarms
- Starting the Director
- Customizing the Director's Environment
- Stopping the Director

The Director's Graphical Display

This section describes the Director's hierarchical map display, and includes the following topics:

- Translating Events to Alarms
- Root Submap (Top-Level)
- Network Typology Submap (NetRanger)
- Daemons Submap
- Status Submap

Translating Events to Alarms

Events are sent to the Director by a Sensor or IDSM that detects a security violation. The *smid* daemon on the Director interprets this event information and passes it to a daemon called *nrdirmap*. *nrdirmap* is responsible for displaying this information on the Director's maps.

Depending on the severity of an alarm, the alarm icon displays different colors: red for severe, yellow for moderate, green otherwise. The icons for the daemon, Sensor, and IDSM that generate the alarm will also be the same color as the most severe alarm generated.

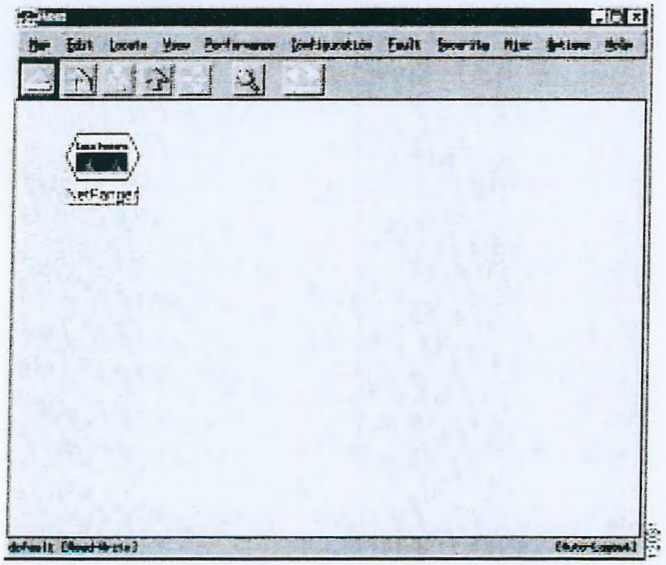
Refer to the following documents for information on the Sensor and the IDSM:

- *Cisco Intrusion Detection System Sensor Installation and Safety Note*
- *Cisco Intrusion Detection System Sensor Version 2.5 Configuration Note*
- *Release Notes for Cisco Intrusion Detection System Sensor Version 2.5(0)S0*
- *Catalyst 6000 Intrusion Detection System Module Installation and Configuration Note*

Root Submap (Top-Level)

The top-level submap (called the Root submap) is the topmost map of the map hierarchy, and is illustrated in Figure 3-1.

Figure 3-1 Root Submap

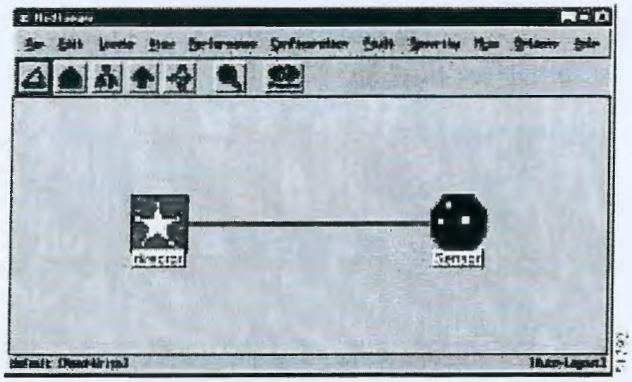


Double-click the NetRanger icon on the Root submap to get to the network typology submap.

Network Typology Submap (NetRanger)

The network typology submap (called the NetRanger submap) contains icons for all Sensor, IDSM, and Director machines (see Figure 3-2).

Figure 3-2 Network Typology Submap (NetRanger)



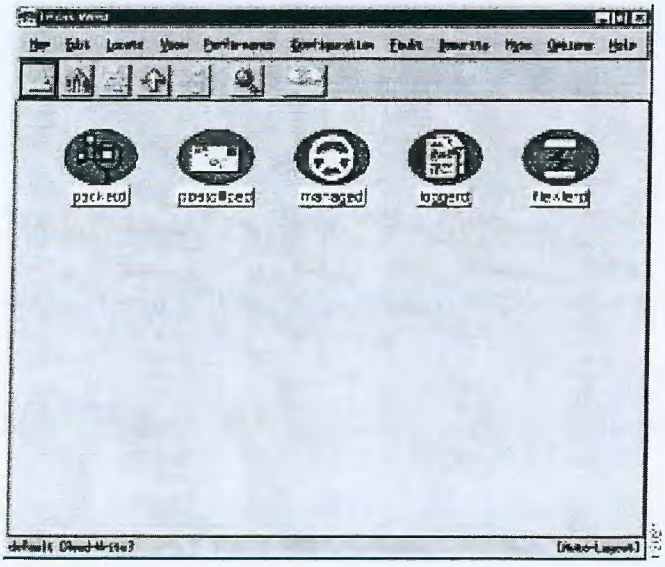
The Director automatically generates all the icons on the submaps as events occur—however, you can manually add icons. For more information on manually adding icons to the Director, see "Working with Icons" in Chapter 10 "Advanced Director Functions."

Daemons Submap

Double-clicking a Sensor/IDSM/Director (machine) icon displays the daemons submap, which contains icons for all the daemons running on that machine (see Figure 3-3).

Cisco IDS is a collection of discrete subsystems that have been implemented via daemons. See "Daemons" in Appendix C, "Cisco IDS Internal Architecture" for more information on the IDS daemons.

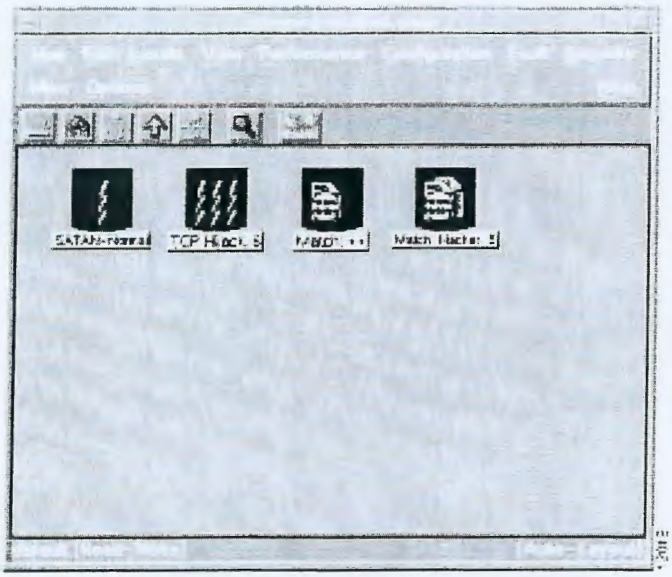
Figure 3-3 Daemons Submap



Status Submap

Double-clicking a daemon icon displays a status submap, which shows the status of that daemon, for example, all of the alarms generated by that daemon (see Figure 3-4).

Figure 3-4 Status Submap



Alarms

This section includes the following topics:

- Intrusion Alarms
- Context Buffer Alarms
- Error Alarms
- OKAlarms
- Alarm Labels

Alarms can be generated by Sensors/IDSMs and by Cisco IOS routers running the Intrusion Detection System feature of the Cisco IOS Firewall Feature Set, also known as IOS-IDS.

When an alarm is sent to the Director, the Director's *nrdirmap* daemon interprets the alarm data in order to graphically present it on the user interface. Alarm icons can indicate different types of events, specifically intrusions, context attacks, or errors.

If multiple alarms of the same type (except for timestamp and sequence number) are generated, then the Director displays these alarms as a group called an alarm set.

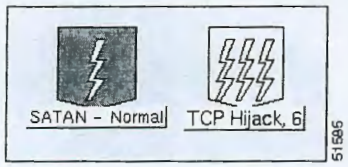
A special type of alarm is the OKAlarm, which when displayed in a submap, indicates that there are no unresolved alarms for that daemon.

Intrusion Alarms

Intrusion alarms are depicted as lightning bolts, and indicate that some type of unauthorized activity has occurred.

Intrusion alarm sets are depicted with three lightning bolts. Figure 3-5 illustrates both an intrusion alarm and intrusion alarm set icon.

Figure 3-5 Intrusion Alarm and Intrusion Alarm Set Icons

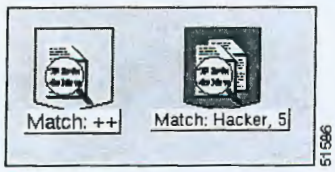


Context Buffer Alarms

Certain alarms have associated context buffers, which contain up to 256 bytes of data in both incoming and outgoing directions. These context buffer alarms are depicted as a magnifying glass over a sheet of paper with writing on it. The magnifying glass is a visual reminder that you can view additional alarm information by selecting the alarm icon and clicking **Security>Show>Context Buffer**.

Context buffer alarm sets are depicted as a magnifying glass over two sheets of paper with writing on them. Figure 3-6 illustrates a context buffer alarm and context buffer alarm set icon.

Figure 3-6 Context Buffer Alarm and Context Buffer Alarm Set



Following is a partial list of signatures that trigger context buffer alarms:

- 3100 Smail Attack
- 3101 Sendmail Invalid Recipient
- 3102 Sendmail Invalid Sender
- 3103 Sendmail Reconnaissance
- 3104 Archaic Sendmail Attacks
- 3200 WWW Phf Attack

- 3201 WWW General cgi-bin Attack
- 6251 Telnet Authorization Failure
- 8000 FTP Retrieve Password File
- 8000 Telnet-IFS Match
- 8000 Telnet-/etc/shadow Match
- 8000 Telnet-+ +
- 8000 Rlogin-IFS Match
- 8000 Rlogin-/etc/shadow Match
- 8000 Rlogin-+ +

For more information on signatures, see "Chapter 8, "The NSDB and Signatures."

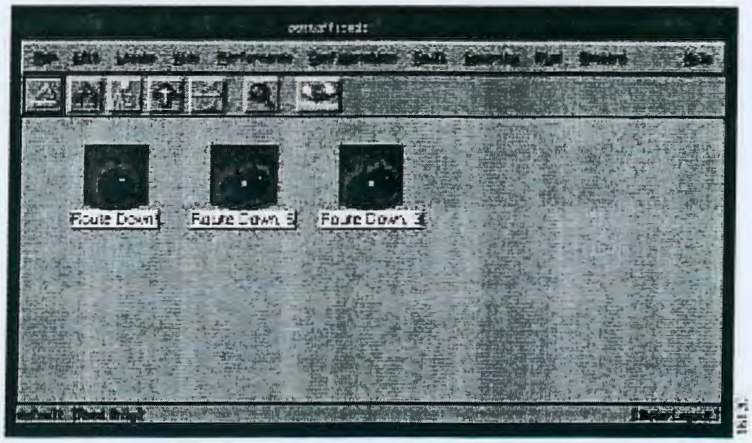
Error Alarms

This section describes the types of error alarms, and includes the following topics:

- Daemon Down
- Daemon Unstartable
- Route Down

Error alarms are depicted as a single bomb. Error alarm sets are depicted as two bombs. Both error alarms and error alarm sets are illustrated in Figure 3-7.

Figure 3-7 Error Alarm Icons



Daemon Down

The daemon down error alarm indicates that *postofficed* has detected that a daemon has stopped.

After an error alarm occurs, you must manually delete the icon, regardless of whether *postofficed* is able to restart the daemon.

To delete the icon, right-click it, and click **Delete Symbol**.

Daemon Unstartable

The daemon unstartable error alarm indicates that *postofficed* cannot restart a daemon that was previously down.

After an error alarm occurs, you must manually delete the icon, regardless of whether you are able to manually restart the daemon.

Route Down

The route down error alarm is generated each time *postofficed* detects that a connection to another machine is down. These error alarms have a severity level of 5. To get details on the alarm, right-click the alarm, and click **Show>Alarm Details**. The **Alarm Details** window for this alarm displays the following information:

HostID.*OrgID* `route` *route-number* `down`

where *HostID* and *OrgID* indicate the host and organization ID of the IDS host involved in the route down error alarm, and *route-number* indicates which route failed.

A different error alarm is generated for each communication route. For example, if the route between *sensor-one* and *sensor-two* is down, then the managing Director will receive two error alarms: one indicating that *sensor-one* is unreachable, and another indicating that *sensor-two* is unreachable.

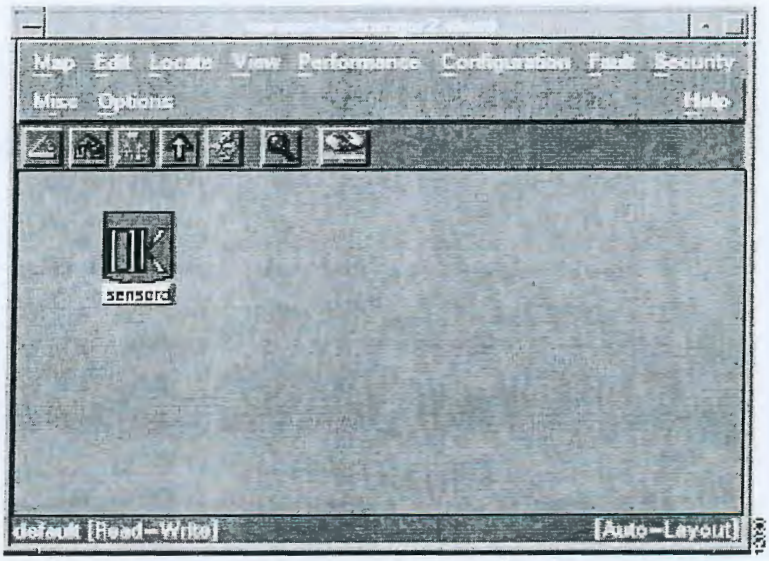
Because *postofficed* repeatedly checks to see if a machine is reachable, there is a chance that error alarm sets could be consolidated. For example, if *sensor-two* in the preceding example remains unreachable, then the error alarm associated with it is displayed as a consolidated error alarm set.

Route down error alarms are automatically deleted when the Director receives an indication that the route is operational.

OKAlarms

If a daemon has not generated any alarms or alarm sets, then the special OKAlarm is displayed in the status submap (see Figure 3-8). As the name of this alarm implies, it means that no alarms have been generated by the daemon.

Figure 3-8 OKAlarm



Alarm Labels

In most cases, an alarm's label will be the name of the signature that matches the alarm's signature ID. The Director uses the /usr/nr/etc/signatures file to determine a match. However, there are exceptions to this rule:

- If the signature ID of the alarm is not in the /usr/nr/etc/signatures file, then the label is the alarm's signature ID.
- For alarm sets, the label has the name of the signature ID followed by a comma, followed by a number indicating the number of alarms in the set.
- For error alarms, the label is either "Down!" to indicate that a daemon has stopped running, or "Unstartable!" to indicate that a daemon cannot be restarted.

- For alarms triggered by string-matching signatures, the label is "Match:" followed by the string that was matched.
- For policy violations, the label comes from the Alarm:Details field of the alarm's properties.

Starting the Director

To start the Director, follow these steps:

Step 1 Log on as user netrangr.

Step 2 To see a status of IDS daemons, type:

```
idsstatus
```

Step 3 If no daemons are running, type:

```
idsstart
```

Step 4 To start the Director, type:

```
ovw &
```

Note If the user interface does not start, manually start the network management background processes by typing `/opt/OV/bin/ovstart` and then typing the `ovw &` command.

The Director opens to the Root submap window.

Customizing the Director's Environment

This section provides information on configuring important Director settings, and includes the following topics:

- Changing Map Configuration Parameters
- Setting HTML Browser Preference
- Setting Color Preferences

Changing Map Configuration Parameters

There are five global map-level configuration parameters that can be set. These parameters affects the display of *all* Director security data, such as icon consolidation into alarm sets and mappings of alarm levels to alarm colors.

To set these global parameters, follow these steps:

Step 1 On the Director interface (Root submap), click:

- **Map>Maps>Describe/Modify** if your Director machine has HP OpenView 4.x or 5.x
- click **Map>Properties** if your Director machine has HP OpenView 6.x

The **Map Description** dialog box opens.

Step 2 Click **NetRanger/Director**, and click **Configure For This Map**.

The **NetRanger/Director Configuration** window opens.

Step 3 Make entries to the following:

a. Set the default lowest event severity that generates a marginal icon. For example, setting the default lowest event severity to **3** would create a marginal (yellow) icon if an alarm level 3 is generated.

b. Set the default lowest event severity that generates a critical icon. For example, setting the default lowest event severity in this case to **4** would create a critical (red) icon if an alarm level 4 is generated.

c. Set the default number of identical alarms before icon consolidation. For example, setting this number to **5** would create an Alarm Set when the number of identical alarms reached 5 or more.

d. Make sure that *nrdirmap* is enabled.

Setting HTML Browser Preference

The Network Security Database (NSDB) is an HTML-based encyclopedia of network security information. To access this information from the Director interface, you must set your HTML browser preference.

To set your HTML browser preference, follow these steps:

Step 1 On the Director interface (Root submap), click **Security>Configure**.

The **NetRanger Configuration File Management Utility** (nrConfigure) window opens.

Step 2 Click **File>Preferences**.

The **Preferences** dialog box opens.

Step 3 Type the path to your HTML browser in the **Browser Location** field, and click **OK**.

Setting Color Preferences

To configure your color preferences, follow these steps:

Step 1 On the Director interface (Root submap), click **Security>Configure**.

The **NetRanger Configuration File Management Utility** (nrConfigure) window opens.

Step 2 Click **File>Preferences**.

The **Preferences** dialog box opens.

Step 3 Click the **System Colors** tab.

You can select from three color preferences:

- **Use System Color Scheme**—This setting uses your windowing system's (CDE, OpenWindows, and so forth) color scheme.
- **Use Color Scheme from nrConfigure.properties file**—This setting uses the values found in the /usr/nr/etc/nrConfigure.properties file. The first time you select this, nrConfigure creates the file. You can customize it with any text editor.
- **Use NetRanger Color Scheme**—This setting uses the Director's predefined color scheme, and is the default setting.

Stopping the Director

You may need to stop the Director to upgrade IDS software, perform maintenance or troubleshooting on the Director workstation, or for other reasons.

To stop the Director, follow these steps:

Step 1 On the Director interface (Root submap), stop the network management user interface by clicking **Map>Exit**.

Note Stopping the network management user interface will not stop the background processes. To do so, log on as user root and type `ovstop`.

Step 2 As user netrangr, stop the IDS background processes by typing:

```
/usr/nr/bin/idsstop
```

Step 3 Check the status of the network management background processes by typing:

```
ovstatus
```

Step 4 Check the status of the IDS background processes by typing:

```
idsstatus
```

CHAPTER 5

IDS Device Manager Administration Tasks

The Administration tab enables you to perform the following tasks:

Viewing Diagnostics

You can obtain diagnostics information on your sensors for troubleshooting purposes.

Note Running diagnostics takes several minutes to complete.

To run diagnostics, follow these steps:

Step 1 Select **Administration > Support > Diagnostics**.

The Diagnostics page appears.

Figure 5-1 Diagnostics Page

Step 2 Click **Run Diagnostics**.

The Cancel Diagnostics Command page appears. Then, the View Diagnostics Result page appears.

Step 3 Click **View Results** to see the diagnostics report.

The IDS 4.0 System Status Report appears in another window in HTML format.

Note The next time you open the Diagnostics page, there is an additional button, View Last Report. Click **View Last Report** to view the most recent report. This report is deleted when you run a new one.

Viewing System Information

The System Information page displays the following information:

- TAC contact information.
- Software version.
- Status of applications.
- Interface information.
- Resource usage.

To view system information, follow these steps:

Step 1 Select **Administration > Support > System Information**.

The System Information page appears.

Figure 5-2 System Information Page

Step 2 To access the Cisco Technical Support Website, click the following link:

http://www.cisco.com/en/US/support/index.html

Applying Service Pack and Signature Updates

The Update page enables you to immediately apply service pack and signature updates.

Note The sensor cannot download service pack and signature updates from Cisco.com. You must download the service pack and signature updates from Cisco.com to your FTP server, and then configure the sensor to download them from your FTP server.

See Supported FTP Servers, page 3-37, for a list of supported servers.

To immediately apply a service pack and signature update, follow these steps:

Step 1 Select **Administration > Update**.

The Update page appears.

Figure 5-3 Update Page

Step 2 In the URL field, enter the URL where the update can be found.

For example:

```
URL: ftp://user@10.1.1.1/UPDATES/IDS-K9-sp-4.0-1.1-S36-0.1-.rpm.pkg
```

Note You must have already downloaded the update from Cisco.com and put it on the FTP server.

Step 3 In the Password field, enter the particular transport protocol password.

Note You can use the following transport protocols: SCP, FTP, HTTP, or HTTPS.

Note To reset the form, click **Reset**.

Step 4 Click **Apply to Sensor** to apply the update.

Note To schedule regular updates, see Configuring Automatic Updates, page 3-35.

Configuring IP Logging

You can configure the sensor to catch all IP traffic associated with the hosts you specify by IP address.

Note IP Logging requires that event logging be enabled with Informational as the severity level. See Configuring Signatures, page 3-1, for more information.

To generate logs files for specific IP addresses, follow these steps:

Step 1 Select **Administration > IP Logging**.

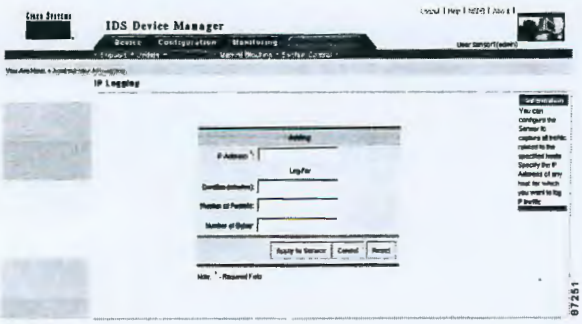
The Ip Logging Configuration page appears.

Figure 5-4 Ip Logging Configuration Page

Step 2 Click **Add** to add the IP addresses of the hosts whose IP traffic you want to log.

The Adding page appears.

Figure 5-5 Adding Page



Step 3 In the IP address field, enter the source IP address of the host whose IP traffic you want to log.

Step 4 In the Duration field, enter the number of minutes you want to the sensor to log IP traffic (optional).

Step 5 In the Number of Packets field, enter the number of packets you want the sensor to count (optional).

Step 6 In the Number of Bytes field, enter the number of bytes you want to log (optional).

Note To reset the form, click **Reset**.

Step 7 Click **Apply to Sensor** to save your changes.

The Ip Logging Configuration page now displays the new Log ID.

Note The sensor begins logging and creates a log file that you can view by selecting **Monitoring > IP Logs**. See Downloading IP Logs, page 4-1, for more information.

Step 8 To discontinue logging IP traffic, select the check box next to the log ID, and then click **Stop**.

Note The IP log is overwritten when the sensor uses up its allocated space for IP logging.

Blocking Hosts Manually

On occasion, you may want to block a host for a short time. From the Host Manual Blocks page, you can configure which host is blocked and for how long, and you can view a list of hosts that are being blocked.

To set up the manual blocking of a host, follow these steps:

Step 1 Select **Administration > Manual Blocking > Host Manual Blocks**.

The Host Manual Blocks page appears.

Figure 5-6 Host Manual Blocks Page

Step 2 Click **Add** to add a host to block.

The Adding Page appears.

Figure 5-7 Adding Page

Step 3 In the Source Address field, enter the IP address of the host you want to block.

Step 4 In the Source Port field, enter the port you want to use to block the host (optional).

Step 5 In the Destination Address field, enter the destination address (optional).

Step 6 From the Protocol list box, select one of these options (optional):

- None
- tcp
- udp

Step 7 Select the **Connection Shun** check box to block only those connections that have the source IP address, destination IP address, destination port, or protocol specified (optional).

Note If you select the Connection Shun check box, the attacking host is free to connect to other hosts or to other services on the protected host. If destination port and protocol are not specified, the attacking host cannot send packets to the protected host at all, but can access other hosts on the network.

Step 8 In the Timeout field, enter the number of minutes you want the block to last.

Note To create a permanent block, enter **-1**.

Note To reset the form, click **Reset**.

Step 9 Click **Apply to Sensor** to save your changes.

The Host Manual Blocks page lists the hosts that you are blocking and the time remaining.

Step 10 To see how many minutes have passed for a specific block, select the check box next to the host you want to check and click **Host Manual Blocks** again. The page is refreshed and the remaining block time is shown.

Step 11 To delete a block, select the check box next to the host you want to discontinue the block for, and then click **Delete**.

The host is no longer in the list of blocked hosts.

Blocking Networks Manually

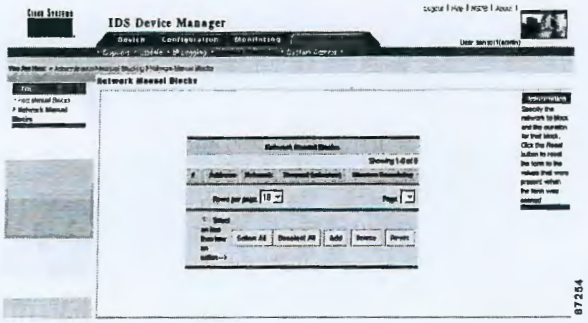
On occasion, you may want to block a network for a short time. From the Network Manual Blocks page, you can configure which network is blocked and for how long, and you can view a list of networks that are being blocked.

To set up manual blocking of a network, follow these steps:

Step 1 Select **Administration > Manual Blocking > Network Manual Blocks.**

The Network Manual Blocks page appears.

Figure 5-8 Network Manual Blocks Page



Step 2 Click **Add** to add a network to block.

The Adding page appears.

Figure 5-9 Adding Page

Step 3 In the IP Address field, enter the IP address of the network you want to block.

Step 4 In the Netmask field, enter the netmask of the network you want to block.

Step 5 In the Timeout field, enter the number of minutes you want the block to last.

Note To create a permanent block, enter **-1**.

Note To reset the form, click **Reset**.

Step 6 Click **Apply to Sensor** to save your changes.

The Network Manual Blocks page lists the networks that you are blocking and the time remaining.

Step 7 To see how many minutes have passed for a specific block, select the check box next to the network you want to check, and then click **Network Manual Blocks**. The page is refreshed and the remaining block time is shown.

Step 8 To delete a block, select the check box next to the network you want to discontinue a block for, and then click **Delete**.

The network is no longer in the list of blocked networks.

Resetting and Powering Down the Sensor

You can reset and power down the sensor from the System Control page. Reset shuts down the sensor safely and then restarts the sensor. Power Down safely shuts down the sensor.

To reset or power down the sensor, follow these steps:

Step 1 Select **Administration > System Control**.

The System Control page appears.

Figure 5-10 System Control Page

Step 2 Select one of the following options from the list box:

- **Reset**—Shuts down the IDS applications and the sensor, and then reboots. After the reboot, you must log in again.

  Note There is a 30-second delay during which users who are currently logged in to the CLI are notified that the IDS applications and sensor are going to shut down.

- **Power Down**—Shuts down the IDS applications and then shuts off the sensor.

Note There is a 30-second delay during which users who are currently logged in to the CLI are notified that the IDS applications and the sensor are going to shut down.

CHAPTER 7

Tuning Sensor Configurations

After configuring your sensors, you need to tune them to achieve optimal performance on your network, particularly to minimize false positives and false negatives.

Note Tuning sensor configurations should not be confused with tuning signature parameters.

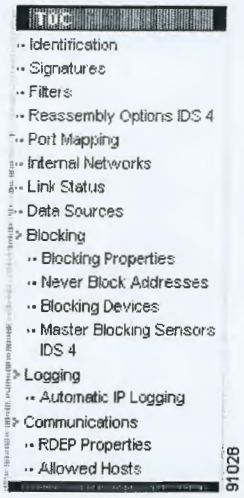
Some legitimate network activity, such as virus scanning, can appear to be an attack on your network. When legitimate network activity is reported as an attack, that report is called a *false positive*. More generally, a false positive can be defined as the interpretation of an instance of legitimate and expected network activity as an attack because that activity meets criteria that were specified to identify an attack prior to the occurrence of the attack. You can decrease the number of false positives by tuning your sensor configurations.

Tuning your sensor configurations can also help you solve another problem. You can decrease the number of *false negatives* by tuning your sensor configurations. A false negative can be defined as an attack that was not detected.

You can tune sensor configurations by using four general methods:

- Specifying *reassembly settings* for IP fragments and TCP sessions.
- Port mapping (that is, identifying additional ports).
- Identifying hosts and networks that should be exempt from *blocking*.
- *Filtering* alarms in accordance with their severity and their source.

Reassembly Options, Port Mapping, Never Block Addresses, and Filtering are in the TOC that appears when you select Configure > Settings in IDS MC.



You can tune sensor configurations by specifying reassembly options for IP fragments and TCP sessions. Specifying reassembly options prevents false negatives that are caused because the sensor cannot reconstruct the datagram or session.

When using IDSM devices supported by IDS MC, you can identify additional ports that should be considered by a sensor signature. This process is known as port mapping. Examples of these additional ports are those used by custom TCP services and those used by well-known services that you have reassigned to another port. Identifying additional ports is important because some sensor signatures are based on specific port numbers.

You can tune sensor configurations by identifying hosts and networks that should be exempt from blocking.

For example, your sensor configuration may include instructions to block sources of a particular attack whenever that attack is detected; you may also have a trusted network device whose normal, expected behavior appears to be that attack. (This situation results in a false positive.) In this situation, you can tune your sensor configuration to ignore that particular perceived attack when its source is your trusted network device. In that way, you avoid false positives: You avoid the generation of alarms from your trusted network device, and your trusted network

device is not blocked. You still receive alarms if that particular attack is detected in traffic from other sources. Also, you can still block other, untrusted devices if your sensor detects that particular attack in traffic from those other, untrusted devices.

You can tune sensor configurations by filtering audit events. Tuning a sensor by filtering audit events reduces the number of false positives. You can set the minimum level of events that will be reported to you. Also, you can enable and disable alarms from specific hosts and networks.

When using IDSM devices supported by IDS MC, you can define rules that prevent the sensor from generating alarms and audit event records for suspicious behavior based on traffic originating from or destined to specific networks and hosts. You can use the Filters page to define these rules.

Task List for Tuning Sensor Configurations

After configuring your sensors, you need to tune them. You can tune sensor configurations by using four general methods:

- Specifying *reassembly options* for IP fragments and TCP sessions.
- Port mapping (that is, by identifying additional ports).
- Identifying hosts and networks that should be exempt from *blocking*.
- *Filtering* alarms in accordance with their severity and their source.

You can tune sensor configurations by performing one of the following tasks. For step-by-step procedures on performing a specific task, refer to the corresponding section.

- Specifying IP Fragment and TCP Session Reassembly Settings for a Sensor, page 7-4
- Identifying Additional Ports Used by Specific Signatures Applied to a Sensor, page 7-5
- Defining Filters for a Sensor, page 7-7
- Specifying Networks and Hosts that Should Never Be Blocked, page 7-13

Specifying IP Fragment and TCP Session Reassembly Settings for a Sensor

The goal of defining these reassembly settings is to ensure that the sensor does not allocate all of its resources to datagrams that cannot be completely reconstructed, either because the sensor missed some frame transmissions or because an attack is generating random fragmented datagrams.

These settings ensure that valuable system resources are not reserved for sessions that are no longer active. These settings apply to sensors globally, not to individual settings such as signatures.

To specify IP fragment reassembly options and TCP session reassembly options, follow these steps:

Step 1 Select **Configuration > Settings**.

Step 2 In the TOC, click the **Object Selector** handle.

Step 3 In the Object Selector, select the sensor for which you want to specify reassembly options.

The Object Selector closes.

Step 4 In the TOC, select **Reassembly Options**.

The Reassembly Options page appears.

When configuring an IDSM or a 4.x sensor appliance, you have the option of TCP strict reassembly. The 3.x sensor appliance does not have that option.

When configuring a sensor appliance (3.x or 4.x), you have the option of specifying Maximum Total Fragments. The IDS module does not have that option.

Step 5 When configuring a 4.x sensor appliance, specify the operating system in the IP Reassemble Mode list box.

Step 6 To specify that you want the sensor to reassemble IP datagrams, select the **Reassemble Fragments** check box under IP Fragment Reassembly. Reassembling fragments is done by default by all sensors, both appliances and modules.

Step 7 To specify the maximum number of partial datagrams that the sensor can attempt to reconstruct at one time, enter that value in the Maximum Partial Datagrams field. Maximum Partial Datagrams is not available for 4.x sensor appliances.

Step 8 To specify the maximum number of fragments that can be accepted into a single datagram, enter that value in the Maximum Fragments Per Datagram field. Maximum Fragments Per Datagram is not available for 4.x sensors.

Step 9 To specify the maximum total fragments, enter that value in the Maximum Total Fragments field. Maximum Total Fragments is available for sensor appliances but not for IDS modules.

Step 10 To specify the maximum number of seconds that can elapse before the sensor stops keeping track of a particular exchange for which it is trying to reassemble a datagram, enter that value in the Fragmented Datagram Timeout field.

Step 11 To specify that the sensor track only sessions for which the three-way handshake is completed, select the **TCP Three Way Handshake** check box.

Step 12 To specify how strict the reassembly requirements for this sensor should be when it attempts to reassemble the entire TCP session, select that type from the TCP Strict Reassembly list box. TCP Strict Reassembly is available for IDS modules but not for sensor appliances.

Step 13 To specify the number of seconds that can elapse before the sensor frees the resources allocated to a fully established TCP session, enter that value in the TCP Open Establish Timeout field.

Step 14 To specify the number of seconds that can elapse before the sensor frees the resources allocated for an initiated, but not fully established, TCP session, enter that value in the TCP Embryonic Timeout field.

Step 15 To accept your changes and close the Reassembly Options page, click **Apply**.

Identifying Additional Ports Used by Specific Signatures Applied to a Sensor

When using IDSM devices supported by IDS MC, you can specify additional ports that should be considered by signatures that study specific network services (identified by the TCP port used by that network service). These port settings enable you to identify any well-known network service ports that you have reassigned on your internal network. These port settings also enable you to identify any custom TCP-based services, running across your internal networks, that you want the sensor to study for specialized attacks that target these network services.

Port mapping applies only to 3.x IDS modules, 4.x sensor appliances, and IDS MC groups. It does not apply to 3.x sensor appliances.

To identify additional or remapped ports for more extensive evaluation by specific signatures, follow these steps:

Step 1 Select **Configuration > Settings**.

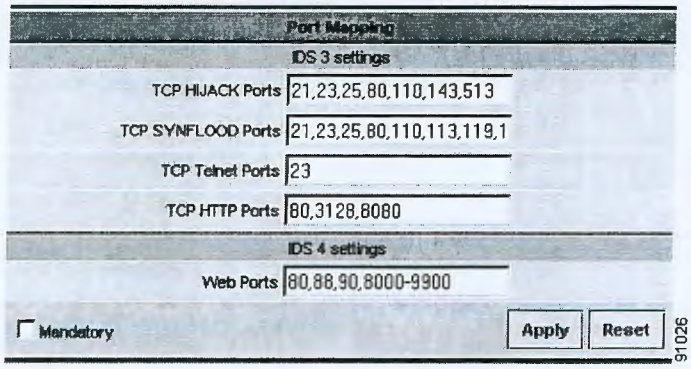
Step 2 Click the **Object Selector** handle.

Step 3 In the Object Selector, select the device or group for which you want to identify additional or remapped ports.

The Object Selector closes.

Step 4 In the TOC, select **Port Mapping**.

The Port Mapping page appears.



Step 5 To specify additional ports that should be considered by the signature that studies for hijacked ports on a TCP-based service, enter each port number in the TCP HIJACK Ports field, separating entries with a comma.

Step 6 To specify additional ports that should be considered by the signature that studies for TCP-based flood attacks, enter each port number in the TCP SYNFLOOD Ports field, separating entries with a comma.

Step 7 To specify additional ports that should be considered by the attack signature that studies for Telnet-based attacks, enter each port number in the TCP TELNET Ports field, separating entries with a comma.

Step 8 To specify additional ports that should be considered by the attack signature that studies for HTTP-based attacks, enter each port number in the TCP HTTP Ports field, separating entries with a comma.

Step 9 To accept your changes and close the Port Mapping page, click **Apply**.

Defining Filters for a Sensor

Filters can be used to reduce the number of false positives reported by your sensors, so they are considered a method of tuning your sensors.

Filtering an alarm means that the sensor will analyze the data stream but will not generate an alarm. Filtering all alarms from a particular signature is not the same thing as disabling that signature, which results in no analysis of the data stream for that signature.

Note Filters for a sensor in IDS MC should not be confused with event filters that are part of an event rule in Security Monitor.

A filter is defined by specifying the signature, the source address, and the destination address and whether it is an inclusive or exclusive filter. You cannot define any particular part of the filter (such as the source address) as inclusive or exclusive; you have to define the entire filter as inclusive or exclusive. Also, if you define more than one filter, IDS MC will apply them in the order in which you defined them.

An example of how filters work can be helpful in seeing how to define them. In this example, you want to exclude all alarms that originate from Network 10.10.10.0/24 because that network is using some applications that generate large numbers of false positives. However, there are two signatures that are important to you, so you don't want them to be excluded: They are 994 (Traffic Flow Started) and 995 (Traffic Flow Stopped).

1. Begin by defining an exclusive filter. Specify the source address as 10.10.10.0, which is the network that is generating large numbers of false positives. Specify all signatures so that no alarms are sent to Security Monitor.
2. Next, define an inclusive filter. Specify the same source address, which is Network 10.10.10.0. But specify Signatures 994 and 995, which are the ones that you want to include because they are important to you.

By using these two filters, and in this order, you can filter out a large number of alarms that would be false positives. But you can selectively let some of them (Signatures 994 and 995) pass through. This is possible because you defined the exclusive filter first and the inclusive filter next. Note that if you had defined the inclusive filter first, then the exclusive filter would have filtered out all the alarms from Network 10.10.10.0. This is because filters are evaluated in order.

This procedure defines filters for a sensor as described in this example. The example assumes that you have added Device11 in GroupW to your network. Device11 is a 4.x appliance sensor in this example.

To define a filter for a sensor as described in the example, follow these steps:

Step 1 Select **Configuration > Settings**.

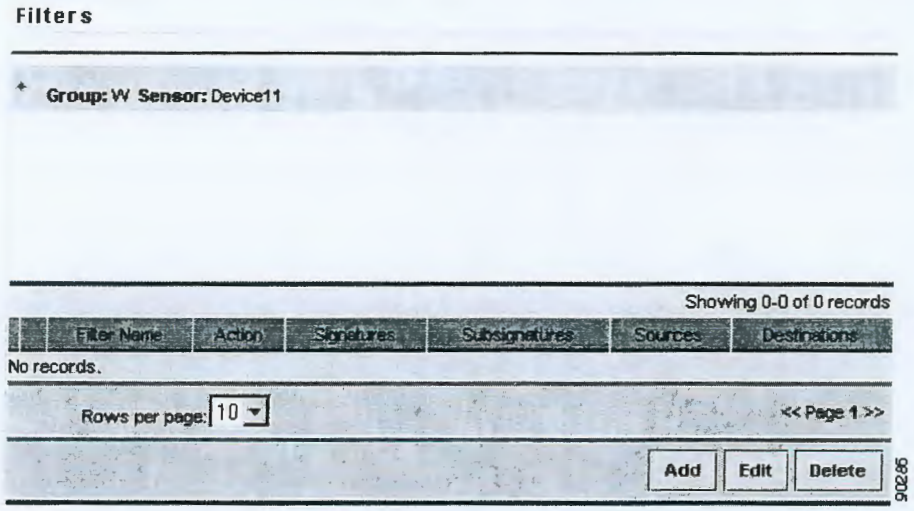
Step 2 In the TOC, click the **Object Selector** handle.

Step 3 In the Object Selector, select Device11, the sensor for which you want to define a filter in this example. Device11 is a 4.x sensor.

The Object Selector closes.

Step 4 In the TOC, select **Filters**.

The Filters page appears. This page shows that no filters have been defined for Device11, the sensor that you selected.



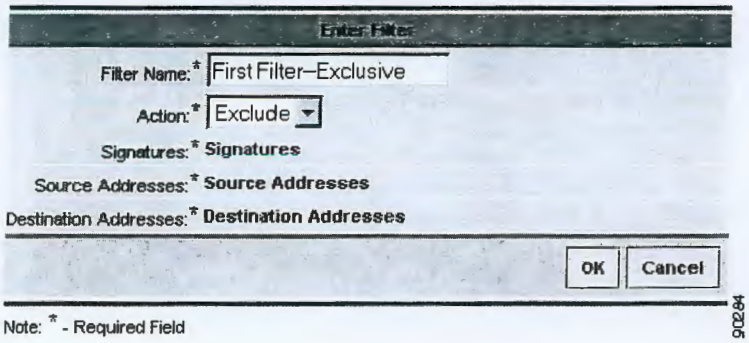
Step 5 To begin defining the exclusive filter in this example, click **Add**.

The Enter Filter page appears.

Step 6 Enter a name for the filter: Use "First Filter--Exclusive"

Step 7 Select the action of **Exclude**.

The Enter Filter page now appears as shown here.

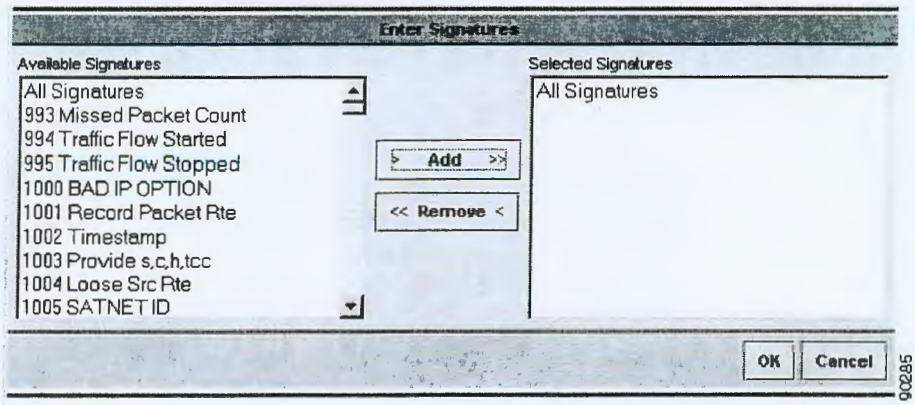


Step 8 Click the **Signatures** link.

The Enter Signatures page appears.

Step 9 On the Enter Signatures page, add **All Signatures** from the Available Signatures field to the Selected Signatures field.

The Enter Signatures page now appears as shown here.



Step 10 Click **OK**.

The Enter Filter page appears again.

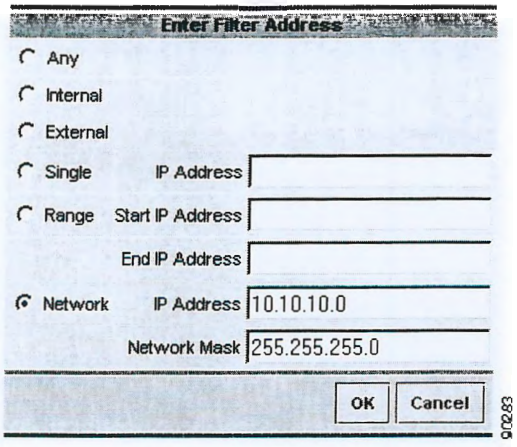
Step 11 Click the **Source Addresses** link.

The Filter Source Addresses page appears.

Step 12 Click **Add**.

The Enter Filter Address page appears.

Step 13 Select the radio button corresponding to Network and enter 10.10.10.0, the network address being used in this example, along with its network mask of 255.255.255.0. The **Enter Filter Address** page now appears as shown here.



Step 14 Click **OK**.

Step 15 The Filter Source Addresses page appears, showing the addition of Network 10.10.10.0 with a subnet mask of 255.25.255.0.

Step 16 Click **OK**.

The Enter Filter page appears again.

Step 17 Click the **Destination Addresses** link.

The Filter Destination Addresses page appears.

Step 18 Click **Add**.

The Enter Filter Address page appears.

Step 19 Select the radio button corresponding to an address of Any and click **OK**.

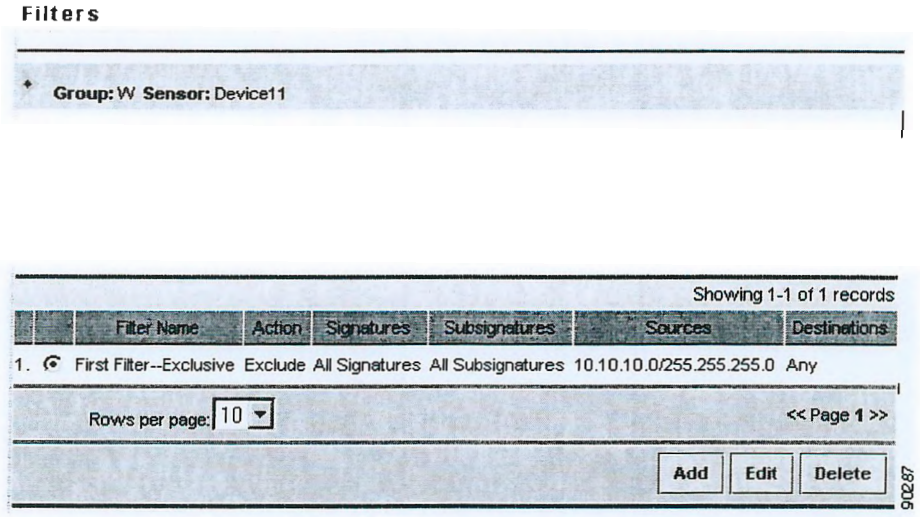
The Filter Destination Addresses page appears, showing the addition of Any.

Step 20 Click **OK**.

The Enter Filter page appears again.

Step 21 Click **OK**.

The Filters page now appears as shown here. You have just finished defining the first filter in this example.

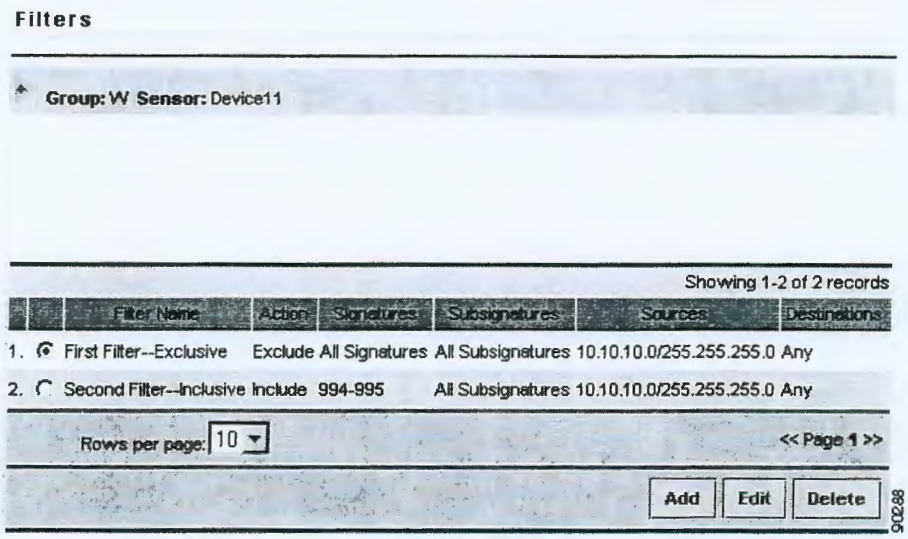


Step 22 To begin defining the inclusive filter in this example, click **Add**.

Step 23 Add a filter with the name "Second Filter--Inclusive" with an action of Include.

Step 24 Continue with this example by adding Signature 994 and Signature 995.

Step 25 Add the same source address and destination address that were used for the first filter, and then display the Filters page again. It should now appear as shown here.



The filter named `First Filter--Exclusive` will be applied first. It will exclude all alarms from Network 10.10.10.0. The filter named `Second Filter--Inclusive` will be applied next. It will allow alarms from Network 10.10.10.0 if they result from Signatures 994 or 995. Signatures 994 and 995 will not be disabled.

Specifying Networks and Hosts that Should Never Be Blocked

You can configure a sensor to block an attack by generating ACL rules for publication to an Cisco IOS router. However, it is important to tune your sensor signatures to identify hosts and networks that should never be blocked. For example, you may have a trusted network device whose normal, expected behavior appears to be an attack. But such a device should never be blocked. Also, trusted, internal networks should never be blocked. Proper tuning reduces the number of false positives and helps ensure proper network operation.

To specify the networks or hosts that should never be blocked when an attack is detected, follow these steps:

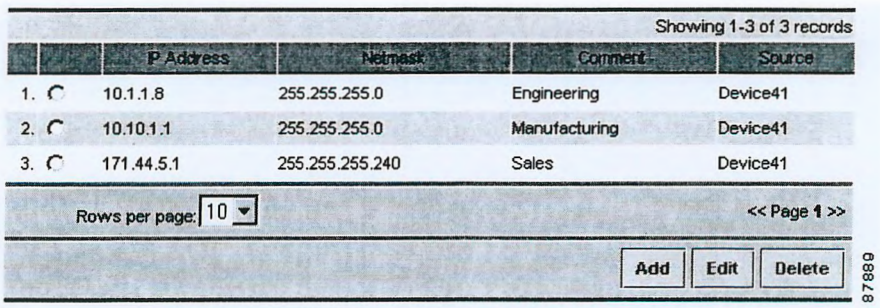
Step 1 Select **Configuration > Settings**.

Step 2 Click the **Object Selector** handle.

Step 3 In the Object Selector, select the sensor for which you want to identify hosts and networks that should be exempt from blocking.

Step 4 In the TOC, select **Blocking > Never Block Addresses**.

The IP Addresses page appears. This page shows the list of devices and networks that are capable of being blocked by configuring the sensor that you selected. On this page, you can add, edit, and delete hosts and networks.



Step 5 To add a host or network to the list of those that should never be blocked by the sensor that you selected, click **Add**.

The Enter Network page appears.

Enter the following information in the Enter Network page:

- IP address
- Network mask
- Comment

Step 6 To edit information associated with a host or network on the list of those that should never be blocked by the sensor that you selected, select the check box adjacent to the address of that host or network, and click **Edit**.

The Enter Network page appears.

Enter the following information on the Enter Network page:

- IP address
- Network mask
- Comment

Step 7 To delete a host or network from the list of those that should never be blocked by the sensor that you selected, select the check box corresponding to the address of that host or network, and click **Delete**.

The host or network that you selected is deleted.

Step 8 To add, edit, or delete additional hosts or networks, repeat Step 2 through Step 7.

Step 9 To continue configuring sensors, select **Configuration > Settings**.

NEC

13128
A.

Comprovação das Especificações Exigidas no Edital 050/2003

7. Rack para equipamentos

Servers
Intel-based servers
Rack-optimized
Universal
Appliance
Storage
Accessories & upgrades
Services
Support
Certification
Education and training
News and awards
Library
HW/SW compatibility

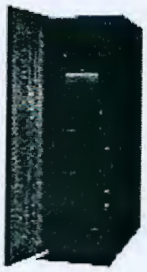
NetBAY42 Enterprise Rack Cabinet

Technical Detai
·Compatibility
·Technical Inform
·Warranty
·Weights & Dime
·Other

$2,649.00 IBM List Price

Model Name:

Part Number: **930842S**



New NetBAY rack cabinets provide a comprehensive selection of rugged, rack solutions tailored for "deep" servers and high-density installations. Cabinet provides 42U of rack space with depth capacity to support "deep" servers up to 28 inches. All models feature a perforated-steel front door to optimize cooling while maintaining security by lock and key. These NetBAY rack cabinets support all current rack-mountable IBM eServer xSeries and Netfinity servers.

Features & Benefits:

Includes side panels and a stabilizer kit
- Robust design allows shipping with preconfigured servers
- Perforated front door provides improved air flow for a fan-free environment
- Lockable front and rear doors maximize security

Provides the most room of all NetBAY racks for cable management

Technical Details

Compatibility

Restrictions:	When servicing or sliding devices out of the NetBAY42 ER or EX, it is required that the front stabilizer plate be used in accordance with the instructions included in the installation/safety publications.
Supported software:	
Hardware prerequisites	
IBM systems:	Netfinity 4500R, Netfinity 4500R Rack Mounted models, Netfinity 5100, Netfinity 5100 Rack Mounted models, Netfinity 5000, Netfinity 5000 Rack Mounted models, Netfinity 5500, Netfinity 5500 M10, Netfinity 5500 M10 Rack Mounted models, Netfinity 5500 M20, Netfinity 5500 M20 Rack Mounted models, Netfinity 5600, Netfinity 5600 Rack Mounted models, Netfinity 6000R, Netfinity 7000 M10 Rack Mounted models, Netfinity 7100, Netfinity 7600, Netfinity 8500 Rack Mounted models, xSeries 200, xSeries 220, xSeries 230, xSeries 240, xSeries 250, xSeries 330, xSeries 340, xSeries 232, xSeries 225, xSeries 235, xSeries 255, xSeries 342, xSeries 345, xSeries 360, xSeries 380, xSeries 440, xSeries Datacenter solutions
Non-IBM systems:	-To obtain proper air flow and allow for servicing of internal devices, the following installation clearances are required: -Service: Front - 1524mm, Rear - 762mm -Operational: Front - 914mm, Rear - 660mm -Tower models are supported if converted to rack configurations using a supported rack conversion kit.
Operating system requirements:	
Adapters:	
Mounting Kit etc.:	Cable requirements are dependent upon the devices installed in the NetBAY42 ER cabinets.
Product Approvals	
Product approval/certifications4:	
Energy Star Compliant:	

Technical Information

Server Option:	Netfinity Rack
Supported Devices:	
Connection to IBM Netfinity Rack Configurator:	
Rack Options:	Caster set
Security Features:	Lockable front/rear door; Lockable side panels

Safety Features:
Cluster Compatible:

-Heavy-duty rack cabinets specifically designed for enterprise environments.
-Ideal solution for environments where multiple server types are required and where an extremely rugged, versatile enclosure is needed to handle demanding enterprise installations.
-Supports up to fourteen Netfinity EXP storage units for massive data storage solutions of over 5 terabytes.
-Standard side panels
-Support for larger servers and better cable management
-Server consolidation supporting
-High-availability, clustering of server nodes
-I/S centralization/control
-Multiple Netfinity Enterprise Rack and Netfinity Enterprise Expansion Cabinets can be installed side-by-side to support your expanding business requirements. These units bolt together to form multi-rack suites to efficiently handle clustering or server consolidation requirements.
-Internal dimensions: Height: 1869mm; Width: 450mm; Depth: 1016mm frame; Depth: 717mm front to rear mounting flanges

93126

Warranty [3]

Limited Warranty period and type:	Three year Customer Carry-in

Weight & Dimentions [6]

Weight:	575lbs
Travel weight:	--
Height:	79.5in
	--
Width:	25.5in
	--
Depth:	43.3in
Operating Temperature (C) (low; high):	
Relative Humidity (%) (low; high):	
Ship Information	340Kg
Box 1	
Weight:	
Height:	2172mm
Width:	762mm
Depth:	1207mm
Box 2	--
Weight:	
Height:	--
Width:	--
Depth:	--
Special ship information:	

Other

Recommendation :	

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0948
Doc: 3696

Important Legal Information

13125

United States

Search

Home | Products & services | Support & downloads | My account | Call 1-888-SHOP-IBM

Select a country

- Servers

Intel processor-based servers

- Rack-optimized
- Universal
- High-performance scalable
- Blade servers
- Storage
- Systems Management
- Accessories & upgrades
- Services
- Support
- Certification
- Education and training
- News and awards
- Literature
- HW/SW compatibility
- Solutions

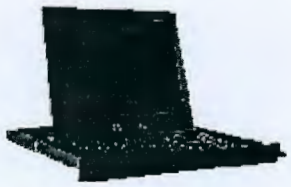
Shopping help

- Warranty info
- Shop by part number
- View cart
- Open saved carts
- Estimate shipping
- Estimate leasing
- Order status
- Returns policy
- Shopping guarantee

Related links:

- Home / home office
- Small & Medium Business
- Government
- Education

NetBAY 1U Flat Panel Monitor Console Kit



IBM Web Price
$2,195.00*
$78.00 /mo. for 36 mos. SuccessLease® for Small Business***
Availability: **Within 2-4 weeks****

Add to cart

This 1U, high-density rack option comes complete with the key components to set up and monitor IBM eServer (logo) xSeries rack servers. It includes a U.S. Space Saver 2 keyboard, 15-inch flat panel monitor, slide rails and cable management and console switch mounting brackets. This rack option provides greater flexibility, saves valuable rack space and adds installation convenience to your NetBAY rack solutions.

Features and Benefits:

High-density allows more room for other rack components
ServerProven support for configuration and compatibility with xSeries servers and NetBAY rack products
3-year limited warranty

General	
Model name	32P1031
Description	NetBAY 1U Flat Panel Monitor Console Kit
IBM Web Price*	$2,195.00
SuccessLease® for Small Business***	$78.00/mo. for 36 mos.
Compatibility	
Hardware prerequisites (System unit)	All xSeries Servers
Product approvals/certifications	BCIQEMC Type Certifications (Taiwan), C-Tick Mark (AS/NZS 3548 Class A), CCIB/CCEE (China), CE MARK (EN 55022 Class A), CSA C22.2 No. 950, FCC Class A - Part 15, GOST (Russia), NOM 019, UL, VDE, VCCI Class A (Japan)
Memory	
Memory (RAM) std	--
Standard features	
Keyboard type standard	Basic 101 key (rubber dome)
Power management	
Sound emissions	
Dimensions	
Weight	37 lbs
Height	1.75 inches
Width	19 inches
Depth	29.6 inches
Warranty	
Limited Warranty period	Three year
Type of Service	Limited warranty
Monitor	
Monitor Included	No

Add to cart

13124
A.

*Price does not include tax or expedited shipping and is subject to change without notice. Reseller prices may vary. IBM does not warrant non-IBM products. PCs shown here, except for Servers and Network Stations, ship with an operating system. All offers subject to availability. IBM reserves the right to alter product offerings and specifications at any time without notice. IBM is not responsible for photographic or typographic errors.

** An estimated ship date will be included with your order confirmation e-mail. Availability does not determine when your order will ship since inventory status may change before your order is final (following the receipt of any credit or payment authorization) as other orders are processed. "In stock" indicates we currently have at least one of the item in stock. Orders are normally held until all the products on the order are in inventory. "Within 2 weeks" indicates that the product should be available in inventory within 2 weeks. "Within 2-4 Weeks" indicates that the product should be available in inventory in 2-4 weeks. To obtain the latest information about the availability of a specific part number, please call 1-888-SHOP-IBM.

*** SuccessLease® for Small Business is offered and administered in the US and Canada by third party providers of business financing who are approved by IBM Global Financing. All terms are provided by third party providers of business financing who are approved by IBM Global Financing.; example of monthly lease payments based on a 36 month term, prespecified purchase option at end of lease, to qualified business customers installing in the US and are for planning purposes only, actual payments may vary. A documentation fee and first month payment due at signing. Any taxes are additional. Other terms and financing structures are available. $750 minimum lease order applies.
SuccessLease® for Small Business

Important Legal Information

Select a country

← Personal computing

Accessories & upgrades

Services

Support

ThinkVantage Technologies

Presentations

News & awards

Library

Request a Catalog

Shopping help

Warranty info

Shop by part number

View cart

Open saved carts

Estimate shipping

Estimate leasing

Order status

Returns policy

Shopping guarantee

Related links:

Home / home office

Small & Medium Business

Government

Education

NetBAY 2X8 Console Switch

IBM Web Price
$1,359.00*
Availability: **In stock****

Add to cart

The NetBAY 2x8 CONSOLE Switch supports up to eight servers from one or two consoles. This modular console switch provides versatility, lower-cost and increased functionality for your rack installation. This option supports universal voltage requirements (100-240V AC) and new locking-cable sets in 7-foot or 12-foot lengths.

Features and Benefits:

Features eight ports to support up to eight servers on a single switch and can be tiered for larger configurations
Utilizes easy to follow user interface
Universal voltage (100-240V AC, 50-60Hz)
Supports new locking cable set or current cable set

General	
Model name	09N4291
Description	NetBAY 2X8 Console Switch
IBM Web Price*	$1,359.00
Compatibility	
Hardware prerequisites (System unit)	xSeries 130, xSeries 135, xSeries 200, xSeries 225, xSeries 220, xSeries 230, xSeries 240, xSeries 250, xSeries 340, xSeries 232, xSeries 342, xSeries 350, xSeries 360, xSeries 370, xSeries 380, xSeries 440, xSeries 235, xSeries 255, xSeries 345, Intelli
Product approvals/certifications	BSMI (Taiwan), C-Tick Mark (AS/NZS 3548 Class A), CSA, EMI, IEC, TUV, UL
Characteristics	
Weight	5.3 lbs
Height	1.7 inches
Width	17 inches
Depth	8 inches

Add to cart

*Price does not include tax or expedited shipping and is subject to change without notice. Reseller prices may vary. IBM does not warrant non-IBM products. PCs shown here, except for Servers and Network Stations, ship with an operating system. All offers subject to availability. IBM reserves the right to alter product offerings and specifications at any time without notice. IBM is not responsible for photographic or typographic errors.

** An estimated ship date will be included with your order confirmation e-mail. Availability does not determine when your order will ship since inventory status may change before your order is final (following the receipt of any credit or payment authorization) as other orders are processed. "In stock" indicates we currently have at least one of the item in stock. Orders are normally held until all the products on the order are in inventory. "Within 2 weeks" indicates that the product should be available in inventory within 2 weeks. "Within 2-4 Weeks" indicates that the product should be available in inventory in 2-4 weeks. To obtain the latest information about the availability of a specific part number, please call 1-888-SHOP-IBM.

13122
4.

← Personal computing

Accessories & upgrades

Services

Support

ThinkVantage Technologies

Presentations

News & awards

Library

Request a Catalog

Shopping help

Warranty info

Shop by part number

View cart

Open saved carts

Estimate shipping

Estimate leasing

Order status

Returns policy

Shopping guarantee

Related links:

Home / home office

Small & Medium Business

Government

Education

NetBAY Console Cable 12FT

IBM Web Price
$65.00*
Availability: **Within 2 weeks****

Add to cart

Options by IBM

13121
A

No matter what system you buy or own, chances are you bought it for one important reason: to help boost your productivity. So where do you turn when it's time to expand? The answer is simple--IBM. Options by IBM offers hundreds of peripherals and system enhancements for both IBM and non-IBM systems that let you make the most of your computing investment.

General	
Model name	94G7447
Description	NetBAY Console Cable 12FT
IBM Web Price*	$65.00
Compatibility	
Restrictions	--
Hardware prerequisites (System unit)	Netfinity Rack 9306 model 900, Netfinity 4500R, Netfinity 4500R Rack Mounted models, Netfinity 5000, Netfinity 5000 Rack Mounted models, Netfinity 5100, Netfinity 5500, Netfinity 5500 M10, Netfinity 5500 M10 Rack Mounted models, Netfinity 5500 M20, Netfi
Hardware prerequisites(Adapters)	Console Server Selector Switch
Hardware prerequisites (Mounting kit etc.)	--
Supported software	--
Product approvals/certifications	--
Warranty	
Limited Warranty period	One year
Type of Service	Customer Carry-in Exchange (CCE)

Add to cart

*Price does not include tax or expedited shipping and is subject to change without notice. Reseller prices may vary. IBM does not warrant non-IBM products. PCs shown here, except for Servers and Network Stations, ship with an operating system. All offers subject to availability. IBM reserves the right to alter product offerings and specifications at any time without notice. IBM is not responsible for photographic or typographic errors.

** An estimated ship date will be included with your order confirmation e-mail. Availability does not determine when your order will ship since inventory status may change before your order is final (following the receipt of any credit or payment authorization) as other orders are processed. "In stock" indicates we currently have at least one of the item in stock. Orders are normally held until all the products on the order are in inventory. "Within 2 weeks" indicates that the product should be available in inventory within 2 weeks. "Within 2-4 Weeks" indicates that the product should be available in inventory in 2-4 weeks. To obtain the latest information about the availability of a specific part number, please call 1-888-SHOP-IBM.

Important Legal Information

951

← Personal computing

Accessories & upgrades

Services

Support

ThinkVantage Technologies

Presentations

News & awards

Library

Request a Catalog

Shopping help

Warranty info

Shop by part number

View cart

Open saved carts

Estimate shipping

Estimate leasing

Order status

Returns policy

Shopping guarantee

Related links:

Home / home office

Small & Medium Business

Government

Education

Blank Filler Panel Kit

Options by IBM

IBM Web Price
$55.00*
Availability: **Within 2 weeks****

Add to cart

13120
A.

Provides two 1U panels, one 3U panel and one 5U panel to cover unused rack mounting space in the IBM Netfinity Rack.

General	
Model name	94G6670
Description	Blank Filler Panel Kit
IBM Web Price*	$55.00
Compatibility	
Restrictions	--
Hardware prerequisites (System unit)	Netfinity Rack 9306 model 900
Hardware prerequisites(Adapters)	--
Hardware prerequisites (Mounting kit etc.)	--
Supported software	--
Product approvals/certifications	--
Warranty	
Limited Warranty period	One year
Type of Service	Customer Carry-in Exchange (CCE)

Add to cart

*Price does not include tax or expedited shipping and is subject to change without notice. Reseller prices may vary. IBM does not warrant non-IBM products. PCs shown here, except for Servers and Network Stations, ship with an operating system. All offers subject to availability. IBM reserves the right to alter product offerings and specifications at any time without notice. IBM is not responsible for photographic or typographic errors.

** An estimated ship date will be included with your order confirmation e-mail. Availability does not determine when your order will ship since inventory status may change before your order is final (following the receipt of any credit or payment authorization) as other orders are processed. "In stock" indicates we currently have at least one of the item in stock. Orders are normally held until all the products on the order are in inventory. "Within 2 weeks" indicates that the product should be available in inventory within 2 weeks. "Within 2-4 Weeks" indicates that the product should be available in inventory in 2-4 weeks. To obtain the latest information about the availability of a specific part number, please call 1-888-SHOP-IBM.

Important Legal Information

352

NetBAY Rack Power Distribution Unit

Technical Detai
·Compatibility
·Warranty
·Weight & Dimen

$179.00 IBM List Price

Part Number: **37L6866**

IIII

13119
LA

The NetBAY RACK POWER DISTRIBUTION UNIT (PDU) is a low-cost, basic PDU that supports up to seven devices in which electrical demands do not exceed 15 amps. This universal voltage PDU provides versatility, lower-cost and increased function for your rack installation. The NetBAY Rack PDU is modular, can help you satisfy a wide array of rack power requirements and supports one universal voltage (100-240V) AC power input and seven outputs. This PDU gives you increased flexibility and versatility as your needs require housing multiple servers and other equipment in a single cabinet and you must consider the power needs of each device and the effect of the combined needs on your power source.

Features & Benefits:

- Universal voltage (100-240V AC, 50-60Hz)
- Brackets for vertical and horizontal rack mounting
- Two pole 15-amp circuit breaker with time-delay protection
- Seven IEC 320-C13 power outlets
- One IEC 320-C20 power inlet
- Cable retention aids

Technical Details

Characteristics

Power adapter type:	
Input voltage:	--
Output voltage:	--
Form factor:	
Connector:	
Cable length (m):	--
Power (Watts):	--
Battery technology:	
Battery voltage:	--
Battery intelligence:	
Other Information:	**-Low-cost, basic PDU that supports up to seven devices in which current demands do not exceed 3600 watts.** **-Universal voltages (100-240V AC 50/60Hz)** **-Two pole 20-amp circuit breaker with time delay protection** **-Ten IEC 320-C13 power outlets** **-One IEC 320-C20 power inlet** **-Reversible side mounting brackets for vertical and horizontal rack mounting** **-Cable retention aids** **-Power indicator light**

Compatibility

Restrictions:	
Hardware prerequisites:	
System Units	
_ IBM Systems:	Netfinity Enterprise Rack, Netfinity Rack, Netfinity NetBAY22, xSeries 130, xSeries 235, xSeries 255, xSeries 135, xSeries 330, xSeries 232, xSeries 250, xSeries 342, xSeries 360, xSeries 345, xSeries 380, xSeries 440, IntelliStation R Pro (6851) -Require an EIA 310D standard rack cabinet. 1 U of space is required or space available in the sidewall compartment of a Netfinity Rack or Netfinity Enterprise Rack
_ Non-IBM systems:	
Operating system requirements:	
Adapters:	
Mounting kit etc.:	

Power Cable Type C12

Options by IBM

IBM Web Price
$19.00*
Availability: **In stock****

Add to cart

13118
A-

To connect server system units and other devices to a PDU or UPS in a rack enclosure when longer power cables are required.

General	
Model name	94G7448
Description	Power Cable Type C12
IBM Web Price*	$19.00
Compatibility	
Restrictions	--
Hardware prerequisites (System unit)	Netfinity Rack 9306 model 900
Hardware prerequisites(Adapters)	--
Hardware prerequisites (Mounting kit etc.)	--
Supported software	--
Product approvals/certifications	--
Warranty	
Limited Warranty period	One year
Type of Service	Customer Carry-in Exchange (CCE)

Add to cart

*Price does not include tax or expedited shipping and is subject to change without notice. Reseller prices may vary. IBM does not warrant non-IBM products. PCs shown here, except for Servers and Network Stations, ship with an operating system. All offers subject to availability. IBM reserves the right to alter product offerings and specifications at any time without notice. IBM is not responsible for photographic or typographic errors.

** An estimated ship date will be included with your order confirmation e-mail. Availability does not determine when your order will ship since inventory status may change before your order is final (following the receipt of any credit or payment authorization) as other orders are processed. "In stock" indicates we currently have at least one of the item in stock. Orders are normally held until all the products on the order are in inventory. "Within 2 weeks" indicates that the product should be available in inventory within 2 weeks. "Within 2-4 Weeks" indicates that the product should be available in inventory in 2-4 weeks. To obtain the latest information about the availability of a specific part number, please call 1-888-SHOP-IBM.

Important Legal Information

DOC.
000233

CPL/AC

PREGÃO
050/2003

LOCAÇÃO DE EQUIPAMENTOS DE INFORMÁTICA INCLUINDO ASSISTÊNCIA TÉCNICA E TREINAMENTO

NEC DO BRASIL S/A – MANUAL VOLUME I

2003
PASTA 23

Roteador Tipo 2 doc1

Data Sheet

Cisco **1751** Modular Access Router

Cisco 1751 Modular Access Router is ideally suited to help you evolve your organization into an e-Business. It supports e-Business features such as VPNs; secure Internet, intranet, and extranet access with optional firewall technology; broadband DSL and cable connectivity; and multiservice voice/video/data/fax integration. The Cisco 1751 Modular Access Router offers:

- Flexibility to adapt to changing requirements
- Modularity that allows you to individually configure the system to meet specific business needs
- Investment protection with features and performance to support new WAN services such as broadband DSL and cable access, multiservice voice/data integration, and VPNs
- Integration of multiple network functions, including an optional firewall VPN, and data service unit/channel service unit (DSU/CSU) to simplify deployment and management

The Cisco 1751 Router delivers these capabilities with the power of Cisco IOS Software in a modular integrated access solution. The Cisco 1751 Router provides a cost-effective solution to support e-Business applications through a comprehensive feature set including support for:

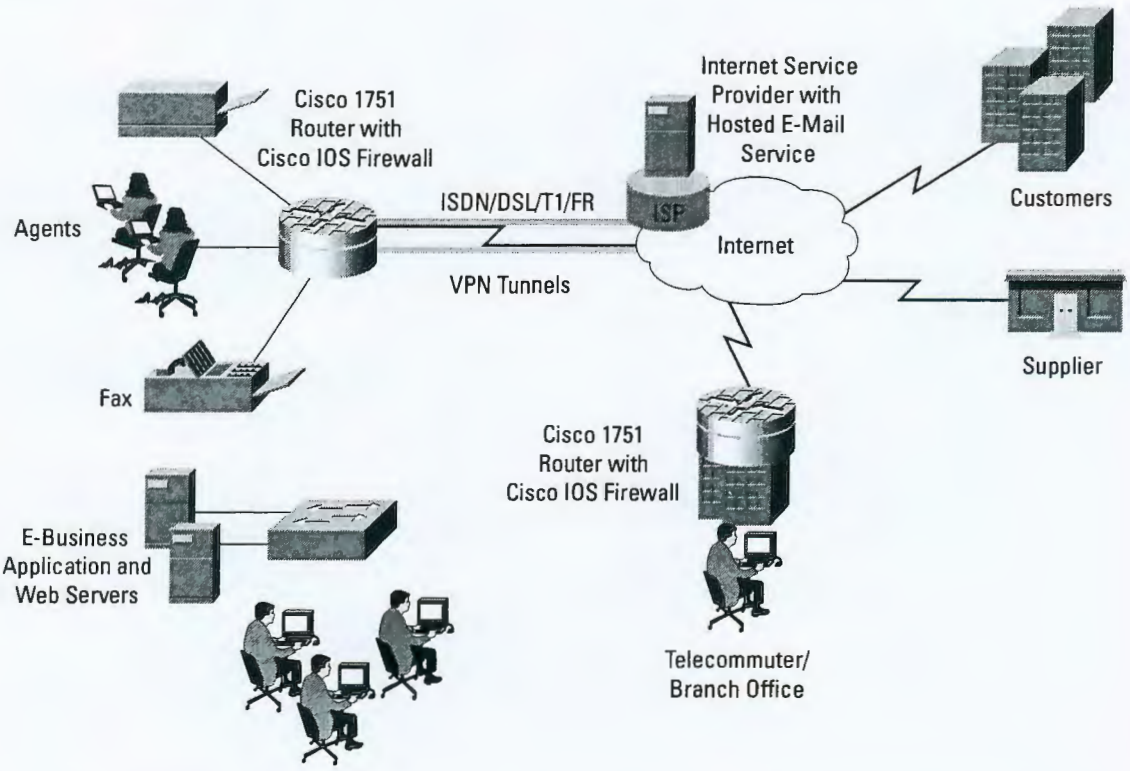
- Multiservice voice/fax/data integration
- Secure Internet, intranet, and extranet access with VPN and firewall
- Integrated broadband DSL connectivity
- VLAN support (IEEE 802.1Q)

The Cisco 1751 Router, a member of the Cisco 1700 Family, features a modular architecture that enables cost-effective upgrades and additions of WAN and voice interfaces. Integrated network services and functions, such as optional firewall, DSU/CSU, and VPN features, reduce the complexity of deploying and managing e-Business solutions. The Cisco 1751 Router offers investment protection when your business needs it, with a RISC architecture and features to support new technologies and applications such as voice/video/data/fax integration and VPNs. See Figure 2.

Figure 1
The Cisco 1751 Router delivers a versatile e-Business WAN access solution.

Figure 2

Cisco 1751 Routers provide all necessary capabilities to connect to the Internet and communicate with vendors, customers, and other employees and offices.



The Cisco 1751 Router is available in two models that enable you to easily tailor an access solution to suit your e-Business requirements today and in the future. See Table 1.

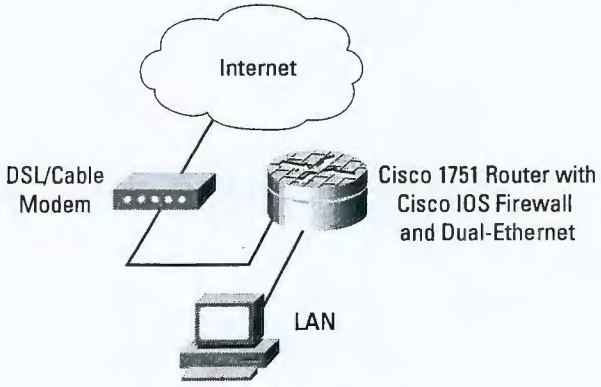
Table 1 The Cisco 1751 Modular Access Router

Cisco 1751 Base Model	Includes everything an office needs for data networking now (16 MB Flash, 32 MB DRAM, and Cisco IOS IP software feature set), with a simple upgrade path to full voice functionality. WAN interface cards are available separately.
Cisco 1751-V Multiservice Model	Includes all the features needed for immediate integration of data and voice services with support for up to two voice channels (32 MB Flash and 64 MB DRAM, one DSP (PVDM-256K-4), and Cisco IOS IP Plus Voice feature set). Voice and WAN interface cards are available separately.

All Cisco 1751 models offer three modular slots for voice and data interface cards, an autosensing 10/100BaseT Fast Ethernet LAN port supporting standards-based IEEE 802.1Q VLAN, a console port, and an auxiliary port. The Cisco 1751 Router supports the same WAN interface cards as the Cisco 1600, 1700, 2600, and 3600 Series routers, and the same voice interface cards and voice-over-IP (VoIP) technology as the Cisco 1700, 2600, and 3600 Series routers. This simplifies support requirements. The WAN interface cards support a wide range of services, including synchronous and asynchronous serial, Integrated Services Digital Network Basic Rate Interface (ISDN BRI), ADSL,

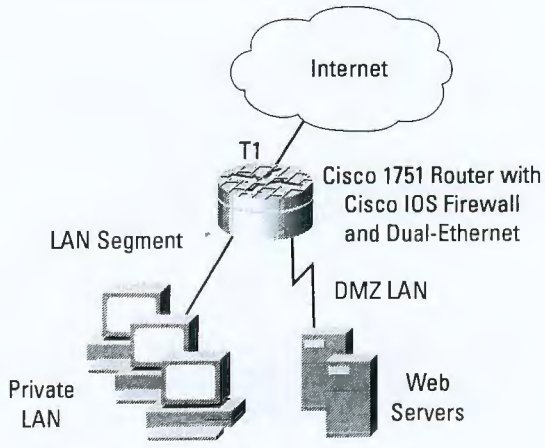
and serial with DSU/CSU options for primary and backup WAN connectivity. The voice interface cards support Foreign Exchange Office (FXO), Foreign Exchange Station (FXS), Network and User Side Voice BRI (ISDN BRI NT/TE), Ear & Mouth (E&M), direct inward dial (DID), and T1/E1 Multiflex VWICs. Additionally, an Ethernet interface card provides the Cisco 1751 Router with dual-Ethernet capability to support the external broadband modem devices. See Figure 3.

Figure 3
Cisco 1751 Router Incorporating Ethernet WAN Interface Card (WIC) Deployed with Broadband Modem



In addition, dual-Ethernet capability on the Cisco 1751 Router enables the creation of perimeter/DMZ (demilitarized zone) LANs to enhance security by physically separating private and public data. See Figure 4.

Figure 4
Cisco 1751 Router Incorporating Ethernet WIC to Deploy Perimeter/DMZ LAN



Combined, these interfaces support a comprehensive set of applications, including multiservice voice/video/data/fax integration, Frame Relay, ISDN BRI, SMDS, X.25, broadband DSL and cable services, and VPNs.

Key Benefits

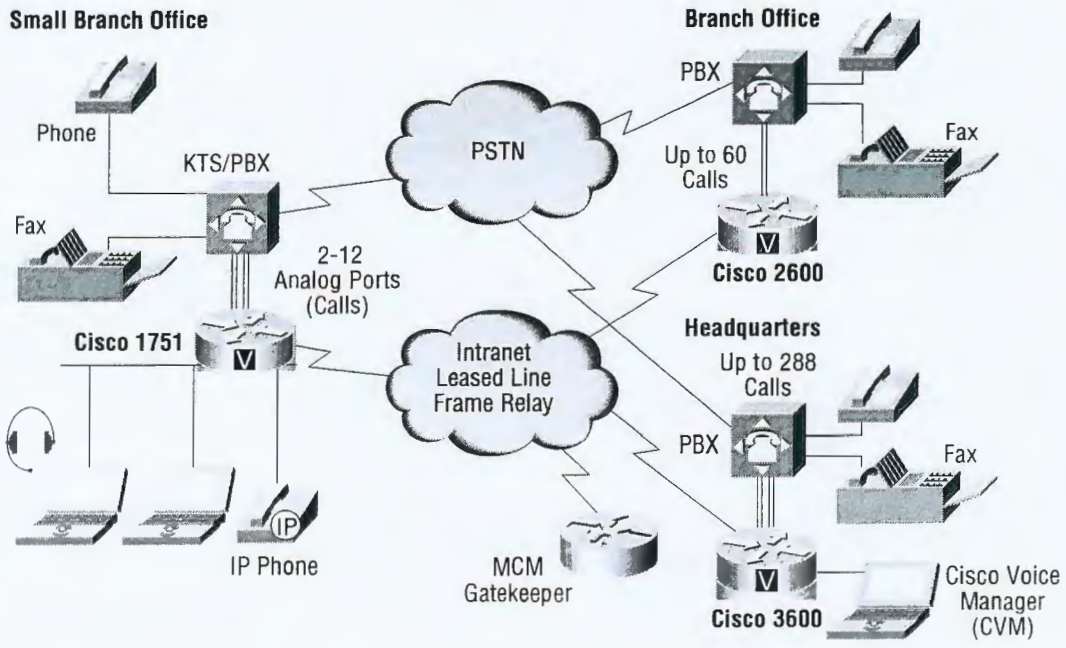
The Cisco 1700 Series routers support the value of end-to-end Cisco network solutions with the following benefits:

Flexibility—The modular Cisco 1751 Router adapts easily to fit the needs of growing businesses. Interchangeable WAN interface cards enable easy additions or changes in WAN technologies without requiring a forklift upgrade of the entire platform. Modular data and voice slots enable users to tailor data and voice services as needed. With the ability to use the same field-upgradable WAN and voice interface cards across multiple Cisco access router platforms, the Cisco 1751 Router reduces requirements for spare parts inventory and support training.

Multiservice Access—For businesses that want to become e-Businesses and incorporate applications that integrate multiservice voice/video/data/fax capabilities now or in the future, the Cisco 1751 Router offers a flexible, cost-effective answer. The Cisco 1751 Router enables network managers to save on long-distance interoffice billing costs. It also interoperates with next-generation voice-enabled applications such as integrated messaging and Web-based call centers. The Cisco 1751 Router works with the existing telephone infrastructure—phones, fax machines, key telephone systems (KTS) units, and PBX (including digital PBXs)—minimizing capital costs. See Figure 5.

Figure 5

Voice/video/data/fax integration. The Cisco 1751 Router integrates data and voice capabilities, significantly lowering toll charges for small- and medium-sized businesses and enterprise small branch offices.



Lower Cost of Ownership—The Cisco 1751 Router provides a complete solution for integrated voice and data access in a single product, eliminating the need to install and maintain a large number of separate devices. You can combine optional functions—including a voice gateway, dynamic firewall, VPN tunnel server, DSU/CSU, ISDN network

termination-1 (NT1) device, and more—to reduce deployment and management costs. This solution can be managed remotely using network management applications such as CiscoWorks2000 and CiscoView or any SNMP-based management tool.

Investment Protection—The Cisco 1751 Router RISC architecture, Cisco IOS Software, and modular slots provide solid investment protection. The Cisco 1751 incorporates services such as multiservice voice/video/data/fax integration, VPNs, and broadband DSL and cable communications to enable today's successful e-Business. An internal expansion slot on the mother- board offers the ability to support hardware-assisted IPSec data encryption at T1/E1 speeds.

For a complete list of Cisco 1751 Router features and benefits, see Table 2.

Table 2 Key Features and Benefits

Features	Benefits
Flexibility	
Full Cisco IOS Software support, including multiprotocol routing (IP, IPX, Apple Talk, IBM/ SNA) and bridging	• Provides the industry's most robust, scalable, and feature-rich internetworking software support using the de facto standard networking software for the Internet and private WANs • Part of the Cisco end-to-end network solution
Integrated Voice and Data Networking	
Cisco 1751 router chassis accepts both WAN and voice interface cards	• Reduces long-distance toll charges by allowing the data network to carry interoffice voice and fax traffic • Works with existing handsets, key units, and PBXs, eliminating the need for a costly phone-equipment upgrade
Modular Architecture	
Accepts an array of WAN and voice interface cards	• Adds flexibility and investment protection
WAN interface cards and voice interface cards are shared with Cisco 1600, 1700, 2600, and 3600 routers	• Reduce cost of maintaining inventory • Lower training costs for support personnel • Protect investments through re-use on various platforms
Autosensing 10/100 Fast Ethernet	• Simplifies migration to Fast Ethernet performance in the office
Expansion Slot on Motherboard	• Allows expandability to support hardware-assisted encryption at T1/E1 speeds • Allows support for future technologies
Dual DSP Slots	• Allow expandability to support additional voice channels
Security	
The Cisco IOS Firewall Feature Set includes context-based access control for dynamic firewall filtering, denial-of-service detection and prevention, Java blocking, real-time alerts, Intrusion Detection System (IDS), and encryption	• Allows internal users to access the Internet with secure, per-application-based, dynamic access control, while preventing unauthorized Internet users from accessing the internal LAN

Table 2 Key Features and Benefits (Continued)

Features	Benefits
IPSec DES and 3DES	• Enable creation of VPNs by providing industry-standard data privacy, integrity, and authenticity as data traverses the Internet or a shared public network • Supports up to 168-bit encryption
Hardware-Based Encryption Using Optional VPN Module	• Supports wire-speed encryption up to T1/E1 speeds
Device Authentication and Key Management	
IKE, X.509v3 digital certification, and support for certificate enrollment protocol (CEP) with certification authorities (CAs) such as Verisign and Entrust	• Ensure proper identity and authenticity of devices and data • Enable scalability to very large IPSec networks through automated key management
User Authentication	
PAP/CHAP, RADIUS, TACACS+	• Support all leading user identity verification schemes
VPN Tunneling	
IPSec, GRE, L2TP, L2F	• Offer choice of standards-based tunneling methods to create VPNs for IP and non-IP traffic • Allow standards-based IPSec or L2TP client to interoperate with Cisco IOS tunneling technologies • Fully interoperable with public certificate authorities and IPSec standards-based products • Part of the scalable Cisco end-to-end VPN solution portfolio
Cisco Easy VPN client	• Allows the router to act as remote VPN client and have VPN policies pushed down from the VPN concentrator
Cisco Unified VPN Access Server	• Allows the router to terminate remote access VPNs initiated by mobile and remote workers running Cisco VPN client software on PCs; and allows the router to terminate site-site VPNs initiated by IOS routers using the Cisco Easy CPN client feature
Management	
IEEE 802.1Q VLAN Support	• VLANs enable efficient traffic separation, provide better bandwidth utilization, and alleviate scaling issues by logically segmenting the physical LAN infrastructure into different subnets
Manageable via SNMP (CiscoView, CiscoWorks2000), Telnet, and console port	• Allow central monitoring, configuration, and diagnostics for all functions integrated in the Cisco 1751 router, reducing management time and costs
Cisco SDM	• Simplifies router and security configuration through smart wizards to enable customers to quickly and easily deploy, configure and monitor a Cisco access router without requiring knowledge of Cisco IOS Command Line Interface (CLI)

Table 2 Key Features and Benefits (Continued)

Features	Benefits
Ease of Use and Installation	
Cisco ConfigMaker, SETUP configuration utility, AutoInstall, color-coded ports/cables, and LED status indicators	• Simplifies and reduces deployment time and costs with graphical LAN/VPN policy configurator; command-line, context-sensitive configuration questions; and straightforward cabling • LEDs allows quick diagnostics and troubleshooting
Network Address Translation (NAT) and Easy IP	• Simplifies deployment and reduces Internet access costs
QoS	
CAR, Policy Routing, WFQ, PQ/CBWFQ, GTS, RSVP, DSCP, cRTP, MLPPP and LFI	• Allocates WAN bandwidth to priority applications for improved performance
Reliability and Scalability	
Cisco IOS Software, dial-on-demand routing, dual-bank Flash memory, scalable routing protocols such as OSPF, EIGRP, and HSRP	• Improves network reliability and enables scalability to large networks
Broadband Connectivity Options	
ADSL and cable connectivity deliver business-class broadband access	• Leverage broadband access technologies like cable and DSL to increase WAN connectivity speeds and reduce WAN access costs • The Cisco 1751 supports ADSL connectivity with ADSL WIC • Cable connectivity with the Cisco 1751 and optional integrated Cisco uBR910 Series Cable DSU deliver business-class broadband access
Device Integration	
Integrated router, voice gateway, firewall, encryption, VPN tunnel server, DSU/CSU, and NT1 in a single device	• Reduce costs and simplifies management

Cisco IOS Technology

Internet and Intranet Access

Cisco IOS Software provides an extensive set of features that make the Cisco 1751 Router ideal for flexible, high-performance communications across both intranets and the Internet:

- Multiprotocol routing (IP, IPX, and AppleTalk), IBM/SNA, and transparent bridging over ISDN, asynchronous serial, and synchronous serial such as leased lines, Frame Relay, SMDS, Switched 56, X.25, and X.25 over ISDN D
- WAN optimization—including dial-on-demand routing (DDR), bandwidth-on-demand (BOD) and OSPF-on-demand circuit, Snapshot routing, compression, filtering, and spoofing to reduce WAN costs

Security

Cisco IOS Software supports an extensive set of basic and advanced network security features, including access control lists (ACLs); user authentication, authorization, and accounting (such as PAP/CHAP, TACACS+, and RADIUS); and data encryption. To increase security, the integrated Cisco IOS Firewall Feature Set protects internal LANs from attacks with context-based access control (CBAC) and Intrusion Detection (IDS), while IPSec tunneling with data encryption standard DES and 3DES encryption provide standards-based data privacy, integrity, and authenticity as data travels through a public network. Additionally, remote management applications, such as Cisco Security Device Manager (SDM), make it easier than ever to deploy and monitor security applications on your Cisco router.

The Cisco 1700 Series routers support the Cisco Easy VPN client feature that allows the routers to act as remote VPN clients. As such, these devices can receive predefined security policies from the headquarters' VPN head-end, thus minimizing configuration of VPN parameters at the remote locations. This solution makes deploying VPN simpler for remote offices with little IT support or for large deployments where it is impractical to individually configure multiple remote devices. While customers wishing to deploy and manage site-to-site VPN would benefit from Cisco Easy VPN client because of its simplification of VPN deployment and management, managed VPN service providers and enterprises who must deploy and manage numerous remote sites and branch offices with IOS routers for VPN will realize the greatest benefit.

The Cisco 1700 Series routers also support the Cisco Unified VPN Access Server feature that allows a Cisco 1700 router to act as a VPN head-end device. In site-to-site VPN environments, the Cisco 1700 router can terminate VPN tunnels initiated by the remote office routers using the Cisco Easy VPN client. Security policies can be pushed down to the remote office routers from the Cisco 1700 Series routers. In addition to terminating site-to-site VPNs, a Cisco 1700 Series router running the Unified VPN Access Server can terminate remote access VPNs initiated by mobile and remote workers running Cisco VPN client software on PCs. This flexibility makes it possible for mobile and remote workers, such as sales people on the road, to access company intranet where critical data and applications exist.

For remote access, VPNs, Layer 2 Forwarding (L2F), and Layer 2 Tunneling Protocol (L2TP) combine with IPSec encryption to provide a secure multiprotocol solution for IP, IPX, and AppleTalk traffic, and more. Mobile users can dial in to a service provider's local point of presence (POP) and data is "tunneled" (or encapsulated inside a second protocol such as IPSec or L2TP) back to the Cisco 1751 router to securely access the corporate network via the Internet.

Cisco IOS Software QoS Features

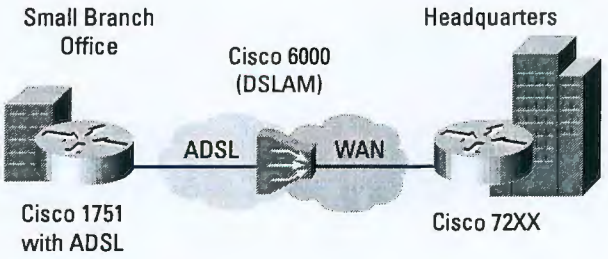
Through Cisco IOS Software, the Cisco 1751 Router delivers quality of service (QoS) capabilities, including Resource ReSerVation Protocol (RSVP), Weighted Fair Queuing (WFQ), Committed Access Rate (CAR), and IP Precedence. These features enable businesses to prioritize traffic on their networks by user, application, traffic type, and other parameters, to ensure that business-critical data and delay-sensitive voice are appropriately prioritized.

Because the Cisco 1751 Router provides robust voice compression, up to 8 voice calls can occupy a single 64K data channel simultaneously, without compromising data performance. Cisco IOS voice compression technology integrates data and voice traffic to enable efficient use of existing data networks.

High-Performance Architecture for VPNs and Broadband Service

A robust RISC architecture and Cisco IOS features enable the Cisco 1751 Router to support VPN applications with tunneling and security, as well as DSL, cable, and other broadband access technologies. An internal slot on the Cisco 1751 motherboard supports an optional VPN module that provides hardware-assisted IPSec DES and 3DES encryption at T1/E1 speeds. The Cisco 1751 Router equipped with the WIC-1ADSL supports VPN over ADSL service. See Figure 6. The Cisco 1751 Router with the uBR910 series cable DSU supports business-class broadband cable access. The Ethernet WIC (WIC-1ENET) provides an alternate method of deploying DSL/cable Internet access with the use of an external modem. In some cases, the ISP provides the broadband modem.

Figure 6
The Cisco 1751 Router, deployed in conjunction with the ADSL WIC, enables SMB and small branch customers to reap the benefits of ADSL.



Network Management and Ease of Installation

The Cisco 1751 Router supports a range of network-management and ease-of-installation tools:

- The Cisco Security Device Manager (SDM) is an intuitive, web-based device management tool embedded within the Cisco IOS access routers. SDM simplifies router and security configuration through smart wizards to enable customers to quickly and easily deploy, configure and monitor a Cisco access router without requiring knowledge of Cisco IOS Command Line Interface (CLI). For more information visit www.Cisco.com/go/sdm.
- Cisco ConfigMaker is a Windows wizard-based tool designed to configure a small network of Cisco routers, switches, hubs, and other network devices from a single PC. This tool makes it easy to configure value-add security features such as the Cisco IOS Firewall Feature Set, IPSec encryption, and network address translation (NAT); establish VPN policies (including QoS and security); and configure the Dynamic Host Configuration Protocol (DHCP) server.
- CiscoWorks for Windows, a comprehensive network management solution for small to medium sized networks that provides Web-based network monitoring and device configuration management.
- CiscoWorks2000, the industry-leading Web-based network management suite from Cisco, simplifies tasks such as network inventory management and device change, rapid software image deployment, and troubleshooting.
- For service providers, Cisco Service Management (CSM) provides an extensive suite of service management solutions to enable planning, provisioning, monitoring, and billing.

Extending Cisco End-to-End Solutions

As part of the comprehensive Cisco end-to-end networking solution, the Cisco 1700 Series routers enable businesses to extend a cost-effective, seamless network infrastructure to the small branch office. The Cisco 1700 Family of access routers includes the Cisco 1751 Router and Cisco 1721 Router—a modular device optimized for data-only connections. WAN cards work with both devices, as well as with Cisco 1600, 2600, and 3600 Series routers. They are powered by Cisco IOS Software for robust WAN service between branches and central offices in organizations with multiple sites. Both feature RISC-based processors to provide performance for encryption and support for emerging broadband technologies.

The Cisco 1751 Router also shares VoIP technology and analog voice interface cards with Cisco 2600 and 3600 Series routers. This feature provides an end-to-end solution for multiservices communications between offices, simplifying inventory needs and leveraging IT expertise across more devices in an organization.

For a complete list of physical interfaces, see Tables 3, 4, 5, and 6.

Table 3 Physical Interfaces/Architecture

One 10/100 BaseT Fast Ethernet Port (RJ45)	Automatic speed detection; automatic duplex negotiation; VLAN support
One Voice Interface Card Slot	Supports a single voice interface card with two ports per card
Two WAN Interface Card/Voice Interface Card Slots	Supports any combination of up to two WAN interface cards or voice interface cards
Ethernet WAN Interface Cards	Supports PPP and PPPoE; operates in full and half-duplex modes
One Auxiliary (AUX) Port	RJ-45 jack with RS232 interface (plug compatible with Cisco 2500 Series AUX port); asynchronous serial DTE with full modem controls (CD, DSR, RTS, CTS); asynchronous serial data rates up to 115.2 kbps
One Console Port	RJ-45 jack with RS232 interface (plug compatible with Cisco 1000/1600/2500 series console ports); asynchronous serial DTE; transmit/receive rates up to 115.2 kbps (default 9600 bps, not a network data port); no hardware handshaking such as RTS/CTS
One Internal Expansion Slot	Supports hardware-assisted services such as encryption (up to T1/E1)
RISC Processor	Motorola MPC860P PowerQUICC at 48MHz

Table 4 WAN Support

Asynchronous Serial Interfaces on Serial WAN Interface Cards	Interface speed: up to 115.2 Kbps; asynchronous serial protocols: Point-to-Point Protocol (PPP), Serial Line Internet Protocol (SLIP); asynchronous interface; EIA/TIA-232
ISDN WAN Interface Cards	ISDN dialup and ISDN leased line (IDSL) at 64 and 128 Kbps; encapsulation over ISDN leased line; Frame Relay and PPP
ADSL WAN Interface Cards	Supports ATP adaption Layer 5 (AAL5) services and applications; interoperates with Alcatel DSLAM with Alcatel chipset and Cisco 6130/6260 DSLAM with Globespan chipset; ANSI T1.413 issue 2 and ITU 992.1 (G.DMT) compliant

Table 5 WAN Interface Cards for the Cisco 1751 Router

Module	Description
WIC-1T	One serial, async, and sync (T1/E1)
WIC-2T	Two serial, async, and sync (T1/E1)
WIC-2A/S	Two low-speed serial (up to 128 kbps), async, and sync
WIC-1B-S/T	One ISDN BRI S/T
WIC-1B-U	One ISDN BUI U with integrated NT1
WIC-1DSU-56K4	One integrated 56/64-kbps, four-wire DSU/CSU
WIC-1DSU-T1	One integrated T1/fractional T1 DSU/CSU
WIC-1ADSL	One-port ADSL interface
WIC-1ENET	One-port 10BaseT Ethernet Interface
WIC-1SHDSL	One-port G.SHDSL interface
WIC-1AM	One-port V.90 analog modem WIC
WIC-2AM	Two-portV.90 analog modem WIC

Table 6 Voice Interface Cards for the Cisco 1751

VIC-2FXS	Two-port FXS voice/fax interface card for voice/fax network module
VIC-2DID	Two-port DID (direct inward dial) voice/fax interface card
VIC-2FXO	Two-port FXO voice/fax interface card for voice/fax network module
VIC-2FXO-EU	Two-port FXO voice/fax interface card for Europe
VIC-2FXO-MI	Two-port FXO voice/fax interface card with battery reversal detection and Caller ID support (for US, Canada, and others) [enhanced version of the VIC-2FXO]
VIC-2FXO-M2	Two-port FXO voice/fax interface card with battery reversal detection and Caller ID support (for Europe) [enhanced version of the VIC-2FXO-EU]
VIC-2FXO-M3	Two-port FXO voice/fax interface card for Australia
VIC-2E/M	Two-port E&M voice/fax interface card for voice/fax network module
VIC-2BRI-NT/TE	Two-port network Side ISDN BRI interface
VIC-4FXS/DID[1]	Four-port FXS and DID voice/fax interface card
VWIC-1MFT-T1	One-port RJ-48 multiflex trunk - T1
VWIC-2MFT-T1	Two-port RJ-48 multiflex trunk - T1
VWIC-2MFT-T1-DI	Two-port RJ-48 multiflex trunk - T1 with drop and insert
VWIC-1MFT-E1	One-port RJ-48 multiflex trunk - E1
VWIC-2MFT-E1	Two-port RJ-48 multiflex trunk - E1

Table 6 Voice Interface Cards for the Cisco 1751

VWIC-2MFT-E1-DI	Two-port RJ-48 multiflex trunk - E1 with drop and insert
VWIC-1MFT-G703	One-port RJ-48 multiflex trunk - E1 G.703
VWIC-2MFT-G703	Two-port RJ-48 multiflex trunk - E1 G.703

1. The Cisco 1751 can support three VIC-4FXS/DID cards with a maximum of four ports in DID mode

Voice Implementation Requirements

The Cisco 1751 Modular Access Router supports FXO, FXS, E&M, ISDN BRI VICs, and T1/E1 multiflex V/WICs.

The FXO interface allows an analog connection to the central office of the Public Switched Telephone Network (PSTN). The FXS interface connects basic telephone service phones (home phones), fax machines, key sets, and PBXs through ring voltage and dial tone. The E&M interface allows connection for PBX trunk lines (tie lines). The ISDN-BRI NT/TE VIC is used to connect to the PSTN or a PBX/KTS, whereas the T1/E1 multiflex V/WIC (multiflex V/WIC) supports both data and voice services. The multiservice-ready Cisco 1751-V router version includes all the features needed for immediate integration of data and voice services:

- One DSP—(PVDM-256K-4)
- 32-MB Flash memory
- 64-MB DRAM
- Cisco IOS IP/VOX Plus feature set

VICs and WICs are available separately.

The Cisco 1751 and Cisco 1751-V routers have two DSP module slots on the motherboard and a maximum of eight DSPs are supported per router.

DSP Requirements

Cisco 1751 routers support 3 types of DSP images: high complexity (HC), medium complexity (MC) and Flexi-6. HC and MC are used for analog[1] and BRI (VIC-2BRI-NT/TE) VICs; Flexi-6 is used for T1/E1 VWICs[2] and BRI VIC. MC is introduced in Cisco 1751 starting from Cisco IOS 12.2(8)YN release, which will merge into 12.3(1)T. Therefore, please make sure to use Cisco 12.2(8) YN or later releases when using MC. In addition, starting from 12.2(8)YN release, the default DSP image for BRI VIC is changed from HC to Flexi-6. Table 7 lists the default images for each type of VICs; Table 8 lists IOS support for each DSP image. Table 9 lists the number of channels supported by one DSP (PVDM-256K-4) for each codec type.

Please use the following rules for calculating DSP requirements on the Cisco 1751:

1. For the Early Deployment (ED) releases: Cisco IOS 12.2(2)XK, 12.2(4)XW, 12.2(4)XL, 12.2(4)XM, 12.2(4)YA, 12.2(4)YB, 12.2(8)YL, 12.2(8)YM and 12.2(11)YT, or T train releases prior to 12.3(1)T:

1. Analog VICs include VIC-2FXS, VIC-2FXO, VIC-2FXO-M1, VIC-2FXO-M2, VIC-2FXO-M3, VIC-2FXO-EU, VIC-2E/M, VIC-2DID,VIC-4FXS/DID
2. T1/E1 VWICs include VWIC-1MFT-T1, VWIC-2MFT-T1, VWIC-2MFT-T1-DI, VWIC-1MFT-E1, VWIC-2MFT-E1, VWIC-2MFT-E1-DI, VWIC-1MFT-G703, VWIC-2MFT-G703

- a. Each 2-port analog VIC requires 1 DSP (PVDM-256K-4)
- b. Each VIC-2BRI-NT/TE requires 2 DSPs (PVDM-256K-8)
- c. For VWICs, refer to Table 9. For example, 12 G.711 digital T1/E1 voice calls require two DSPs; 12 G.729 calls require four DSPs
- d. Total DSP requirement is the sum of a, b and c. The DSP resources can not be shared between analog VICs, BRI VIC and VWICs.

2. For the Early Deployment (ED) releases: Cisco IOS 12.2(8)YN or later (Note: not including 12.2(11)YT) or T train releases 12.3(1)T or later, please always refer to the DSP Calculator in the following link:

   http://www.cisco.com/cgi-bin/Support/DSP/cisco_prodsel.pl

The DSP calculator optimizes the DSP resources for your configuration and suggests CLI configurations.

Table 7 DSP Firmware for each type of VICs

VIC Type	Firmware Support
2-port Analog VICs	HC (default), MC (starting from 12.2(8)YN)
4-port Analog VIC	HC, MC (default, starting from 12.2(8)YN)
VIC-2BRI-NT/TE	HC (default for ED releases prior to 12.2(8)YN or T train releases prior to 12.3(1)T); MC; Flexi-6 (default for ED releases 12.2(8)YN or later or T train releases 12.3(1)T or later);
T1/E1 VWICs	Flexi-6 (default)

Table 8 Cisco IOS support for DSP firmware

Firmware Support	IOS Release Support
HC	In all orderable IOS Releases
MC	ED Releases: Cisco IOS 12.2(8)YN or later [1] T Train Releases: Cisco IOS 12.3(1)T or later
Flexi-6	For T1/E1 VWICs: • ED Releases: Cisco IOS 12.2(4)YB or later [2] • T Train Releases: 6th releases of 12.2T or later For VIC-2BRI-NT/TE: • ED Releases: Cisco IOS 12.2(8)YN or later [3] • T Train Releases: Cisco IOS 12.3(1)T or later

1. It doesn't include Cisco 12.2(11)YT. 12.2(11)YT doesn't support MC.
2. It doesn't include Cisco 12.2(11)YT. 12.2(11)YT doesn't support Flexi-6.
3. It doesn't include Cisco 12.2(11)YT. 12.2(11)YT doesn't support Flexi-6.

Table 9 The number of channels supported by one DSP (PVDM-256K-4) per codec type

	Firmware		
Codec	HC (for analog & BRI VICs)	MC (for analog & BRI VICs)	Flexi 6 (for VWICs & BRI VIC[1])

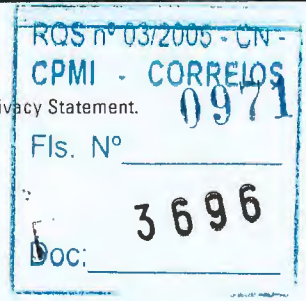


Table 9 The number of channels supported by one DSP (PVDM-256K-4) per codec type

	Firmware		
G.711	2	4	6
G.729ab[2] /G.729a	2	4	3
G.726	2	4	3
G.723	2	-	2
G.728	2	-	2
Fax Relay	2	4	3

1. BRI VIC support in Flexi-6 starts from 12.2(8)YN or 12.3(1)T.
2. G.729 and G.729b is not supported in MC or Flexi-6 images.

Table 10 DSP Modules Available on Cisco 1751

Modules	DSPs
PVDM-256K-4	1 DSP Module
PVDM-256K-8	2 DSP Modules
PVDM-256K-12	3 DSP Modules
PVDM-256K-16HD	4 DSP Modules
PVDM-256K-20HD	5 DSP Modules

Cisco IOS Software Feature Sets

The Cisco 1751 Router supports a choice of Cisco IOS Software feature sets. Each feature set requires specific amounts of Flash and DRAM memory in the product. For default memory configurations, please see Table 11.

Table 11 Cisco 1751 Router Memory Defaults and Maximums

Model Number	Default FLASH/Maximum FLASH	Default DRAM/Maximum DRAM
Cisco 1751	16 MB/16 MB	32 MB/96 MB
Cisco 1751-V Multiservice Model	32 MB/32 MB	64 MB/128 MB

The Cisco 1751 Router supports a choice of Cisco IOS Software feature sets with rich data features as well as data/voice features (Table 12). Each feature set requires specific amounts of RAM and Flash memory in the product.

- Cisco IOS IP base feature sets include: NAT, OSPF, RADIUS, and NHRP.
- Plus feature sets contain L2TP, L2F, the Border Gateway Protocol (BGP), IP Muliticast, Frame Relay SVC, RSVP, the NetWare Link Services Protocol (NLSP), AppleTalk SMRP, the Web Cache Control Protocol (WCCP), and the Network Timing Protocol (NTP).

- Encryption is offered in special encryption feature sets (Plus IPSec 56, and Plus IPSec 3DES). The VPN encryption module requires an IOS IP Plus IPSec image.
- DSL support is only in the Plus feature sets.

Table 12 Cisco IOS Features

Cisco 1751 Router Data Software Feature Sets for Cisco IOS Release 12.1.(5)YB		
Feature Name	**Product Code**	**CD Number**
IP	S17C-12105YB	CD17-C-12.1.5=
IP ADSL	S17C7-12105YB	CD17-C-12.1.5=
IP Plus ADSL	S17C7P-12105YB	CD17-C7P-12.1.5=
IP Plus IPSec 56 (DES) ADSL	S17C7L-12105YB	CD17-C7L-12.1.5=
IP Plus IPSec 3DES ADSL	S17C7K2-12105YB	CD17-C7K2-12.1.5=
IP/FW/IDS	S17CH-12105YB	CD17-CH-12.1.5=
IP/FW/IDS Plus IPSec 56 (DES) ADSL	S17C7HL-12105YB	CD17-C7HL-12.1.5=
IP/IPX	S17B-12105YB	CD17-B-12.1.5=
IP/IPX/FW/IDS Plus ADSL	S17B7HP-12105YB	CD17-B7HP-12.1.5=
IP/FW/IDS Plus IPSec 3DES ADSL	S17C7HK2-12105YB	CD17-C7HK2-12.1.5=
IP/IPX/AT/IBM	S17Q-12105YB	CD17-Q-12.1.5=
IP/IPX/AT/IBM Plus ADSL	S17Q7P-12105YB	CD17-Q7P-12.1.5=
IP/IPX/AT/IBM/FW/IDS Plus IPSec 56 (DES) ADSL	S17Q7HL-12105YB	CD17-Q7HL-12.1.5=
IP/IPX/AT/IBM/FW/IDS Plus IPSec 3DES ADSL	S17Q7HK2-12105YB	CD17-Q7HK2-12.1.5=
Cisco 1751 Router Data/Voice Software Feature Packs for Cisco IOS Release 12.1.(5)YB		
Feature Name	**Product Code**	**CD Number**
IP/Voice Plus	S17CVP-12105YB	CD17-C7VP-12.1.5=
IP/Voice Plus ADSL	S17C7VP-12105YB	CD17-C7VP-12.1.5=
IP/Voice Plus IPSec 56 (DES) ADSL	S17C7VL-12105YB	CD17-C7VL-12.1.5=
IP/Voice/FW/IDS Plus ADSL	S17C7HV-12105YB	CD17-C7HV-12.1.5=
IP/Voice/FW/IDS Plus IPSec 56 ADSL	S17C7HVL-12105YB	CD17-C7HVL-12.1.5=
IP/Voice Plus IPSec 3DES ADSL	S17C7VK2-12105YB	CD17-C7VK2-12.1.5=
IP/Voice/FW/IDS Plus IPSec 3DES ADSL	S17C7HVK2-12105YB	CD17-C7HVK2-12.1.5=
IP/IPX/Voice/FW/IDS Plus ADSL	S17B7HPV-12105YB	CD17-B7HPV-12.1.5=
IP/IPX/AT/IBM/FW/IDS Voice Plus IPSec 56 (DES) ADSL	S17Q7HVL-12105YB	CD17-Q7HVL-12.1.5=
IP/IPX/AT/IBM/FW/IDS/Voice Plus IPSec 3DES ADSL	S17Q7HVK2-12105YB	CD17-Q7HVK2-12.1.5=

Other IOS Features Include:

QoS Features

- Frame Relay Fragmentation (FRF.12)
- IP Precedence
- Generic Traffic Shaping (GTS)
- Frame Relay Traffic Shaping (FRTS)
- Weighted Random Early Detection (WRED)
- DSCP Marking
- Compressed RTP
- Multiple Link PPP & Link Fragmentation and Interleaving
- Resourse Reservation Protocol (RSVP)
- Queuing Techniques: Weighted Fair Queuing (WFQ), Priority Queuing (PQ), Low Laterey Queuing (LLQ) and Custom Queuing (CQ)
- Preclassification for IPSec Tunneling

Voice Support

- VoIP
- VoFR
- VoATM
- Fax Pass Through
- Fax Relay
- Modem Pass Through

VoIP Protocol Support

- H.323 V2
- Media Gateway Control Protocol 1.0
- Session Initiation Protocol 2.0

Codec Support

- G.711
- G.729
- G.729a
- G.723.1
- G.726
- G.728

Technical Specifications

Dimensions

- Width: 11.2 in. (28.4 cm)
- Height: 4.0 in. (10.0 cm)
- Depth: 8.7 in. (22.1 cm)
- Weight (minimum): 3.0 lb (1.36 kg)
- Weight (maximum): 3.5 lb (1.59 kg)

Power

- Locking connector on power socket
- External Power Brick
- AC Input Voltage: 100 to 240 VAC
- Frequency: 50 - 60 Hz
- AC Input Current: rated 1 A, measured 0.5 A
- Power Dissipation: 20W (maximum)

Environmental

- Operating Temperature: 32 to 104 F (0 to 40 C)
- Nonoperating Temperature: -4 to 149 F (-20 to 65 C)
- Relative Humidity: 10 to 85% noncondensing operating; 5 to 95% noncondensing, nonoperating

Safety

- Regulatory Approvals
  - UL 1950, 3rd Edition
  - CSA 22.2 No 950-95, 3rd Edition
  - EN60950 with A1 through A4 and A11
  - EN41003
  - TCA TS001-1997
  - AS/NZS 3260 with A1 through A4
- IEC 60950 with A1 through A4 and all country deviations
- NOM-019-SCFI
- GB4943
  - ETSI 300-047
  - BS 6301 (power supply) EMI
  - AS/NRZ 3548 Class B
- CNS-13438
  - FCC Part 15 Class B
  - EN60555-2 Class B

  - EN55022 Class B
  - VCCI Class II
  - CISPR-22 Class B
- EN55024 comprised of:
  - IEC 1000-4-2 (EN61000-4-2)
  - IEC 1000-4-3 (ENV50140)
  - IEC 1000-4-4 (EN61000-4-4)
  - IEC 1000-4-5 (EN61000-4-5)
  - IEC 1000-4-6 (ENV50141)
  - IEC 1000-4-11
  - IEC 1000-3-2 Network Homologation
  -
- Europe: CTR2, CTR3, TBR21
- Canada: CS-03
- United States: FCC Part 68
- Japan: Jate NTT
- Australia/New Zealand: TS013/TS-031, TS002, TS003
- Hong Kong: CR22

Service and Support

Leading-edge technology deserves leading-edge support. Service and support for the Cisco 1751 is available on a one-time or an annual contract basis. Support options range from help desk assistance to proactive, onsite consultation. All support contracts include:

- Major Cisco IOS Software updates in protocol, security, bandwidth, and feature improvements
- Full access to Cisco.com for technical assistance, electronic commerce, and product information
- 24-hour-a-day access to the industry's largest dedicated technical support staff

A support contract maximizes the value of your technology investment throughout its lifecycle, ensuring optimum performance and availability. Augment your internal staff's capabilities by taking full advantage of Cisco expertise.

Contact your local sales office for further information.

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 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

ETMG 202903 01/03

Roteador Tipo 2 doc 2

• Cisco Systems, Inc.(R) Close Window •

Feedback | Help

Cisco Feature Navigator II

Search by Feature Search by Release Compare Images

Objective: Define a specific software image in order to view its supported features.

Select from the pull down menus to find releases which support particular platform and feature set combinations.View your results in the table below and repeat as necessary to define a specific software image.

Your Selections:

Major Release	12.2T
Release	12.2(8)T
Platform	1751
Feature Set	IP/ADSL/VOICE/FW/IDS PLUS IPSEC 3DES

New Search

Search Results

Image Info

Image Name (Dram/Flash) :	c1700-k9o3sv3y7-mz.12.2-8.T (48/16)
Enterprise Product Number :	S17C7HVK9-12208T S17C7HVK9-12208T=

This image has software advisories associated with it.Click here for details.
Get This Image Compare Images View MIBs Release Notes

Features

AAA Broadcast Accounting
AAA DNIS Map for Authorization
AAA Server Group
AAA Server Group Deadtimer
AAA Server Group Enhancements
AAA Server Groups Based on DNIS
Ability to Disable Xauth for Static IPsec Peers
Accounting of VPDN Disconnect Cause
ACL Authentication of Incoming RSH and RCP
Additional Vendor-Proprietary RADIUS Attributes
Address Resolution Protocol (ARP)
ADSL - Asymmetric Digital Subscriber Line Support
Always On Dynamic ISDN (AO/DI)
Asynchronous Rotary Line Queuing
Asynchronous Serial Traffic Over UDP
ATM PVC Trap Support
ATM SNMP Trap and OAM Enhancements
ATM-DXI
Authentication Proxy Accounting for HTTP
AutoInstall over Frame Relay-ATM Interworking Connections
AutoInstall Using DHCP for LAN Interfaces
Automatic modem configuration

Bandwidth Allocation Control Protocol (BACP)
BGP
BGP 4
BGP 4 Multipath Support
BGP 4 Prefix Filter and In-bound Route Maps
BGP 4 Soft Config
BGP Conditional Route Injection
BGP Hide Local-Autonomous System
BGP Link Bandwidth
BGP Multipath Load Sharing for Both eBGP and iBGP in an MPLS-VPN
BGP Named Community Lists
BGP Prefix-Based Outbound Route Filtering
BGP Soft Reset
Call Admission Control for H.323 VoIP Gateways
CEF on Multipoint GRE Tunnels
CEF/dCEF - Cisco Express Forwarding
Certificate Auto-Enrollment
Certificate Enrollment Enhancements
Certification Authority Interoperability (CA)
CGMP - Cisco Group Management Protocol
Challege Handshake Authentication Protocol (CHAP)
Circuit Interface Identification Persistence for SNMP
Cisco Discovery Protocol (CDP)
Cisco Discovery Protocol (CDP) - IPv6 Address Family Support for Neighbor Information
Cisco Discovery Protocol (CDP) over ATM
Class Based Weighted Fair Queuing (CBWFQ)
Class-Based Packet Marking
CLI String Search
CNS Agents SSL Security
CNS Configuration Agent
CNS Event Agent
CNS Flow-Through Provisioning
Commented IP Access List Entries
Committed Access Rate (CAR)
Compression Control Protocol
Context-Based Access Control (CBAC)
CUG Selection Facility Suppress Option
Custom Queueing (CQ)
Customer Profile Idle Timer Enhancements for Interesting Traffic
Default Passive Interface
DF Bit Override Functionality with IPSec Tunnels
DHCP Client
DHCP Client - Dynamic Subnet Allocation API
DHCP Client on WAN Interfaces

DHCP Proxy Client
DHCP Relay Agent Support for Unnumbered Interfaces
DHCP Server - On Demand Address Pool Manager
DHCP Server - Option to Ignore all BOOTP Requests
DHCP Server Options - Import and Autoconfiguration
DHCP Server-Easy IP Phase 2
Dial backup
Dial Peer Enhancements
Dial-on-demand
Dialer Idle Timer Inbound Traffic Configuration
Dialer Map VRF Aware
Dialer Persistent
Dialer profiles
Dialer Watch
Dialer Watch Connect Delay
Diffserv Compliant WRED
Distinguished Name Based Crypto Maps
DNS based X.25 routing
DNS Lookups over an IPv6 Transport
Double Authentication
Dynamic Multiple Encapsulation for Dial-in over ISDN
Easy IP (Phase 1)
Easy VPN Server
Encrypted Vendor Specific Attributes
Enhanced ATM VC Configuration and Management
Enhanced IGRP (EIGRP)
Enhanced IGRP Stub Routing
Enhanced Local Management Interface (ELMI)
Enhanced Password Security
Fast-Switched Policy Routing
Firewall Authentication Proxy
Firewall Feature Set
Firewall Intrusion Detection System
Flow-Based WRED
Frame Relay
Frame Relay Encapsulation
Frame Relay End-to-End Keepalive
Frame Relay Fragmentation (FRF.12)
Frame Relay FRF.9 Payload Compression
Frame Relay PVC Interface Priority Queueing
Frame Relay Router ForeSight
Frame Relay SVC Support (DTE)
Frame Relay Switching
Frame Relay Traffic Shaping (FRTS)

FXO Answer and Disconnect Supervision
Gatekeeper Ecosystem Interoperability
Generic Routing Encapsulation (GRE)
Generic Routing Encapsulation (GRE) Tunnel Keepalive
Generic Traffic Shaping (GTS)
H.323 Call Redirection Enhancements
H.323 Scalability and Interoperability Enhancements for Gateways
Half bridge/half router for CPP and PPP
Hoot and Holler over IP
HSRP - Hot Standby Router Protocol
HSRP - Hot Standby Router Protocol and IPSec
HSRP support for ICMP Redirects
HTTP Security
iBGP Multipath Load Sharing
IEEE 802.1Q VLAN Support
IGMP Version 3
IGMP Version 3 - Explicit Tracking of Hosts, Groups, and Channels
IGRP
IKE - Initiate Aggressive Mode
IKE Extended Authentication (Xauth)
IKE Mode Configuration
IKE Security Protocol
IKE Shared Secret Using AAA Server
Integrated routing and bridging (IRB)
Interface Alias Long Name Support
Interface Index Display
Interface Range Specification
Internet Protocol Control Protocol (IPCP) address negotiation
IP Enhanced IGRP Route Authentication
IP Header Compression Enhancement - PPPoATM and PPPoFR Support
IP Multicast Load Splitting across Equal-Cost Paths
IP Named Access Control List
IP Precedence for GRE Tunnels
IP Routing
IP RTP Priority
IP Summary Address for RIPv2
IPSec MIB Support for Cisco IPSec VPN Management
IPSec Network Security
IPSec Triple DES Encryption (3DES)
IPSec VPN High Availability Enhancements
IPv6 for Cisco IOS Software
ISDN
ISDN Advice of Charge (AOC)
ISDN Caller ID Callback

ISDN Cause Code Override
ISDN Leased Line at 128kbps
L2TP Dial-Out
L2TP Layer 2 Tunneling Protocol
L2TP Security
L2TP Tunnel Preservation of IP TOS
Layer 2 Forwarding-Fast Switching
Lock and Key
Low Latency Queueing (LLQ)
Low Latency Queueing (LLQ) for Frame Relay
Low Latency Queueing (LLQ) with Priority Percentage Support
MD5 File Validation
Message Banners for AAA Authentication
Microsoft Point-to-Point Compression (MPPC)
Modem User Interface Option
Modular QoS CLI (MQC)
MS Callback
MS-CHAP Version 1
Multicast NAT
Multicast Source Discovery Protocol (MSDP)
Multilink PPP
Multiple RSA Keypair Support
Named Method Lists for AAA Authorization and Accounting
NAT-Network Address Translation
NAT-Support for NetMeeting Directory (Internet Locator Service - ILS)
NAT-Support for SIP
NAT-Support of H.323v2 RAS
NAT-Support of IP Phone to Cisco Call Manager
NBAR - Network-based Application Recognition
NBAR Real-time Transport Protocol Payload Classification
Netflow
NetFlow Aggregation
Netflow Multiple Export Destinations
NetFlow Policy Routing (NPR)
NetFlow ToS-Based Router Aggregation
Network Time Protocol (NTP)
Next Hop Resolution Protocol (NHRP)
On Demand Routing (ODR)
OSPF
OSPF ABR type 3 LSA Filtering
OSPF Flooding Reduction
OSPF Not-So-Stubby Areas (NSSA)
OSPF On Demand Circuit (RFC 1793)
OSPF Packet Pacing

OSPF Sham-Link Support for MPLS VPN
OSPF Stub Router Advertisement
PAD Subaddressing
Parse Bookmarks
Parser Cache
Password Authentication Protocol (PAP)
Per-User Configuration
PGM Router Assist
PIM Dense Mode State Refresh
PIM MIB Extension for IP Multicast
PIM Multicast Scalability
PIM Version 1
PIM Version 2
Policy-Based Routing (PBR)
Port to Application Mapping (PAM)
PPP
PPP over ATM
PPP over ATM (IETF-Compliant)
PPP over Frame Relay
PPPoE Client
PPPoE on Ethernet
PPTP with MPPE
Priority Queueing (PQ)
QoS Device Manager (QDM)
QoS Packet Marking
QoS Priority Percentage CLI Support
RADIUS
RADIUS Attribute 44 (Accounting Session ID) in Access Requests
RADIUS Attribute 82: Tunnel Assignment Id
RADIUS for Multiple User Datagram Protocol Ports
RADIUS Route Download
RADIUS Tunnel Preference for Load Balancing and Fail-over
Random Early Detection (RED)
Rate Queues for SVC's per sub-interface
Reflexive Access Lists
Response Time Reporter (RTR)
Response Time Reporter (RTR) enhancements
Restart-delay Granularity
Reverse Route Injection (RRI)
RIP
RMON events and alarms
Rotating Through Dial Strings
RSVP - Resource Reservation Protocol
RSVP Support for Frame Relay

RSVP support for LLQ
RTP Header Compression
Secure Copy (SCP)
Secure Shell SSH Support over IPv6
Secure Shell SSH Terminal-line access
Secure Shell SSH Version 1 Integrated Client
Secure Shell SSH Version 1 Server Support
Service Assurance Agent (SAA) APM Application Performance Monitor
Service Assurance Agent (SAA) DHCP Operation
Service Assurance Agent (SAA) Distribution of Data
Service Assurance Agent (SAA) DLSW Operation
Service Assurance Agent (SAA) DNS Operation
Service Assurance Agent (SAA) Frame Relay Operation
Service Assurance Agent (SAA) FTP Operation
Service Assurance Agent (SAA) History Statistics
Service Assurance Agent (SAA) HTTP Operation
Service Assurance Agent (SAA) ICMP Echo Operation
Service Assurance Agent (SAA) ICMP Path Echo Operation
Service Assurance Agent (SAA) Jitter Operation
Service Assurance Agent (SAA) MPLS VPN Operation
Service Assurance Agent (SAA) One Way Jitter
Service Assurance Agent (SAA) Path Jitter
Service Assurance Agent (SAA) Reaction Threshold
Service Assurance Agent (SAA) Scheduling Operation
Service Assurance Agent (SAA) SNA LU2 Echo
Service Assurance Agent (SAA) SNMP Support
Service Assurance Agent (SAA) TCP Connect Operation
Service Assurance Agent (SAA) UDP Echo Operation
Simple Network Time Protocol (SNTP)
Single Rate 3-Color Marker for Traffic Policing
SIP - Session Initiation Protocol for VoIP Enhancements
Snapshot routing
SNMP (Simple Network Management Protocol)
SNMP Inform Request
SNMP Manager
SNMP Support for IOS vLAN Subinterfaces
SNMP Support for vLAN (ISL, DOT1Q) Subinterfaces
SNMP Support over VPN
SNMPv2C
Spanning Tree Protocol (STP)
Spanning Tree Protocol (STP) Extension
Standard IP Access List Logging
Static Cache Entry for IPv6 Neighbor Discovery
Stub IP Multicast Routing

Subnetwork Bandwidth Manager (SBM)
Switched Multimegabit Data Service (SMDS)
T.38 Fax Relay for VoIP H.323
Tacacs SENDAUTH function
Tacacs Single Connection
TACACS+
TCP Window Scaling
Time-Based Access Lists Using Time Ranges
Timer and Retry Enhancements for L2TP and L2F
Traffic Policing
Transparent Bridging
Triggered RIP
Trusted Root Certification Authority
Trustpoint CLI
Tunnel Endpoint Discovery
Tunnel Type of Service (TOS)
Turbo Flooding of UDP Datagrams
UDLR Tunnel ARP and IGMP Proxy
Uni-Directional Link Routing (UDLR)
Unicast Reverse Path Forwarding (uRPF)
User Maximum Links
Virtual Interface Template Service
Virtual Private Dial-up Network (VPDN)
Virtual Profiles
Voice over Frame Relay (FRF.11)
Voice Over IP
VoIP Call Admission Control using RSVP
VPDN Group Session Limiting
VPN Tunnel Management
WCCP Redirection on Inbound Interfaces
WCCP Version 1
WCCP Version 2
Weighted Fair Queueing (WFQ)
Weighted RED (WRED)
Wildcard Pre-Shared Key
WRED Enhancement - Explicit Congestion Notification (ECN)
x Digital Subscriber Line (xDSL) Bridge Support
X.25
X.25 Closed User Group
X.25 Failover
X.25 Load Balancing
X.25 on ISDN D-Channel
X.25 over Frame Relay (Annex G)
X.25 over TCP (XOT)

X.25 Over TCP Profiles

X.25 Remote Failure Detection

X.25 Switch Local Acknowledgement

X.25 Switching between PVCs and SVCs

X.28 Emulation

Some features are dependent on product model, interface modules (i.e. Line Cards & Port Adapters), and/or require a software feature license. Click here for more information.

Close Window

Roteador Tipo 2 doc 3

• Cisco Systems, Inc.(R) Close Window •

Feedback | Help

MIB Locator

Make Selections to get to a Specific Cisco IOS Release:

Release

12.2(8)T

Platform Family

1750

Feature Set

IP/ADSL/VOICE/FW/IDS PLUS IPSEC 3DES

New Search

Download all V1 , V2 MIBs

Image Information

c1700-k9o3sv3y7-mz.12.2-8.T

Get list of features for this image from Cisco Feature Navigator

MIBS Supported in this Image	Details	Download MIB	
BGP4-MIB		V1	V2
BRIDGE-MIB		V1	
CISCO-AAL5-MIB		V1	V2
CISCO-ATM-EXT-MIB		V1	V2
CISCO-CALL-APPLICATION-MIB		V1	V2
CISCO-CALL-HISTORY-MIB		V1	V2
CISCO-CAR-MIB		V1	V2
CISCO-CAS-IF-MIB		V1	V2
CISCO-CDP-MIB		V1	V2
CISCO-CIRCUIT-INTERFACE-MIB		V1	V2
CISCO-CLASS-BASED-QOS-MIB		V1	V2
CISCO-CONFIG-COPY-MIB		V1	V2
CISCO-CONFIG-MAN-MIB		V1	V2
CISCO-DIAL-CONTROL-MIB		V1	V2
CISCO-DSL-CPE-MIB	Note		
CISCO-ENTITY-ASSET-MIB		V1	V2
CISCO-ENTITY-VENDORTYPE-OID-MIB		V1	V2
CISCO-FLASH-MIB		V1	V2
CISCO-FRAME-RELAY-MIB		V1	V2
CISCO-H323-TC-MIB		V1	V2
CISCO-HSRP-EXT-MIB		V1	V2
CISCO-HSRP-MIB		V1	V2
CISCO-ICSUDSU-MIB		V1	V2
CISCO-IETF-ATM2-PVCTRAP-MIB		V1	V2
CISCO-IETF-ATM2-PVCTRAP-MIB-EXTN	Note		
CISCO-IMAGE-MIB		V1	
CISCO-IP-STAT-MIB		V1	
CISCO-IPMROUTE-MIB		V1	

CISCO-IPSEC-FLOW-MONITOR-MIB		V1	V2
CISCO-IPSEC-MIB		V1	V2
CISCO-IPSEC-POLICY-MAP-MIB		V1	V2
CISCO-ISDN-MIB		V1	V2
CISCO-ISDNU-IF-MIB		V1	V2
CISCO-MEMORY-POOL-MIB		V1	V2
CISCO-MMAIL-DIAL-CONTROL-MIB		V1	V2
CISCO-NTP-MIB		V1	V2
CISCO-PIM-MIB		V1	V2
CISCO-PING-MIB		V1	V2
CISCO-PPPOE-MIB		V1	V2
CISCO-PROCESS-MIB		V1	V2
CISCO-PRODUCTS-MIB		V1	V2
CISCO-QUEUE-MIB		V1	V2
CISCO-RAS-MIB	Note		
CISCO-RTTMON-MIB		V1	V2
CISCO-SIP-UA-MIB		V1	V2
CISCO-SNAPSHOT-MIB		V1	V2
CISCO-STACKMAKER-MIB		V1	V2
CISCO-SYSLOG-MIB		V1	V2
CISCO-TCP-MIB		V1	V2
CISCO-VOICE-ANALOG-IF-MIB		V1	V2
CISCO-VOICE-COMMON-DIAL-CONTROL-MIB		V1	V2
CISCO-VOICE-DIAL-CONTROL-MIB		V1	V2
CISCO-VOICE-DNIS-MIB	Note		
CISCO-VOICE-IF-MIB		V1	V2
CISCO-VPDN-MGMT-EXT-MIB		V1	V2
CISCO-VPDN-MGMT-MIB		V1	V2
DIAL-CONTROL-MIB		V1	V2
ENTITY-MIB		V1	V2
ETHERLIKE-MIB		V1	V2
HC-RMON-MIB			V2
IF-MIB		V1	V2
IGMP-STD-MIB		V1	V2
INT-SERV-GUARANTEED-MIB		V1	V2
INT-SERV-MIB		V1	V2
IP-FORWARD-MIB		V1	V2
IPMROUTE-MIB		V1	V2
ISDN-MIB		V1	V2
MSDP-MIB		V1	V2
OLD-CISCO-CHASSIS-MIB		V1	
OLD-CISCO-CPU-MIB		V1	
OLD-CISCO-FLASH-MIB		V1	
OLD-CISCO-INTERFACES-MIB		V1	
OLD-CISCO-IP-MIB		V1	
OLD-CISCO-MEMORY-MIB		V1	
OLD-CISCO-SYSTEM-MIB		V1	
OLD-CISCO-TCP-MIB		V1	

OLD-CISCO-TS-MIB		V1	
PIM-MIB		V1	V2
RFC1213-MIB		V1	
RFC1253-MIB		V1	
RFC1315-MIB		V1	
RFC1381-MIB		V1	
RFC1382-MIB		V1	
RFC1406-MIB		V1	
RMON-MIB		V1	V2
RMON2-MIB		V1	V2
RS-232-MIB		V1	V2
RSVP-MIB		V1	V2
SMON-MIB		V1	V2
SNMP-FRAMEWORK-MIB		V1	V2
SNMP-NOTIFICATION-MIB		V1	V2
SNMP-PROXY-MIB	Note		
SNMP-TARGET-MIB		V1	V2
SNMP-USM-MIB		V1	V2
SNMP-VACM-MIB		V1	V2
SNMPv2-MIB		V1	V2
TCP-MIB		V1	V2
UDP-MIB		V1	V2
XGCP-MIB		V1	V2

Close Window

Roteador Tipo 2 doc 4

APPENDIX **B**

ROM Monitor

This appendix describes the Cisco router ROM monitor (also called the *bootstrap program*). The ROM monitor firmware runs when the router is powered up or reset. The firmware helps to initialize the processor hardware and boot the operating system software. You can perform certain configuration tasks, such as recovering a lost password or downloading software over the console port, by using the ROM monitor. If there is no Cisco IOS software image loaded on the router, the ROM monitor runs the router.

This appendix contains the following sections:

- Entering the ROM Monitor
- ROM Monitor Commands
- Command Descriptions
- Disaster Recovery with TFTP Download
- Configuration Register
- Console Download

Entering the ROM Monitor

To use the ROM monitor, you must be using a terminal or PC that is connected to the router by means of the console port. Refer to the installation chapter in the Hardware Installation Guide for your router, for information about connecting the router to a PC or terminal.

Follow these steps to configure the router to boot up in ROM monitor mode the next time it is rebooted.

	Command	Router Prompt	Task
Step 1	**enable**	`Router>`	If there is an enable password configured, enter the enable command and the enable password to enter privileged EXEC mode.
Step 2	**configure terminal**	`Router#`	Enter global configuration mode.
Step 3	**config-reg 0x0**	`Router(config)#`	Reset the configuration register.
Step 4	**exit**	`Router(config)#`	Exit global configuration mode.
Step 5	**reload**	`Router#`	Reboot the router with the new configuration register value. The router remains in ROM monitor and does not boot the Cisco IOS software. As long as the configuration value is 0x0, you must manually boot the operating system from the console. See the **boot** command in the "Command Descriptions" section on page B-4.
Step 6		`rommon 1>`	After the router reboots, it is in ROM monitor mode. The number in the prompt increments with each new line.

Timesaver A break (system interrupt) is always enabled for 60 seconds after the router reboots, regardless of its setting (on or off) in the configuration register. During this 60-second window, you can break to the ROM monitor prompt by pressing the Break key.

ROM Monitor Commands

Enter **?** or **help** at the ROM monitor prompt to display a list of available commands and options, as follows:

```
rommon 1 > ?
alias             set and display aliases command
boot              boot up an external process
break             set/show/clear the breakpoint
confreg           configuration register utility
cont              continue executing a downloaded image
context           display the context of a loaded image
cookie            display contents of cookie PROM in hex
dev               list the device table
dir               list files in file system
dis               display instruction stream
dnld              serial download a program module
frame             print out a selected stack frame
help              monitor builtin command help
history           monitor command history
meminfo           main memory information
repeat            repeat a monitor command
reset             system reset
set               display the monitor variables
stack             produce a stack trace
sync              write monitor environment to NVRAM
sysret            print out info from last system return
tftpdnld          tftp image download
unalias           unset an alias
unset             unset a monitor variable
xmodem            x/ymodem image download
```

Commands are case sensitive. You can halt any command by pressing the Break key on a terminal. If you are using a PC, most terminal emulation programs halt a command when you press the Ctrl and the Break keys at the same time. If you are using another type of terminal emulator or terminal emulation software, refer to the documentation for that product for information on how to send a Break command.

Command Descriptions

Table B-1 describes commonly used ROM monitor commands.

Table B-1 Common ROM Monitor Commands

Command	Description
help or **?**	Displays a summary of all available ROM monitor commands.

-?	Displays information about command syntax, for example:
	`rommon 16 > dis -?`
	`usage : dis [addr] [length]`
	
	The output for this command is slightly different for the **xmodem** download command:
	`rommon 11 > xmodem -?`
	`xmodem: illegal option -- ?`
	`usage: xmodem [-cyrx] destination filename`
	`-c CRC-16`
	`-y ymodem-batch protocol`
	`-r copy image to dram for launch`
	`-x do not launch on download completion`

reset or **i**	Resets and initializes the router, similar to a power-up.

dev	Lists boot device identifications on the router. For example:
	`rommon 2> dev`
	`Devices in device table:`
	`id name`
	`flash: flash`
	`eprom: eprom`

dir *device*:	Lists the files on the named device (Flash, for example):
	`rommon 1> dir flash:`
	`File size Checksum File name`
	`7729736 bytes (0x75f248) 0xb86d`
	`c1700-bk9no3r2sy7-mz.0412`

Table B-2 describes the ROM monitor boot commands. For more information about the ROM monitor boot commands, refer to the *Cisco IOS Configuration Guide* and *Cisco IOS Command Reference* publications.

Table B-2 Boot Commands

Command	Description
b	Boots the first image in Flash memory.
b flash: [*filename*]	Attempts to boot the image directly from the first partition of Flash memory. If you do not enter a filename, this command will boot the first image in Flash.
b flash:2: [*filename*]	Attempts to boot the image directly from the second partition of Flash memory. If you do not enter a filename, this command will boot the first image in the second partition of Flash memory.

Disaster Recovery with TFTP Download

The standard way to load new software on your router is using the **copy tftp flash** privileged EXEC command from the Cisco IOS software command-line interface (CLI). However, if the router is unable to boot the Cisco IOS software, you can load new software while in ROM monitor mode.

This section tells how, in ROM monitor mode, to download a Cisco IOS software image from a remote TFTP server to the router Flash memory. Use the **tftpdnld** command only for disaster recovery because it erases all existing data in Flash memory before downloading a new software image to the router.

Note A 10BASE-T Ethernet Port is not active in ROM monitor mode and, thus, cannot be used for TFTP download.

TFTP Download Command Variables

This section describes the system variables that can be set in ROM monitor mode and that are used during the TFTP download process. There are required and optional variables.

Note The commands described in this section are case sensitive and must be entered exactly as shown in the lists.

Required Variables

The following variables must be set with the commands shown before using the **tftpdnld** command:

Variable	Command
IP address of the router.	**IP_ADDRESS=** *ip_address*
Subnet mask of the router.	**IP_SUBNET_MASK=** *ip_address*
IP address of the default gateway of the router.	**DEFAULT_GATEWAY=** *ip_address*
IP address of the TFTP server from which the software will be downloaded.	**TFTP_SERVER=** *ip_address*
The name of the file that will be downloaded to the router.	**TFTP_FILE=** *filename*

Optional Variables

The following variables can be set with the commands shown before using the **tftpdnld** command:

Variable	Command
Whether or not the router performs a checksum test on the downloaded image: **1**—Checksum test is performed. **0**—No checksum test is performed.	**TFTP_CHECKSUM=***setting*

Variable	Command
Number of times the router attempts ARP and TFTP download. The default is 7.	**TFTP_RETRY_COUNT=** *retry_times*
Amount of time, in seconds, before the download process times out. The default is 2400 seconds (40 minutes).	**TFTP_TIMEOUT=** *time*
Configures how the router displays file download progress. **0**—No progress is displayed. **1**—Exclamation points (!!!) are displayed to indicate file download progress. This is the default setting. **2**—Detailed progress is displayed during the file download process. For example: Initializing interface. Interface link state up. ARPing for 1.4.0.1 ARP reply for 1.4.0.1 received. MAC address 00:00:0c:07:ac:01	**TFTP_VERBOSE=** *setting*

Using the TFTP Download Command

The steps described in this section should be performed while in ROM monitor mode.

Step 1 Use the appropriate commands to enter all the required variables and any optional variables.

Step 2 Enter the **tftpdnld** command as follows:

```
rommon 1 > tftpdnld [ -r ]
```

Note The **-r** variable is optional. Entering this variable downloads and boots the new software but does not save the software to Flash. You can then use the image that is in Flash the next time you enter the **reload** command in the Cisco IOS software CLI.

You will see output similar to the following:

```
IP_ADDRESS: 10.0.0.1
      IP_SUBNET_MASK: 255.255.0.0
     DEFAULT_GATEWAY: 1.3.0.1
         TFTP_SERVER: 223.255.254.254
           TFTP_FILE: c1700-bnr2sy-mz.070298
Invoke this command for disaster recovery only.
WARNING: all existing data in all partitions on flash will be lost!
Do you wish to continue? y/n:  [n]:
```

Step 3 If you are sure that you want to continue, enter **y** in response to the question in the output:

```
Do you wish to continue? y/n:  [n]:y
```

The router will begin to download the new file.

Pressing Ctrl-C or Break stops the transfer before the Flash memory is erased.

Configuration Register

The virtual configuration register is in NVRAM and has the same functionality as other Cisco routers. You can view or modify the virtual configuration register from either the ROM monitor or the operating system software.

To change the virtual configuration register from the ROM monitor, enter **confreg** by itself for menu mode, or enter the new value of the register in hexadecimal. For example:

confreg [*hexnum*]

This will change the virtual configuration register to the value specified. The value is always interpreted as hexadecimal. Entering **confreg** without an argument displays the contents of the virtual configuration register and a prompt to alter the contents by describing the meaning of each bit.

Whether or not an argument is provided, the new virtual configuration register value is written into NVRAM, but it does not take effect until you reset or power-cycle the router.

The following display shows an example of menu mode:

```
rommon 7> confreg

     Configuration Summary
enabled are:
console baud: 9600
boot: the ROM Monitor

do you wish to change the configuration? y/n  [n]:  y
enable  "diagnostic mode"? y/n  [n]:  y
enable  "use net in IP bcast address"? y/n  [n]:
enable  "load rom after netboot fails"? y/n  [n]:
enable  "use all zero broadcast"? y/n  [n]:
enable  "break/abort has effect"? y/n  [n]:
enable  "ignore system config info"? y/n  [n]:
change console baud rate? y/n  [n]:  y
enter rate: 0 = 9600, 1 = 4800, 2 = 1200, 3 = 2400
 4 = 19200, 5 = 38400, 6 = 57600, 7 = 115200   [0]:  0
change the boot characteristics? y/n  [n]:  y
enter to boot:
 0 = ROM Monitor
 1 = the boot helper image
 2-15 = boot system
    [0]:  0

Configuration Summary
enabled are:
diagnostic mode
console baud: 9600
boot: the ROM Monitor

do you wish to change the configuration? y/n  [n]:


You must reset or power cycle for new config to take effect
```

Console Download

You can use console download, a ROM monitor function, to download over the router console port either a software image or a configuration file. After downloading, the file is saved either to Flash memory or to main memory for execution (image files only).

Use console download when you do not have access to a TFTP server.

Note If you want to download a software image or a configuration file to the router over the console port, you must use the ROM monitor command.

Note If you are using a PC to download a Cisco IOS image over the router console port at 115,200 bps, ensure that the PC serial port is using a 16550 universal asynchronous receiver/transmitter (UART). If the PC serial port is not using a 16550 UART, we recommend using a speed of 38,400 or lower when downloading a Cisco IOS image over the console port.

Command Description

The following are the syntax and argument descriptions for the **xmodem** console download command.

The syntax is as follows:

xmodem [**-cyrx**] *destination_file_name*

The argument descriptions are as follows:

Argument	Description
c	Optional. Performs the download using 16-bit cyclic redundancy check (CRC) error checking to validate packets. Default is 8-bit CRC.

Argument	Description
y	Optional. Sets the router to perform the download using ymodem protocol. Default is xmodem protocol. The protocols differ as follows: • The xmodem protocol supports a 128-block transfer size, whereas the ymodem protocol supports a 1024-block transfer size. • The ymodem protocol uses 16-bit CRC error checking to validate each packet. Depending on the device that the software is being downloaded from, this function might not be supported by the xmodem protocol.
r	Optional. Image is loaded into DRAM for execution. Default is to load the image into Flash memory.
x	Optional. Image is loaded into DRAM without being executed.
destination_file_name	The name of the system image file or the system configuration file. In order for the router to recognize it, the name of the configuration file must be *router_confg*.

Error Reporting

Because the ROM monitor console download uses the console to perform the data transfer, error messages are displayed on the console only when the data transfer is terminated.

If an error does occur during a data transfer, the transfer is terminated, and an error message is displayed. If you have changed the baud rate from the default rate, the error message is followed by a message telling you to restore the terminal to the baud rate specified in the configuration register.

Debug Commands

Most ROM monitor debugging commands are functional only when Cisco IOS software has crashed or stopped. If you enter a debugging command and Cisco IOS crash information is not available, you see the following error message:

```
"xxx: kernel context state is invalid, can not proceed."
```

The following are ROM monitor debugging commands:

- **stack** or **k**—Produce a stack trace. For example:

```
rommon 6> stack
Stack trace:
PC = 0x801111b0
Frame 00: FP = 0x80005ea8    PC = 0x801111b0
Frame 01: FP = 0x80005eb4    PC = 0x80113694
Frame 02: FP = 0x80005f74    PC = 0x8010eb44
Frame 03: FP = 0x80005f9c    PC = 0x80008118
Frame 04: FP = 0x80005fac    PC = 0x80008064
Frame 05: FP = 0x80005fc4    PC = 0xfff03d70
```

- **context**—Display processor context. For example:

```
rommon 7> context
CPU context of the most recent exception:
PC  = 0x801111b0  MSR = 0x00009032  CR  = 0x53000035  LR    =
0x80113694
CTR = 0x801065e4  XER = 0xa0006d36  DAR = 0xffffffff  DSISR =
0xffffffff
DEC = 0xffffffff  TBU = 0xffffffff  TBL = 0xffffffff  IMMR  =
0xffffffff
R0  = 0x00000000  R1  = 0x80005ea8  R2  = 0xffffffff  R3    =
0x00000000
R4  = 0x8fab0d76  R5  = 0x80657d00  R6  = 0x80570000  R7    =
0x80570000
R8  = 0x00000000  R9  = 0x80570000  R10 = 0x0000954c  R11   =
0x00000000
R12 = 0x00000080  R13 = 0xffffffff  R14 = 0xffffffff  R15   =
0xffffffff
R16 = 0xffffffff  R17 = 0xffffffff  R18 = 0xffffffff  R19   =
0xffffffff
R20 = 0xffffffff  R21 = 0xffffffff  R22 = 0xffffffff  R23   =
0xffffffff
R24 = 0xffffffff  R25 = 0xffffffff  R26 = 0xffffffff  R27   =
0xffffffff
```

```
R28 = 0xffffffff  R29 = 0xffffffff  R30 = 0xffffffff  R31    =
0xffffffff
```

- **frame**—Display an individual stack frame.
- **sysret**—Display return information from the last booted system image. This information includes the reason for terminating the image, a stack dump of up to eight frames, and, if an exception is involved, the address where the exception occurred. For example:

```
rommon 8> sysret
System Return Info:
count: 19,  reason: user break
pc:0x801111b0,  error address: 0x801111b0
Stack Trace:
FP: 0x80005ea8, PC: 0x801111b0
FP: 0x80005eb4, PC: 0x80113694
FP: 0x80005f74, PC: 0x8010eb44
FP: 0x80005f9c, PC: 0x80008118
FP: 0x80005fac, PC: 0x80008064
FP: 0x80005fc4, PC: 0xfff03d70
FP: 0x80005ffc, PC: 0x00000000
FP: 0x00000000, PC: 0x00000000
```

- **meminfo**—Display size in bytes, starting address, available range of main memory, the starting point and size of packet memory, and size of nonvolatile random-access memory (NVRAM). For example:

```
rommon 3> meminfo

Main memory size: 64 MB.
Available main memory starts at 0x10000, size 65472KB
IO (packet) memory size: 25 percent of main memory.
NVRAM size: 32KB
```

Roteador Tipo 2 doc 5

Network and Enterprise Core

Cisco SN 5420 Storage Router

The Cisco SN 5420 Storage Router is the industry's first Small Computer Systems Interface-over-IP (iSCSI) networking platform -- providing universal access to data over any distance, networking media, and operating system. The Cisco SN 5420 allows direct access to storage anywhere on an IP network with all the robustness of the TCP/IP protocol suite including security, availability, manageability, and quality of service (QoS). The storage router fits seamlessly into existing Fibre Channel storage and TCP/IP data networks, allowing individual servers to securely access only the storage they're allowed. The Cisco SN 5420 Storage Router is covered in greater detail in "Tapping IP for Storage."
More product information

Cisco VPN 3000 Concentrator Series Version 3.0

The Cisco VPN 3000 Concentrator Series helps enterprises build high-performance, scalable, robust virtual private network (VPN) infrastructures. Version 3.0 of the concentrator offers new support for load balancing, token card authentication using Remote Authentication Dial-In User Service (RADIUS), data compression, and the Cisco VPN Unified Client Framework. The Cisco VPN 3000 Concentrator Series includes models to support any size enterprise, from small businesses with 100 or fewer remote-access users to organizations with up to 10,000 simultaneous users.
More product information

Cisco VPN Solution Center Version 2.0

The Cisco VPN Solution Center Version 2.0 application helps service providers rapidly deploy and manage IP VPN services based on Multiprotocol Label Switching (MPLS) technology. Product capabilities include service provisioning and activation, service auditing, service-level agreement (SLA) monitoring, and usage collection and reporting. Cisco VPN Solution Center Version 2.0 provides a rich set of application programming interfaces (APIs) and is integrated into most Cisco Service Management modules. The product supports numerous Cisco core routers and switches and enterprise access routers.
More product information

Cisco 7200 Series Network Services Engine NSE-1

The Cisco 7200 Series Network Services Engine (NSE-1) processor accelerates select sets of IP services up to 300 percent over traditional route processing. Taking advantage of Cisco Parallel Express Forwarding (PXF) technology, the Cisco 7200 can achieve more than 300,000 packets per second (pps) performance with multiple services turned on in the network. The NSE-1 delivers high-performance services throughput for select QoS and WAN edge features such as access control lists (ACLs), Network Address Translation (NAT), NetFlow, Class-Based Weighted Fair Queuing (CB-WFQ), Committed Access Rate (CAR), and more.
More product information

Catalyst 8540 Multiservice Switch Router: Enhanced ATM Router Module
The new ATM router module (ARM II) for the Cisco Catalyst® 8540 Multiservice Switch Router delivers feature-rich, high-speed internetworking between Layer 3 and ATM interfaces. Seamless integration of Layer 3 and ATM enables service providers to leverage core ATM infrastructures for delivering new services and allows enterprises to aggregate Fast Ethernet and Gigabit Ethernet traffic over public networks or private lines. The ARM II supports Internet Engineering Task Force (IETF) RFC 1577 and RFC 1483 bridging and routing, integrated ACLs, and 256,000 routing table entries.
More product information

Cisco Secure PIX Firewall Operating System Version 6.0
The Cisco Secure PIX® Firewall Operating System Version 6.0 delivers a host of new features, most notably support for the new Cisco PIX Device Manager (PDM), a browser-based GUI for setup, configuration, and monitoring of PIX firewalls. VPN functionality has been enhanced via support for the Cisco VPN Unified Client Framework as well as Layer 2 Tunneling Protocol (L2TP) for Microsoft Windows clients. Voice-over-IP handling has also been improved with enhancements to Session Initiation Protocol (SIP) and new Skinny Client Control Protocol (SCCP) support. Other features include dynamic shunning when combined with a Cisco Intrusion Detection Sensor (IDS), PAT port redirection, stateful failover of HTTP (port 80) sessions, and more.
More product information

Catalyst 6513 Switch
The Cisco Catalyst 6513, a new 13-slot chassis in the Catalyst 6500 Series, delivers the industry's most scalable performance and richest set of intelligent network services to meet the demanding requirements of fast-growing enterprise and service provider networks. With up to 576 10/100 ports and 194 gigabit ports per chassis, the Catalyst 6513 provides densities of 1152 10/100 and 388 gigabit ports per 7-foot rack with unsurpassed levels of network resilience. These high densities combined with the new Switch Fabric Module 2 option for Catalyst 6500 Series switches (see below) provide for scalable switching bandwidth up to 256 Gbps and 210 million pps.
More product information

Catalyst 6500 Series: Switch Fabric Module 2
The Switch Fabric Module 2 provides a framework for delivering the 256-Gbps high-bandwidth architecture for Catalyst 6500 Series switches. The Switch Fabric Module 2 is a key enabler for the optional distributed forwarding technology. The module combined with distributed switching line cards allows up to 24 million pps of local forwarding per line card while providing the highest level of network availability.
More product information

Central Office and Point of Presence

Cisco 12406 Internet Router
The Cisco 12000 and 12400 Series of high-end Internet routers has gained a new family member suited for use in smaller points of presence (POPs). The six-slot Cisco 12406 Internet Router scales to support five 10-Gbps (OC-192/STM-64) uplink connections. eight Fast Ethernet (100 Mbps) interfaces. and three Gigabit Ethernet connections in a quarter-rack-unit footprint. At a price point that's about 40 percent less than the larger Cisco 10-Gbps IP routers. the new Cisco 12406 Internet Router enables service providers with high-speed connectivity requirements in smaller markets to reduce their capital investments. The router is also suited for use in Internet data centers of Web hosting companies and for service provider

private-peering applications where very high speeds but a relatively small number of connections are required.
More product information

Cisco 10000 Series IPsec VPN Service Module
For service providers ready to deploy remote-access and site-to-site IP virtual private network (VPN) services at the network edge, the new Cisco 10000 Series IP Security (IPsec) VPN Service Module offers industry-leading performance on the only IP aggregator with both IPsec and Multiprotocol Label Switching (MPLS) VPN capabilities. Each module can scale up to 25,000 IPsec tunnels with Triple Data Encryption Standard (3DES) throughput of 250 Mbps. The IPsec VPN Service Module enables deployment of services such as content hosting without compromising performance, scalability, or carrier-class availability.
More product information

Cisco ONS 15540 Extended Services Platform
The Cisco ONS 15540 Extended Services Platform (ESP) is a highly modular, scalable, service-rich dense wavelength-division multiplexing (DWDM) system that delivers integrated data and storage networking and information streaming over an ultra-high bandwidth optical infrastructure capable of supporting any packet on any wavelength from any platform. The product supports up to 32 protected wavelengths per fiber pair, operating at variable speeds from 16 Mbps to 2.5 Gbps, for a capacity of 80 Gbps per system that's scalable in the future. The Cisco ONS 15540 ESP is covered in greater detail in "The Metro Ramps Up."
More product information

Cisco uBR7100 Series Universal Broadband Router
The Cisco uBR7100 Series Universal Broadband Router is a Data-over-Cable Service Interface Specification (DOCSIS) 1.0-qualified cable modem termination system (CMTS) that supports broadband cable services with speeds up to 39 Mbps downstream. The Cisco uBR7111 provides one downstream and one upstream channel, and the Cisco uBR7114 provides one downstream and four upstream channels. These compact, two-rack-unit models are ideal for deployment in small distribution hubs serving small residential communities or inside multiunit buildings such as hotels and apartments. Both uBR7100 models include an integrated up converter and Cisco Network Registrar software.
More product information

Cisco ONS 15200 Metro DWDM Series
The Cisco ONS 15200 Series is the first metropolitan DWDM solution capable of delivering wavelengths to buildings -- taking optical intelligence and bandwidth closer to end users. The multichannel Cisco ONS 15252 combines with the single-channel ONS 15201 to deliver wavelength services such as Gigabit Ethernet and OC-48 packet over SONET in a single rack unit. The Cisco ONS 15216 provides optical filtering to combine wavelengths launched by the Cisco ONS 15454 and 15325 optical transport and metro edge optical transport platforms, respectively; as well as optical add-drop multiplexing to exchange wavelengths on SONET/SDH spans between the Cisco ONS 15252, 15201, and 15454 platforms.
More product information

Cisco 10005 Internet Router
The Cisco 10005 Internet Router includes seven slots supporting Layer 2 and 3 software services for thousands of dedicated access connections. This new router enables three service provider applications: decentralized POPs, equipment consolidations for collocation, and high-density aggregation of DS3 circuits. The Cisco 10005 performance routing engine uses Cisco Parallel Express Forwarding (PXF) technology to deliver line-rate IP services.

The router also supports a broad range of transport interfaces and service modules. For more on the Cisco 10005 Internet Router, see "New Routes to Revenue."
More product information

Cisco Intelligence Engine 2100 Series
The Cisco Intelligence Engine 2100 Series is a new type of network device that provides an intelligent network interface to applications and users. Fully integrated with Cisco's Configuration Express ordering solution and the new Cisco embedded agent technology, the IE 2100 Series provides an end-to-end, hands-free deployment solution for Cisco customer premises equipment (CPE)-based network services. The IE 2100 is covered in greater detail in "The Intelligent Engine that Could."
More product information

Cisco TransPath Multiservice System
The Cisco TransPath™ Multiservice System is a cost-effective, turnkey solution for MPLS, Frame Relay, ATM, packet voice, and circuit emulation services. The system is optimized for applications such as network-based IP VPNs, DSL backhaul, and mobile wireless transport. The Cisco BPX® 8620 ATM switch provides the TransPath system foundation. Network managers can add up to two Cisco VXR 7204 Label Switch Controllers for MPLS functionality and five Cisco MGX™ 8230 or Cisco MGX 8250 Concentrators for narrowband services.
More product information

Cisco 7400 Internet Router
The new Cisco 7400 Internet Router delivers OC-3 performance with Cisco PXF processing hardware-accelerated services. Its compact architecture offers a cost-effective, stackable, highly versatile solution for enterprises and service providers, with a choice of more than 40 modular interfaces. The Cisco 7400 is ideal for application-specific deployments in the broadband subscriber aggregation and managed services (customer premises and customer leased equipment) markets. The Cisco 7401 ASR-BB delivers the highest subscriber density available with up to 640,000 subscribers per rack for DSL, ISDN, and fiber-to-the-curb as well as mobile or fixed wireless services. The Cisco 7401 ASR-CP delivers a range of bandwidth management and security services such as Network Address Translation (NAT), access control lists (ACLs), MPLS VPN, MPLS provider edge, and QoS features. The Cisco 7400 can also be deployed as an appliance dedicated to certain network requirements. Its small form factor and stackable architecture enable implementation of specific IP services at optimum performance, for example, QoS enforcement with hardware-accelerated policing, Class-Based Weighted RED, and low-latency queuing. For more on the Cisco 7400 Internet Router, see "New Routes to Revenues."
More product information

Cisco 7600 Internet Router: Two Optical Service Modules
The Cisco 7600 Internet Router now has two new channelized optical service modules (OSMs) for high-speed WAN edge aggregation. The OSMs are available in OC-12 and OC-48 options, each with a choice of two port densities: a four- and eight-port version for OC-12 and a one- and two-port version for OC-48. The Cisco 7600 can now scale to more than 2000 DS3 ports or up to 768 OC-3c ports per 7-foot rack -- making it the highest density, highest-performance edge aggregation solution for IP-enabled DS3 and OC-3 services.

Campus, Departments, and Workgroups

Catalyst 4000 Family 24-Port 10/100/1000BaseT Line Card

The new Cisco Catalyst® 4000 24-port 10/100/1000BaseT line card enhances Cisco's leadership in the enterprise space by providing the industry's highest-density auto-negotiating Gigabit Ethernet from the network edge directly to desktop computers or servers. With Cisco's triple-speed auto-sensing technology, the line card supports 10-Mbps, 100-Mbps, and 1000-Mbps connection speeds on the same interface for flexibility and seamless migration to Gigabit Ethernet. The line card occupies one slot in either the Catalyst 4003 or 4006 Series switches, taking the maximum density to 48 ports in the Catalyst 4003 and 120 ports in the Catalyst 4006.
More product information

Catalyst 3550-12T Switch
The new multilayer Gigabit Ethernet Catalyst 3550-12T Switch gives network managers greater control of their LANs by combining the power of Cisco IOS® Intelligent Network Services with the simplicity of Web-based management using the Cisco Cluster Management Software interface. This 1000BaseT switch significantly improves network availability, scalability, and security by deploying Cisco IOS Intelligent Network Services in either the network backbone or the wiring closet, where it functions as a top-of-the-stack aggregation switch using Category 5 copper cabling. The Catalyst 3550-12T enables multilayer services such as IP routing, advanced quality of service (QoS), and IP Security (IPsec). For more on the Catalyst 3550-12T, see "This Old Wiring Closet."
More product information

Catalyst 2950 Series Switches
The Catalyst 2950 Series switches deliver next-generation performance and functionality for the LAN with 10/100/1000BaseT uplinks, enhanced Cisco IOS services, QoS, and multicast management features using the simple, Web-based Cisco Cluster Management Software interface. These wire-speed, Fast Ethernet desktop switches include the Catalyst 2950-12 with 12 10/100 ports, the 2950-24 with 24 10/100 ports, the 2950T-24 with 24 10/100 ports and two 10/100/1000BaseT uplink ports, and the 2950C-24 with 24 10/100 ports and two 100BaseFX uplink ports. For more on the Catalyst 2950 Series switches, see "This Old Wiring Closet."
More product information

Small and Midsized Businesses, Branch Offices, and Home Offices

Cisco 1751 Modular Access Router
The Cisco 1751 Modular Access Router provides high-speed network access, comprehensive security features, VPN support, and integration of multiple services for voice, data, video, and fax communication. Delivering 12,000 packets per second (pps) routing performance, the Cisco 1751 supports a digital voice port, IEEE 802.1Q virtual LAN (VLAN), an Asymmetric Digital Subscriber Line (ADSL) interface card, encryption at speeds up to T1/E1, and two WAN/voice interface cards.
More product information

Cisco 828 and Cisco SOHO 78 G.SHDSL Routers
The Cisco 828 and Cisco SOHO 78 Routers support G.SHDSL for small businesses and small office/home office (SOHO) customers, enabling value-added services. The Cisco 828 supports extensive quality-of-service (QoS) features and business-class security with an optional stateful inspection firewall and IP Security (IPsec) Triple Data Encryption Standard (3DES) for virtual private networks (VPNs). The Cisco SOHO 78 provides multiuser access for SOHO users with a packet filtering firewall. Both models offer remote management and reliability through Cisco IOS® Software. For more information, see "Last Mile."

More information on Cisco 800 Series Router
More information on the Cisco SOHO Series Router

Cisco 806 Broadband Gateway Router
The Cisco 806 Broadband Gateway Router offers a fixed configuration for connecting two 10BaseT Ethernet LANs. The software-upgradable platform supports multiuser access over a single broadband connection. Business-class security features include a stateful inspection firewall for perimeter security and data encryption for VPNs. The router supports video, voice, and data traffic management with QoS over DSL, cable, Ethernet, or Long-Reach Ethernet (LRE) technology. For more information on the Cisco 806 Broadband Gateway Router, see "Last Mile."
More product information

Catalyst 4224 Access Gateway Switch
The new Cisco Catalyst® 4224 Access Gateway Switch -- an integrated Ethernet switching, IP routing, and voice gateway device -- extends IP telephony to small branch offices with up to 24 users, and reduces capital and labor costs for enterprises. The two-rack-unit Catalyst 4224 allows enterprises to realize a lower total cost of ownership by lowering management and maintenance expenses, decreasing operational complexity, and accelerating time to deployment. The Catalyst 4224 uses the new Cisco Survivable Remote Site (SRS) Telephony software feature to provide backup services in the event of WAN failure, making it a powerful platform for delivering all of Cisco's enhanced IP features and applications to small branch locations simply and cost effectively. For more on the Catalyst 4224 Access Gateway Switch, see "Blurring the Lines."
More product information

New VPN Clients: Cisco VPN Client Version 3.0 and Cisco VPN 3002 Hardware Client
Two new client products are now available for remote access to a VPN. The Cisco VPN Client Version 3.0 establishes secure, end-to-end encrypted tunnels to selected Cisco devices that support the new Cisco Unified Client Framework. The Cisco VPN 3002 Hardware Client is a small appliance for remote-office access to a VPN, accommodating connections to hundreds of stations on a single LAN. This client works with any operating system and supports 56-bit DES or 168-bit 3DES IPsec encryption. Both clients allow policies and configuration to be pushed from the central site.
More information on Cisco VPN 3000 Concetrator Series
More information on Virtual Private Networks

Cisco IP Telephony Solutions
Eight new Cisco software and hardware products help enterprises enhance communications between corporate and branch offices, boost personal and workgroup productivity, reduce administrative costs, and provide greater flexibility in applications deployment to the desktop. New software solutions include Cisco Personal Assistant, QoS Policy Manager Version 2.1, Cisco Unity™ 2.46 Unified Communications Server, Cisco IP Integrated Contact Distribution, the Cisco IP Phone Productivity Applications Suite, Cisco CallManager Version 3.1 Call Processing System, and an innovative SRS Telephony feature that is now part of Cisco IOS® Software. Also available is the Cisco Catalyst 4224 Access Gateway Switch. These new IP telephony solutions are covered in greater detail in "Blurring the Lines".
More product information

Cisco ATA 186 Analog Telephone Adaptor
The Cisco ATA 186 Analog Telephone Adaptor brings basic residential telephones into the networked world. By turning analog phones into IP phones, the Cisco ATA 186 addresses the needs of an emerging market for "second-line" voice-over-IP services among residential customers. With this

easy-to-use accessory, service providers can now offer immediate revenue-generating IP telephony-based services to their residential broadband customers. The new adaptor takes advantage of broadband pipes through DSL, fixed wireless, and cable technologies while seamlessly integrating into service provider architectures.
More product information

Cisco IOS Software Update

Cisco IOS Technologies Release IP Version 6 (IPv6) Support
Cisco IOS® Software Release 12.2(2)T introduces the support of IP Version 6 (IPv6) protocols, which enable IP to scale for billions of users and Internet appliances. IPv6 resolves the address shortage problem by quadrupling the IP address length to 128 bits, thus providing thousands of IP addresses for each Internet user. IPv6 also offers the benefits of integrated auto-configuration and global addressing architecture for quality of service (QoS), security, and mobility. The Cisco IOS IPv6 implementation enables coexistence with IPv4 via a dual stack. IPv6 is covered in greater detail in "Technology."
More product information

About New Product Dispatches

Keeping up with Cisco's myriad new products can be a challenge. To help readers stay informed, *Packet*™ magazine's "New Product Dispatches" provide snapshots of the latest products released by Cisco between January and April 2001. For real-time announcements of the most recently released products, check the "What's New" section of Cisco.com.

Reader Feedback: Tell us what you think.

Acrobat

Download a PDF of "New Product Dispatches." (Or download a PDF of the entire Third Quarter 2001 issue of *Packet*.)

Documentação
Pseries
Servidor RISC Tipo 1
Manuais de 14 a 25 e 37 a 40

ITEM 2.10 (5)

- Height: 172.8 mm (06.8 in)
- Weight:
  - 32.0 kg (70.4 lb) - Minimum Configuration
  - 47.3 kg (104 lb) - Maximum Configuration with rails

Operating Environment

- Temperature: 5 to 35 degrees C (41 to 95 F)
- Relative humidity: 8% to 80%
- Maximum wet bulb: 27 degrees C (80 F)
- Operating voltage: (auto-ranging) 100 to 127 or 200 to 240 V ac
- Operating frequency: 50/60 Hz
- Power requirements:
  - 2-way (typical configuration): 330 watts
  - 2-way (maximum configuration): 500 watts
  - 4-way (typical configuration): 500 watts
  - 4-way (maximum configuration): 750 watts
- Thermal output:
  - 2-way (typical configuration): 1129 BTU/hour
  - 2-way (maximum configuration): 1693 BTU/hour
  - 4-way (typical configuration): 1693 BTU/hour
  - 4-way (maximum configuration): 2540 BTU/hour
- Power source loading:
  - 2-way (typical configuration): 0.348 kVA
  - 2-way (maximum configuration): 0.522 kVA
  - 4-way (typical configuration): 0.522 kVA
  - 4-way (maximum configuration): 0.783 kVA
  - Maximum altitude: 2,135 m (7,000 ft)

Noise Level and Sound Power

- Sound Power: Model 6C4 6.0 Bels Idle/6.0 Bels Operating

EMC Conformance Classification

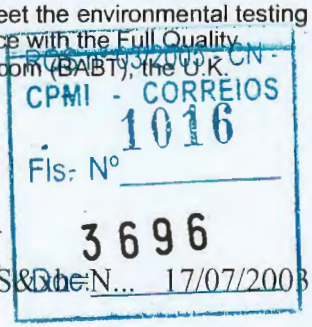
- This equipment is subject to FCC rules and it shall comply with the appropriate FCC rules before final delivery to the buyer or centers of distribution.
  - U.S.A.: FCC Class A for Rack Mount
  - Europe: CISPR 22 Class A for Rack Mount
  - Japan: VCCI-A for Rack Mount
  - Korea: Korean Requirement Class A for Rack Mount
  - China: People's Republic of China commodity inspection law

Homologation – Telecom Environmental Testing (Safety and EMC)

- Homologation approval for specific countries has been initiated with the IBM Homologation and Type Approval (HT&A) organization in LaGaude. These IBM pSeries models and applicable features meet the environmental testing requirements of the country TELECOM and have been designed and tested in compliance with the Full Quality Assurance Approval (FQAA) process as delivered by the British Approval Board for Telecom (BABT), the U.K. Telecom Regulatory authority.

Product Safety/Country Testing/Certification

- UL 1950 Underwriters Laboratory, Safety Information



7028-6C4 IBM eServer pSeries 630 Model 6C4

IBM U.S. Sales Manual
Revised: July 11, 2003.

Document options

Printable version

IBM U.S. Product Life Cycle Date

Type Model	Announced	Available	Marketing Withdrawn	Service Discontinued	Replaced By
7028-6C4	2002/06/25	2002/08/30	-	-	-

Back to top

Abstrac

IBM UNIX systems consist of the IBM eServer pSeries and IBM RS/6000 product lines. Providing unprecedented value, these innovative systems feature IBM's leading-edge technology and run the top-rated UNIX operating system, AIX. This broad product line ranges from powerful workstations ideal for mechanical design; to mission-critical symmetric multiprocessing (SMP) servers for ERP, SCM, CRM, transaction processing, and Web serving; up to parallel RS/6000 SP systems that can handle demanding scientific and technical computing and business intelligence tasks. These platforms provide the power to create change and the flexibility to manage it, with thousands of applications that provide real value. More than 1,000,000 systems have shipped to over 135,000 businesses worldwide.

Model Abstract 7028-6C4

The 7028 IBM eServer pSeries 630 Model 6C4 is a Rack-mount Server. The Model 6C4 provides the power, capacity, and expandability required for e-business computing. It offers 64-bit scalability via the 64-bit POWER4 or POWER4+ processor packaged as 1-way and 2-way cards. With its two-processor positions, the Model 6C4 can be configured into 1-, 2- or 4-way configurations. The processor cards operate at 1.0 GHz with 32 MB of L3 cache per processor card, or 1.2 and 1.45 GHz with 8 MB of L3 cache per processor. Memory DIMMs are mounted on the CPU card and can contain up to 32 GB of memory.

The Model 6C4 contains six bays. The four front-accessible, hot-swap capable bays can accommodate up to 587.2 GB of disk storage.

Other integrated features include:

- Four hot-swap, 64-bit PCI-X slots with 1.0 GHz processor systems, Six hot-swap, 64-bit PCI-X slots with 1.2 and 1.45 GHz processor systems.
- Service processor
- Two 10/100 ethernet ports
- Two Ultra3 SCSI ports (internal/external)
- Three serial ports and one parallel port
- Keyboard and mouse ports
- Optional hot-swap fans

- Attributes required: 1 processor card slot
- For 7028-6C4: (#5132)
  - Minimum required: 0
  - Maximum allowed: 2 (Initial order maximum: 0)
  - OS level required: AIX 5.1, or later
  - Initial Order/MES/Both/Supported: MES
  - CSU: No
  - Return parts MES: Yes

(#5133) 1-way 1.2 GHz POWER4+ Processor Card

1-way processor card with 1.20 GHz POWER4+ processor, 8 memory DIMM slots, and 8MB of L3 cache.

- Attributes provided: 1-way processor card
- Attributes required: 1 processor card slot
- For 7028-6C4: (#5133)
  - Minimum required: 0
  - Maximum allowed: 2 (Initial order maximum: 2)
  - OS level required: AIX 5.1 or AIX 5.2, or later
  - Initial Order/MES/Both/Supported: Both
  - CSU: Yes
  - Return parts MES: Feature conversion only

(#5134) 2-way 1.2 GHz POWER4+ Processor Card

2-way processor card with 1.20 GHz POWER4+ processor, 8 memory DIMM slots, and 8MB of L3 cache per processor.

- Attributes provided: 2-way processor card
- Attributes required: 1 processor card slot
- For 7028-6C4: (#5134)
  - Minimum required: 0
  - Maximum allowed: 2 (Initial order maximum: 2)
  - OS level required: AIX 5.1 or AIX 5.2, or later
  - Initial Order/MES/Both/Supported: Both
  - CSU: Yes
  - Return parts MES: Feature conversion only

(#5700) IBM Gigabit Ethernet-SX PCI-X Adapter:

The IBM Gigabit Ethernet-SX PCI-X Adapter provides a 1 Gbps (1000 Base-SX) full-duplex Ethernet LAN connection with throughput on a standard shortwave multimode optical cable which conforms to the IEEE 802.3z standard. The adapter supports distances of 260m for 62.5 micron Multi Mode Fiber (MMF) and 550m for 50.0 micron MMF. AIX Network Install Manager (NIM) boot capability is supported with this adapter.

Note: For optimum performance, the adapter should be placed in a 64-bit PCI-X card slot.

Note: The IBM Gigabit Ethernet-SX PCI-X Adapter (#5700) incorporates an LC type connector on the card. This new, smaller form factor connector is being used by the industry for the next generation of fiber optic networks. If connecting into an older, existing SC type connector network, an LC-SC 62.5 Micron Fiber Converter Cable (#2459) or LC-SC 50 Micron Fiber Converter Cable (#2456) is required.

Limitation: Half-Duplex (HDX) mode is not supported.

- Attributes provided: One full-duplex 1000Base-SX fiber connection to a Gigabit Ethernet LAN.
- Attributes required: One available PCI or PCI-X card slot
- For 7028-6C4: (#5700)
  - Minimum required: 0
  - Maximum allowed: 5 (Initial order maximum: 5)
  - OS level required: AIX 5.1 with the 12/2002 or later Update CD, AIX 5.2 with the 12/2002 or later Update CD
  - Initial Order/MES/Both/Supported: Both
  - CSU: Yes
  - Return parts MES: No

(#5701) IBM 10/100/1000 Base-TX Ethernet PCI-X Adapter:

The IBM 10/100/1000 Base-TX Ethernet PCI-X Adapter is a Full-Duplex Gigabit Ethernet adapter designed with highly

integrated components. This adapter can be configured to run at 10, 100, or 1000 Mbps data rates. The adapter interfaces to the system via the PCI-X bus and connects to the network using a 4-pair CAT-5 Unshielded Twisted Pair (UTP) cable for distances of up to 100m. AIX Network Install Manager (NIM) boot capability is supported with this adapter. The adapter conforms to the IEEE 802.3ab 1000Base-T standard. The adapter also supports jumbo frames when running at the 1000 Mbps speed.

Note: For optimum performance, adapter should be placed in a 64-bit PCI-X card slot.

Limitations: The 1000 Mbps speed is not supported in Half-Duplex (HDX) mode.

- Attributes provided: One full-duplex 10/100/1000Base-TX UTP connection to a Gigabit Ethernet LAN.
- Attributes required: One available PCI or PCI-X card slot
- For 7028-6C4: (#5701)
  - Minimum required: 0
  - Maximum allowed: 5 (Initial order maximum: 5)
  - OS level required: AIX 5.1 with the 12/2002 or later Update CD, AIX 5.2 with the 12/2002 or later Update CD
  - Initial Order/MES/Both/Supported: Both
  - CSU: Yes
  - Return parts MES: No

(#5706) IBM 2-Port 10/100/1000 BaseTX Ethernet PCI-X Adapter

The IBM 2-Port 10/100/1000 Base-TX Ethernet PCI-X Adapter is a Full-Duplex, dual ported, Gigabit Ethernet adapter designed with highly integrated components. This adapter can be configured to run each port at 10, 100, or 1000 Mbps data rates. The adapter interfaces to the system via a PCI or PCI-X bus and connects to a network using a 4-pair CAT-5 Unshielded Twisted Pair (UTP) cable for distances of up to 100m. AIX Network Install Manager (NIM) boot capability is supported with this adapter. The adapter conforms to the IEEE 802.3ab 1000Base-T standard. The adapter also supports jumbo frames when running at the 1000 Mbps speed.

A function called 'Large Send' or sometimes known as TCP Segmentation is also provided by this adapter. This function offloads the TCP segmentation operation from the AIX IP layer to the adapter for outgoing (transmit side) TCP segments. Another function known as "Checksum Offload" which offloads the TCP/UDP Checksum Operation or workload from the CPU to the adapter is also provided.

The IBM 2-Port 10/100/1000 Base-TX Ethernet PCI-X Adapter (#5706) should be considered where maximum port density is required per I/O card slot. For a suggested maximum number of adapters taking performance into consideration, refer to the RS/6000 & pSeries PCI Adapter Placement Reference SA38-0538. If card slots are not the limiting factor and maximum throughput is required, the single port IBM 10/100/1000 Base-TX Ethernet PCI-X Adapter (#5701) is the preferred solution. Note: For optimum performance, the adapter should be placed in a 64 bit PCI-X card slot whenever possible.

Limitations: The 1000 Mbps speed is not supported in Half-Duplex (HDX) mode.

- Attributes provided: Two full-duplex 10/100/1000Base-TX UTP connections to Gigabit Ethernet LAN(s).
- Attributes required: One available PCI or PCI-X card slot
- For 7028-6C4: (#5706)
  - Minimum required: 0
  - Maximum allowed: 6 (Initial order maximum: 6)
  - OS level required: AIX 5.1 or later, AIX 5.2 or later
  - Initial Order/MES/Both/Supported: Both
  - CSU: Yes
  - Return parts MES: No

Note: For optimum 2-Port Gigabit Ethernet PCI-X Adapter performance, systems manufactured prior to December 6, 2002 may require a system firmware update. Check the following Web URL after December 6, 2002 to review and download latest firmware if needed.

http://www.austin.ibm.com/support/micro/

If Feature Number 9556 or Feature Number 6556 is not installed in the system, the Maximum Allowed and Inital order maximum is 4.

(#5707) IBM 2-Port Gigabit Ethernet-SX PCI-X Adapter

The IBM 2-Port Gigabit Ethernet-SX PCI-X Adapter provides two 1 Gbps (1000 Base-SX) full-duplex Ethernet LAN connections with throughput on a standard shortwave multimode optical cable that conforms to the IEEE 802.3z standard. The adapter supports distances of 260m for 62.5 micron Multi Mode Fiber (MMF) and 550m for 50.0 micron MMF. AIX Network Install Manager (NIM) boot capability is supported with this adapter.

A function called 'Large Send' or sometimes known as TCP Segmentation is also provided by this adapter. This function offloads the TCP segmentation operation from the AIX IP layer to the adapter for outgoing (transmit side) TCP segments.

- Interface: SCSI-2 16-bit Low Voltage Differential(LVD) / Single-ended (SE) Asynchronous/Synchronous
- Compatibility: See the following Technical Support Web page (8mm Tape Interchange Information section) for compatability information:

  http://techsupport.services.ibm.com/server/ mdownload/tapewhdr.html

- Attributes provided: 60/150GB 16-bit 8mm Internal Tape Drive
- Attributes required: One 1.6-inch(41mm) half-high media bay and one SCSI-2 internal 16-bit address
- For 7028-6C4: (#6134)
  - Minimum required: 0
  - Maximum allowed: 1 (Initial order maximum: 1)
  - OS level required: AIX 5.1 or later, AIX 5.2 or later
  - Initial Order/MES/Both/Supported: Both
  - CSU: Yes
  - Return parts MES: No

(#6156) 20/40GB 16-bit 8mm Internal Tape Drive (Black Bezel)

(For IBM US, No Longer Available as of December 6, 2002)

This feature consists of a 5.25-inch half-high, single-ended, 16-bit tape drive. This drive provides a high capacity tape drive for save/restore and archiving functions. This tape drive uses IBM 8mm data cartridges and is compression capable, providing a capacity of up to 40 GB -- a 400% increase over the previous 5/10 GB 8mm internal tape drive. (Black bezel)

Characteristics:

- Capacity: 20.0 GB Native Mode, 40.0 GB (typical) Compression Mode
- Form Factor: 5.25-inch Half-high
- Media: IBM 8mm Data Cartridge
- Technology: Helical Scan, Rotating Head
- Operation: Streaming
- Data Transfer Rate: 3MB/Sec. Native Mode, 6MB/Sec. (typical) Compression M
- Interface: SCSI-2 16-bit (Single-ended) Asynchronous/Synchronous
- Compatibility: 2.3 GB Mode (Read only), 2.3 GB mode with Compression (Read only), 5 GB Mode (Read only), 5 GB Compression (Read only), 7 GB Mode (Read only), 7 GB Compression (Read only), 20 GB Mode (R/W), 20 GB Compression (R/W).
- Attributes provided: 8mm tape capability
- Attributes required: One 1.6-inch(41mm) half-high media bay and one SCSI-2 internal SE 16-bit address
- For 7028-6C4: (#6156)
  - Minimum required: 0
  - Maximum allowed: 1 (Initial order maximum: 1)
  - OS level required: AIX 5.1, or later
  - Initial Order/MES/Both/Supported: Both
  - CSU: Yes
  - Return parts MES: No

(#6158) 20/40GB 4mm Internal Tape Drive

The 20/40 GB 4-mm Internal Tape Drive is a 5.25-inch, half-high, single-ended 16-bit tape drive, which provides a high capacity for save/restore and achieve functions. This tape drive uses IBM 4-mm data cartridges and is compression capable, providing a capacity of up to 40 GB - a significant increase in capacity over the previous 12/24 4-mm internal tape drives (when using DDS-4 media).

Characteristics:

- Capacity: 20 GB native mode, 40 GB (typical) compression mode
- Form Factor: 5.25-inch half high
- Media: IBM 4-mm DDS-4 data cartridge
- Technology: Helical scan, rotating head
- Operation: Streaming
- Data Transfer Rate: 3MBps native mode, 6MBps (typical) compression
- Interface: SCSI-2 (single ended) asynchronous/synchronous
- Compatibility: 4 GB mode (Read/Write), 8 GB compression (Read/Write); 12 GB mode(Read/Write), 24 GB compression (Read/Write), 20 GB mode (Read/Write), 40 GB compression (Read/Write).

- Return parts MES: No

Note: Fibre Channel boot capability is supported on this system with this adapter provided your system firmware is at the proper support level.

(#6273) Power Supply, 645 Watt AC, Hotswap, Base and Redundant

This feature provides a 645 Watt AC power supply, either as the primary power supply in the system, or the secondary power supply for redundant power. Each power supply, base and redundant, comes with one power cord.

- Attributes provided: 645 Watt AC Power Supply
- Attributes required: Available Power Supply Bay
- For 7028-6C4: (#6273)
  - Minimum required: 0
  - Maximum allowed: 2 (Initial order maximum: 2)
  - OS level required: AIX 5.1, or later
  - Initial Order/MES/Both/Supported: Both
  - CSU: Yes
  - Return parts MES: No

(#6274) Power Supply, 645 Watt DC, Hotswap, Base and Redundant

This feature provides a 645 Watt DC power supply, either as the primary power supply in the system, or the secondary power supply for redundant power.

- Attributes provided: 250 Watt DC Power Supply
- Attributes required: Available Power Supply Bay
- For 7028-6C4: (#6274)
  - Minimum required: 0
  - Maximum allowed: 2 (Initial order maximum: 2)
  - OS level required: AIX 5,1, or later
  - Initial Order/MES/Both/Supported: Both
  - CSU: Yes
  - Return parts MES: No

(#6285) Power cable, DC, Drawer (3-pin) to PDP (3-pin), 4M

This 4 meter cable is available to connect a rack system drawer (3-pin) to the appropriate 3-pin connection in the DC Power Distribution Panel (PDP).

- Attributes provided: Cable
- Attributes required: DC power supply
- For 7028-6C4: (#6285)
  - Minimum required: 0
  - Maximum allowed: 2 (Initial order maximum: 2)
  - OS level required: AIX 5.1, or later
  - Initial Order/MES/Both/Supported: Both
  - CSU: Yes
  - Return parts MES: No

(#6286) Power Cable, DC, Drawer (3-pin) to PDP (5-pin)

This 4 meter cable is available to connect a rack system drawer (3-pin) to the apporpriate 5-pin connection in the DC Power Distibution Panel (PDP).

- Attributes provided: Cable
- Attributes required: DC power supply
- For 7028-6C4: (#6286)
  - Minimum required: 0
  - Maximum allowed: 2 (Initial order maximum: 2)
  - OS level required: AIX 5.1, or later
  - Initial Order/MES/Both/Supported: Both
  - CSU: Yes

ITEM 4.2.1 – 1 (3, 9, 10)

Uncompromising high-end server for an on demand world

IBM @server pSeries 690

pSeries 690 high-end server with optional expansion frame

As the flagship system of the IBM **@server**™ pSeries™ product line, the p690—a highly advanced server that can help lower costs, improve efficiency and speed transformation to e-business—is the gold standard for UNIX® computing in the on demand world. Through leading-edge innovations such as high-performance microprocessors, dense packaging, advanced clustering techniques and mainframe-inspired reliability, availability and serviceability (RAS) features, the pSeries 690 can deliver top power, flexibility and reliability for both commercial and technical computing applications.

Highlights

- ***IBM POWER4+ microprocessors provide high performance for diverse workloads***
- ***pSeries on demand capabilities help businesses adapt at the pace of e-business***
- ***Self-managing features enhance resiliency and help reduce total cost of ownership***

Success in today's e-business world requires that companies react immediately—on demand—to any shift in the competitive environment. Customers expect instantaneous adaptation to changing market conditions, which means that companies can no longer afford to wait for their IT infrastructure to catch up to their strategy. They need the agility to scale at a moment's notice with unprecedented power and performance from every component. And to support it all, they need mainframe-level reliability features designed to ensure that applications and data are available 24 hours a day, 7 days a week.

Features such as dynamic logical partitioning and flexible capacity on demand upgrades also contribute to strong pSeries 690 performance while preserving operational versatility. In addition, innovative self-managing RAS features derived from the IBM autonomic computing initiative help drive down costs and complexity by lowering administrative overhead. By combining the most advanced IBM leadership technology for enterprise-class performance and flexible adaptation to changing market conditions, the

pSeries 690 delivers the key capabilities businesses need to compete in today's e-business on demand™ environment.

Fast processors/dense packaging for speed

The pSeries 690 is the ultimate high-end IBM UNIX server. Designed to provide datacenter-class capacity, performance and reliability, the POWER4+™ microprocessors in the pSeries 690 utilize "SMP-on-a-chip" design. At 1.5 GHz or 1.7 GHz, these processors are among the fastest 64-bit chips in the world[1]. Because they also incorporate copper and silicon-on-insulator (SOI) technology, these chips are designed to consume less power—saving energy while delivering high reliability and outstanding performance. For more value-oriented customers, available 1.1 GHz or 1.3 GHz POWER4™ chips can provide similar processing characteristics at a reduced price. Customers with existing POWER4 pSeries 690 systems can upgrade to the POWER4+ configurations to boost application speed and throughput.

Innovative CPU packaging also contributes to enterprise-class performance and reliability from the p690. Advanced Multichip Module (MCM) architecture, similar to the design used in IBM @server zSeries™ servers, places up to eight microprocessors on a single MCM so small that it can fit in the palm of your hand. To further enhance performance, Level 2 (L2) cache and 128MB of Level 3 (L3) cache is packaged with the MCM. L3 cache helps stage information more effectively from processor memory to application programs. By decreasing the physical distance between components, MCM architecture enables faster movement of information—resulting in greater speed and improved reliability compared with earlier, less dense component configurations.

Additional "book" packaging for memory can help protect components from electrostatic discharge and physical damage. With space for up to eight memory books per server, the pSeries 690 offers up to a 32-way configuration with 8GB to 512GB of total memory—providing tremendous enterprise-class processing power for both commercial and technical workloads.

Designed to support the incredible speed of the processors, pSeries 690 architecture also features a peak aggregate memory to L3 cache bandwidth of 204.8GB per second in a 32-way configuration. In addition, the system can deliver an aggregate I/O subsystem bandwidth of up to 44GB/second. With its unique system architecture, the pSeries 690 can offer the speed and power to deliver efficient, cost-effective data sharing and application throughput.

Partitioning for quick response to change

IBM's logical partitioning (LPAR) implementation provides outstanding flexibility in matching resources to workloads, facilitating higher efficiency and lower total cost of ownership (TCO), while providing robust isolation of operating environments. The pSeries 690 system can be divided into as many as 32 independent logical servers or partitions, each with its own memory, processors, I/O and copy of the AIX 5L™ or Linux® operating system. By enabling consolidation of applications using both operating systems onto a single platform, the pSeries 690 can increase system utilization, provide greater flexibility of managing the dynamics of multiple workloads in a single server, reduce complexity and deliver significant administration savings.

Feature	Benefits
Choice of POWER4/POWER4+ microprocessors with L3 cache	• Provides improved system and application performance and higher reliability for commercial applications in a smaller, more efficient dual-processor chip • Enables capacity to grow to 32 processors • Provides flexibility to grow in performance as workloads increase with minimal disruption and incremental cost
Copper and SOI technology	• Improves processor performance and reliability while using less power and producing less heat to help conserve energy and help lower operational costs
High memory and I/O bandwidth	• Helps remove performance bottlenecks that can occur when fast processors must wait for data to be moved through the system • Delivers increased memory bandwidth for the needs of HPC applications
Up to 512GB ECC Chipkill™ bit-steering memory	• Allows exploitation of 64-bit addressing for large database, HPC and key critical business applications • Provides growth options with outstanding throughput • Significantly lowers number of memory failures that can cause system outages, thus increasing system availability • Provides memory spares that are activated when multiple memory errors are encountered
Capacity Upgrade on Demand	• Offers flexibility to cost-effectively and easily add permanent processing and memory capacity to help meet workload growth
On/Off Capacity on Demand	• Provides temporary processor use to meet unexpected workload demands
Book packaging	• Protects memory components against accidental disconnection and/or contamination • Facilitates easier servicing
Logical partitioning (LPAR)	• Permits up to 32 UNIX or Linux operating system servers to be consolidated on a single system, easing maintenance and administration • Offers greater flexibility in using available capacity and dynamically matching resources to changing business requirements (requires AIX 5L V5.2)
Up to 160 PCI/PCI-X hot-plug/blind-swap adapter slots	• Provides growth options for significantly increased capacity • Supports many commonly used adapters for increased availability at a lower cost • Allows adapters to be added or removed without interrupting the system
Hot-swappable disk bays	• Provides greater system availability and smoother growth by allowing swapping or adding of disk drives without powering down the system
Built-in service processor	• Continuously monitors system operations and takes preventive or corrective action for quick problem resolution and high system availability • Allows diagnostics and maintenance to be performed remotely
Redundant hot-plug power and cooling subsystems	• Enhances system availability since cooling fans and power supplies can be changed without interrupting operations • Provides backup power and cooling if primary unit fails
Dynamic processor and PCI bus slot deallocation	• Automatically deallocates resources when impending failure is detected, so applications continue to run uninterrupted
IBM @server Cluster 1600	• Provides centralized management of multiple inter-connected systems • Provides ability to handle unexpected workload peaks by sharing resources • Allows for more granular growth so user demands can be readily satisfied
Linux operating system	• Enables access to thousands of 32- and 64-bit Open Source Linux applications • Provides a common operating environment across IBM **@server** platforms
AIX 5L operating system	• Delivers maximum throughput for mixed workloads without complex system configuration or tuning • Provides upward binary compatibility to help preserve software investments • Extends application choices with Linux affinity

pSeries 690 at a glance

Minimum configuration	
Microprocessor	8-way SMP (one 8-way MCM); 1.5 GHz or 1.7GHz POWER4+ or 1.1 GHz or 1.3 GHz POWER4
L3 cache	128MB (ECC)
RAM (memory)	8GB
Internal disk drives	Two 18.2GB Ultra SCSI
Disk bays	16 hot-swappable via one 7140-61D I/O drawer
Media bays	Five (four available)
Expansion slots	20 PCI or PCI-X (64-bit) via one 7140-61D I/O drawer
PCI bus width	32- and 64-bit
HPC minimum configuration	
Microprocessor:	8-way SMP (two 4-way MCMs); 1.3 GHz POWER4 HPC; 256MB of L3 cache
Standard features	
I/O adapters	Two integrated Ultra3 SCSI controllers
Ports	Two serial ports for connecting Hardware Management Console for pSeries
System expansion	
SMP configurations	16-, 24-, 32-way SMP (two, three or four 8-way MCMs); 1.5GHz or 1.7GHz POWER4+ or 1.1 GHz or 1.3 GHz POWER4
L3 cache	128MB per MCM (512MB maximum)
RAM	Up to 512GB (ECC, Chipkill)
PCI expansion slots	Up to 160 adapters via seven additional 7140-61D I/O drawers
Disk bay expansion	Up to 128 hot-swappable disk bays via seven additional 7140-61D I/O drawers; up to 18.7TB (18.2GB, 36.4GB, 73.4GB and 146.8GB disk drives available)
Optional battery backup	Up to two
Attachment	SP System Attachment Adapter for use in a Cluster 1600 configuration
HPC microprocessor expansion	
SMP configurations	16-way SMP (two 4-way MCMs); 1.3 GHz POWER4 HPC; 256MB of L3 cache
RAS features	Copper, SOI microprocessors Chipkill ECC, bit-steering memory ECC L2 cache, L3 cache Service processor Hot-swappable disk bays Hot-plug/blind-swap PCI slots Hot-plug power supplies and cooling fans Dynamic deallocation of logical partitions and PCI bus slots Redundant power supplies and cooling fans Battery backup (optional)
Operating systems	AIX 5L Versions 5.1/5.2 SuSE Linux Enterprise Server Version 8 (runs in LPAR only)
Power requirements	200v to 240v; 380v to 415v; 480v AC
System dimensions	79.7" H x 30.9" W x 58.8" D (202 cm x 79 cm x 149 cm) Weight 2,666 lb (1,209 kg)*
Warranty	On site 24x7 for one year (limited) at no additional cost

* With acoustic door. Weight will vary when disks, adapters and other peripherals are installed.

Grid readiness for highly efficient computing

The pSeries 690 is designed to participate in Grid Computing—an emerging technology that creates virtual computing resources across an intranet or the Internet using industry-standard protocols. By harnessing unused computing cycles, Grid Computing allows organizations to make more efficient use of existing resources, giving them additional computing power while lowering their overall cost of computing.

Keeping businesses running

Several innovations stemming from the IBM autonomic computing initiative—a blueprint for self-managing systems—helps contribute to uncompromising pSeries reliability, manageability and serviceability. Its goal is to create an intelligent IT infrastructure that responds to unexpected capacity demands or to system failures while at the same time helping to control spiraling pressure on critical skills, software and service/support costs.

To boost availability, an integrated service processor in every pSeries 690 server monitors system health. This feature can detect error conditions within the hardware and automatically place a service call to IBM, often before the problem becomes apparent to users. Then, if repairs are necessary, the service processor can initiate dynamic reconfiguration to correct the failure. In this manner, automated monitoring helps businesses minimize costly outages and reduce administrative overhead and support costs.

First Failure Data Capture (FFDC) identifies and logs both the source and root cause of system failures to help prevent the reoccurrence of intermittent failures that diagnostics cannot reproduce. Designed to prevent outages and reduce repair time by identifying failing components in real time, FFDC also contributes to outstanding pSeries system availability.

To help prevent system shutdowns caused by main memory and L2/L3 cache errors, error checking and correcting (ECC) memory detects both single- and double-bit errors and corrects all single-bit errors dynamically—complementing Chipkill memory to improve reliability. In addition, the pSeries 690 includes redundant, spare main memory chips. Through a technique known as bit-steering, these spares can be dynamically activated to replace a failing memory chip in the event that multiple memory bit errors exceed a threshold.

The use of IBM Chipkill technology allows detection and correction of most multi-bit memory errors. This protection from memory failures helps prevent costly system memory crashes and improves pSeries reliability. In fact, IBM studies show that systems with Chipkill memory are up to 100 times less likely to have outages because of memory failure[2].

The pSeries 690 server also features the ability to deallocate critical system resources, including the processors and PCI-X bus slots. In the unlikely event that one of these components fails or indicates an impending failure, this capability—working with AIX 5L and the service processor—can dynamically take the faulty component offline. The system automatically reassigns the workload to other processors to avoid interruption. If the system must be rebooted, previously deallocated components will not be included to avoid

7040-61D IBM I/O Drawer pSeries 690 Model 61D

IBM U.S. Sales Manual
Revised: June 26, 2003.

(12, 13)

Table of contents

Document options

Printable version

IBM U.S. Product Life Cycle Dates

Type Model	Announced	Available	Marketing Withdrawn	Service Discontinued	Replaced By
7040-61D	2001/10/04	2001/12/14	-	-	-

↑ Back to top

Abstract

IBM UNIX systems consist of the IBM eServer pSeries and IBM RS/6000 product lines. Providing unprecedented value, these innovative systems feature IBM's leading-edge technology and run the top-rated UNIX operating system, AIX. This broad product line ranges from powerful workstations ideal for mechanical design; to mission-critical symmetric multiprocessing (SMP) servers for ERP, SCM, CRM, transaction processing, and Web serving; up to parallel RS/6000 SP systems that can handle demanding scientific and technical computing and business intelligence tasks. These platforms provide the power to create change and the flexibility to manage it, with thousands of applications that provide real value. More than 1,000,000 systems have shipped to over 135,000 businesses worldwide.

Model Abstract 7040-61D

The IBM 7040 Model 61D I/O drawer provides PCI or PCI-X adapter slots and internal disk capabilities for use with pSeries servers such as the pSeries 690 (7040-681). The Model 61D is a 4U drawer which mounts in the 24-inch 7040-61R System Rack and connects to the system Central Electronics Complex via remote I/O cables.

Each model 61D I/O drawer provides 20 blind-swap PCI or PCI-X slots and 16 hot-swap disk bays. The Model 61D utilizes redundant power converters and power cabling to ensure high reliability and availability. It utilizes 350V bulk power supplied from the 7040-61R system rack.

↑ Back to top

Highlights

Not applicable.

↑ Back to top

Description

Not applicable.

↑ Back to top

Model

Model Summary Matrix

```
Model   Description
-----   -----------
61D     4U drawer
```

(#3168) RIO-2 (Remote I/O-2) Cable, 2.5M

This 2.5 meter RIO-2 (Remote I/O-2) cable is utilized to connect RIO-2 based I/O planars and I/O drawers to the system CEC.

- Attributes provided: 2.5M RIO-2 Cable
- Attributes required: I/O Drawer and two RIO-2 connectors on the system CEC.
- For 7040-61D: (#3168)
  - Minimum required: 0
  - Maximum allowed: 4 (Initial order maximum: 4)
  - OS level required: None
  - Initial Order/MES/Both/Supported: Both
  - CSU: No
  - Return parts MES: No

(#3275) 146.8 GB 10,000 RPM Ultra3 SCSI Disk Drive Assembly

The 146.8 GB 10,000 RPM Ultra3 SCSI Disk Drive Assembly provides 146.8 GB of storage capacity and supports the industry standard Ultra3 SCSI interface speed of up to 160 MBps.

Characteristics:

- Form Factor: 3.5-inch, 1-inch (25 mm) high
- Cable included: No
- External Interface: Ultra3 SCSI (16-bit, Low Voltage Differential)
- Attachment Industry Spec: SCSI-3 fast 80
- Average Seek Time: 4.94 ms (based on four(4) READS to one(1) WRITE)
- Average Latency: 2.99 ms
- Rotational Speed: 10,000 RPM
- Maximum Data Transfer Rate: 67 MBps

Limitation: This disk drive requires attachment to a supported Ultra3 SCSI Adapter in a system that supports an Ultra3 SCSI cable/backplane in order for the drive to run at 160MBps. Also, any and all other SCSI devices on the same SCSI bus must also be Ultra2 or Ultra3 SCSI device(s) in order for this disk drive to run at 160MBps.

- Attributes provided: 146.8 GB of disk storage mounted in a carrier.
- Attributes required: One disk drive bay.
- For 7040-61D: (#3275)
  - Minimum required: 0
  - Maximum allowed: 16 (Initial order maximum: 16)
  - OS level required: AIX 5.1 or AIX 5.2 or later
  - Initial Order/MES/Both/Supported: Both
  - CSU: No
  - Return parts MES: No

(#3277) 36.4 GB 15,000 RPM Ultra3 SCSI Disk Drive Assembly

The 36.4 GB 15,000 RPM Ultra3 SCSI Disk Drive Assembly provides 36.4 GB of storage capacity and supports the industry standard Ultra3 SCSI interface speed of up to 160 MBps.

Characteristics:

- Form Factor: 3.5-inch, 1-inch (25 mm) high
- Cable included: No
- External Interface: Ultra3 SCSI (16-bit, Low Voltage Differential)
- Attachment Industry Spec: SCSI-3 fast 80
- Average Seek Time: 3.7 ms (based on four(4) READS to one(1) WRITE)
- Average Latency: 2 ms
- Rotational Speed: 15,000 RPM
- Maximum Data Transfer Rate: 83 MBps

Limitation: This disk drive requires attachment to a supported Ultra3 SCSI Adapter in an system that supports an Ultra3 SCSI cable/backplane in order for the drive to run at 160MBps. Also, any and all other SCSI devices on the same SCSI bus must also be Ultra2 or Ultra3 SCSI device(s) in order for this disk drive to run at 160MBps.

- Attributes provided: 36.4 GB of disk storage mounted in a carrier.
- Attributes required: One disk drive bay.
- For 7040-61D: (#3277)
  - Minimum required: 0
  - Maximum allowed: 16 (Initial order maximum: 16)
  - OS level required: AIX 5.1, or later, AIX 5.2 or later
  - Initial Order/MES/Both/Supported: Both
  - CSU: No
  - Return parts MES: No

(#3278) 73.4 GB 15,000 RPM Ultra3 SCSI Disk Drive Assembly

The 73.4 GB 15,000 RPM Ultra3 SCSI Disk Drive Assembly provides 73.4 GB of storage capacity and supports the industry standard Ultra3 SCSI interface speed of up to 160 MBps.

Characteristics:

13U location of the expansion rack.

- Attributes provided: Redundant I/O Drawer Power Cables
- Attributes required: I/O Drawer with Placement Feature #4413
- For 7040-61D: (#6128)
    - Minimum required: 0
    - Maximum allowed: 1 (Initial order maximum: 1)
    - OS level required: None
    - Initial Order/MES/Both/Supported: Both

(#6129) I/O Drawer Attachment Cable Group, Drawer Position #4419

This feature provides redundant power cabling for an I/O drawer with the bottom of the drawer positioned at the 19U location of the expansion rack.

- Attributes provided: Redundant I/O Drawer Power Cables
- Attributes required: I/O Drawer with Placement Feature #4419
- For 7040-61D: (#6129)
    - Minimum required: 0
    - Maximum allowed: 1 (Initial order maximum: 1)
    - OS level required: None
    - Initial Order/MES/Both/Supported: Both

(#6172) Power Converter Assembly, I/O Drawer

This feature converts power from the bulk power assembly to the voltage levels required for the components I/O drawer.

- Attributes provided: I/O Drawer Power Converter
- Attributes required: Empty Power Converter Location
- For 7040-61D: (#6172)
    - Minimum required: 2
    - Maximum allowed: 2 (Initial order maximum: 2)
    - OS level required: None
    - Initial Order/MES/Both/Supported: Initial

(#6179) Power Cable, I/O Drawer to Media Drawer

This cable provides power from an I/O drawer to run media devices mounted in the media drawer feature.

- Attributes provided: Power Cable
- Attributes required: I/O drawer and Media Drawer
- For 7040-61D: (#6179)
    - Minimum required: 0
    - Maximum allowed: 2 (Initial order maximum: 2)
    - OS level required: None
    - Initial Order/MES/Both/Supported: Both

(#6203) PCI Dual Channel Ultra3 SCSI Adapter

The PCI Dual Channel Ultra3 SCSI Adapter (#6203) is a 64-bit adapter and is an excellent solution for high-performance SCSI applications. The PCI Dual Channel Ultra3 SCSI Adapter provides two SCSI channels (buses). Each SCSI bus can either be internal (on systems that support internal SCSI device or backplane attachments) or external and will support a data rate of up to 160 MBytes per second, up to twice the maximum data transfer rate of the previous Dual Channel Ultra2 SCSI adapter (80 MBytes per second).

In order to achieve an Ultra3 SCSI bus data rate of up to 160 MBytes per second and also maintain a reasonable drive distance, the adapter utilizes Low Voltage Differential (LVD) drivers and receivers. To fully utilize this Ultra3 160 MBytes per second performance, all attaching devices or subsystems should also be Ultra3 LVD devices. But, if Ultra2 and Ultra3 devices coexist on the same bus, each device will operate at its rated speed. For lower speed single-ended (SE) devices, the SCSI bus will switch to single-ended (SE) performance and interface at the lower SE bus data rate of the device.

Two industry standard VHDCI 68-pin connectors are mounted on the adapter's end bracket allowing attachment of various LVD and SE external subsystems. A .3 meter converter cable, VHDCI to P, Mini-68 pin to 68-pin, (#2118) can be used with older external SE subsystems to allow connection to the VHDCI connector on the PCI Dual Channel Ultra3 SCSI Adapter.

Note: If any Single Ended (SE) SCSI subsystem is attached to an external port of this adapter, the SCSI port will auto-throttle to a "Fast" interface speed running no faster than 20MB/s maximum. This auto- throttle function is performed to ensure best signal quality between host adapter and attaching subsystem. The second external port is unaffected unless a SE subsystem is also attached to it. If so, it would also auto- throttle as described above.

The PCI Dual Channel Ultra3 SCSI Adapter (#6203) also is a native boot adapter with AIX 4.3.3 or AIX 5.1 (with appropriate updates) in the supported pSeries or RS/6000 systems.

- Attributes provided: Attachment of internal SCSI devices (on systems that support an internal SCSI device or backplane attachment with this adapter) and external SCSI devices
- Attributes required: One available PCI slot

The above link contains links to SSA publications and other SSA Web sites, including the one below.

http://www.storage.ibm.com/hardsoft/products/ssa/rs6k/index.html

The above link contains lists of the latest SSA support code and provides code download capability for the RS/6000 and AIX environments.
LIMITATION: Internal ports on the adapter are not supported. See machine/model specific information to determine if internal SSA disk drives and associated hardware/cables are supported.

- Attributes provided: Attachment of SSA devices
- Attributes required: One PCI bus slot
- For 7040-61D: (#6230)
  - Minimum required: 0
  - Maximum allowed: 12 (Initial order maximum: 12)
  - OS level required: AIX 5.1 or later
  - Initial Order/MES/Both/Supported: Both

Note: Maximum of 6 adapters per #6563 PCI planar.

(#6231) 128 MByte DRAM Option Card

The 128 MByte DRAM Option Card (#6231) is a field only optional feature to the Advanced SerialRAID Adapter (#6225) or a factory or field option for the Advanced SerialRAID Plus Adapter (#6230). This option is recommended for dual initiator fail-over Fast Write Cache (FWC) configurations. The option increases the existing DRAM on the adapter to 128 MBytes. In this type of dual initiator FWC configuration, the existing DRAM does not have enough capacity to completely contain a copy of each adapter's 32 MByte FWC and also provide a[redacted]al working space. The 128 MByte DRAM Option Card provides this additional space needed to contain a fu[redacted] of each adapters 32 MByte FWC content and allows for full 32 MByte fail-over protection. If the 128 MByte DRAM Option Card (#6231) is not used with dual-initiator FWC configurations, the effective FWC capacity is reduced to 16 MBytes per adapter.
If this feature is ordered as a field upgrade to an existing SerialRAID adapter (#6225 or 6230), a CD-ROM with appropriate software and publications are also provided.

- Attributes provided: 128 MByte DRAM memory
- Attributes required: Advanced SerialRAID Adapter (#6225) or Advanced SerialRAID Plus Adapter (#6230). A 32 MByte Fast-Write Cache Option Card (#6235) is also recommended.
- For 7040-61D: (#6231)
  - Minimum required: 0
  - Maximum allowed: 12 (Initial order maximum: 12)
  - OS level required: AIX 5.1 or later
  - Initial Order/MES/Both/Supported: Both

(#6235) 32 MByte Fast-Write Cache Option Card

The 32 MByte Fast-Write Cache Option Card (#6235) is a 32 MByte fast- write optional feature that plugs into the IBM RS/6000 Advanced SerialRAID Adapter (#6225) or the Advanced SerialRAID Adapter Plus (#6230). It utilizes non-volatile RAM. During the unlikely event of an Advanced SerialRAID Adapter failure, a replacement Advanced SerialRAID Adapter can be installed and the fast-write cache can be removed from the failing adapter and installed in the new adapter insuring data integrity. The 32 MByte Fast-Write Cache Option Card can provide a [redacted]ificant improvement of data throughput and response time during certain sequence write operations co[redacted]d to SSA RAID adapters without the fast-write cache. The response time and data transfer improvement using the optional card will vary depending upon the data block sizes, the percentage of sequential writes, machine type/model, and application parameters. The 32 MByte Fast-Write Cache Option Card plugged into the Advanced SerialRAID Adapter (# 6225) will operate in either non-RAID or RAID 5 mode, in single-initiator configurations. The 32 MByte Fast-Write Cache Option Card plugged into the Advanced SerialRAID Plus Adapter (# 6230) will operate in non-RAID, RAID 5, or RAID 0+1 mode, in single-or dual-initiator configurations.

- Attributes provided: None
- Attributes required: One Advanced SerialRAID Adapter (#6225) or Advanced SerialRAID Plus Adapter (#6230).
- For 7040-61D: (#6235)
  - Minimum required: 0
  - Maximum allowed: 12 (Initial order maximum: 12)
  - OS level required: AIX 5.1 or later
  - Initial Order/MES/Both/Supported: Both

(#6239) 2 Gigabit Fibre Channel PCI-X Adapter

The 2 Gigabit Fibre Channel PCI-X Adapter is a 64-bit address/data, short form factor PCI-X adapter with an LC type external fiber connector that provides single or dual initiator capability over an optical fiber link or loop. With the use of appropriate optical fiber cabling, this adapter provides the capability for a network of high speed local and remote located storage. The 2 Gigabit Fibre Channel PCI-X Adapter will auto-negotiate for the highest data rate (either 1 Gbps or 2 Gbps) of which the device or switch is capable. Distances of up to 500 meters running at 1 Gbps data rate and up to 300 meters running at 2 Gbps data rate are supported between the adapter and an

(6, 14)

10/100/1000 Base-TX Ethernet PCI-X Adapter and
Dual Port 10/100/1000 Base-TX PCI-X Adapter

Installation and Using Guide

SA23-1301-01

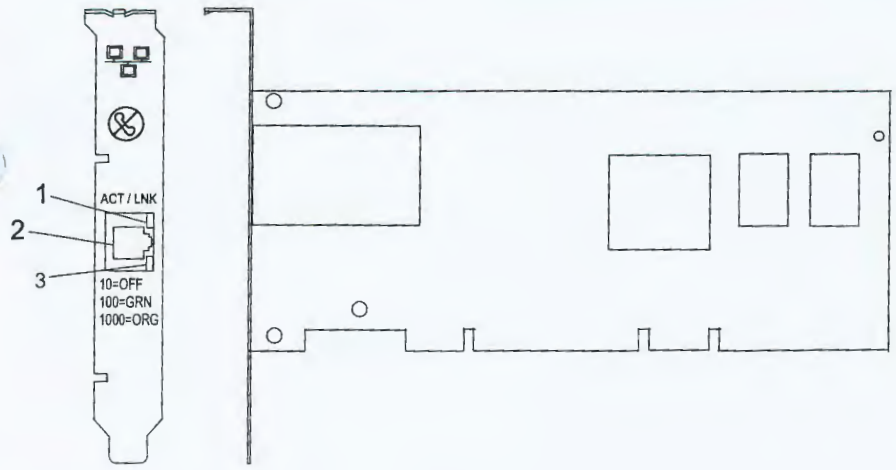
Chapter 1. Overview

The 10/100/1000 Base-TX Ethernet PCI-X Adapter and Dual Port 10/100/1000 Base-TX PCI-X Adapter are high performance, highly integrated, universal Ethernet LAN adapters for PCI-X and PCI systems. The adapters provide 10/100/1000 Mbps connectivity over 4 pairs of standard CAT-5 cable up to 100 meters. Both conform to IEEE 802.3ab 1000 Base-T standard. The adapters run in standard PCI-X V1.0a compliant systems with 32-bit or 64-bit PCI-X Bus Master slots at 66 MHz or 133 MHz, as well as PCI 2.2 compliant systems with 32-bit or 64-bit PCI bus master slots at 33 MHz or 66 MHz.

Both adapters provide the following features:

- Support for 64-bit Direct Bus Mastering on the PCI/PCI-X bus
- Use a shared memory structure in host memory and copy data directly from and to host memory
- Support Boot ROM
- Operate in 10/100/1000 Base-T modes
- Support 1000 Mbps throughput on 4 pairs of standard CAT-5 cabling
- Support 100 Mbs and 10 Mbps throughput on 2 pairs of standard CAT-5 and CAT-3 cabling
- Full-duplex operation
- IEEE 802.3ab 1000 Base-T compliant
- IEEE 802.3u 100 Base-TX compliant
- IEEE 802.3 10 Base-T compliant
- Support Dual address cycle for access to 64-bit addresses
- Support 64-bit addressing for systems with physical memory greater than 4 GB
- Support PCI-X split transactions
- Two bicolor LED adapter status indicators for link activity and baud rate. See the following illustrations.
- RJ-45 UTP Connector for Category-5 Copper Cabling
- Surface mount technology (SMT)

10/100/1000 Base-TX Ethernet PCI-X Adapter



1 ACT/LNK LED

2 RJ-45 Connector

3 Link Speed LED

(7, 15)

IBM AIX 5L Operating System

Summary

AIX 5L is IBM's 64-bit Unix operating system for enterprise computing. AIX has a wide range of availability, connectivity, Linux compatibility, scalability and security features.

Table of Contents

List Of Tables

Mobile IPv6, Simple Network Management Protocol (SNMP) v.3 and an upgrade to Berkeley Internet Name Domain (BIND) v.9. (CSM support for pSeries Linux is not yet available; at this time, CSM support is for Red Hat Linux on Intel. CSM does support heterogeneous management of AIX and Intel Linux systems.)

Dynamic Capacity Upgrade on Demand enables POWER4 systems to be ordered and installed with additional processors that can be held in reserve until required by future application workloads. To enable the additional resources, the system administrator can dynamically turn on the resources using dynamic logical partition (DLPAR) services without having to bring down the system. Dynamic CPU Guard automatically and dynamically removes failing processors from a system image before they cause a system failure. If reserve processors are available on the system, they can automatically replace the failing processors.

Table 1: Features and Functions: IBM AIX 5L Version 5.2

Overview	• AIX 5L is the current version of IBM's 64-bit Unix operating system. • It is used on IBM POWER processors and provides compatibility with Linux. • It runs on a broad range of IBM eServer pSeries systems, including workstations, workgroup servers and enterprise servers.
Standards Compliance	• X/Open Portability Guide release 4 (XPG4) and XPG5. • Posix Institute of Electrical and Electronics Engineers (IEEE) 1003.1-1996 (1003.1c), 1003.2, 1003.4a. • LP64 (32-bit integers, 64-bit long and pointer types) System V Interface Definition 3 (SVID3). • Berkeley Software Distribution (BSD) 4.3. • Open Software Foundation (OSF) Advanced Encryption Standard (AES) • Federal Information Processing Standard (FIPS) 151-2. • 32-bit operating system is Unix 98 branded. • 64-bit operating system is in the process of obtaining Unix 98 branding. • AIX 5L v.5.2 is designed to conform to the International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 9899:1999 international standard for the C programming language, commonly referred to as C99. • AIX 5L v.5.2 is designed to provide the asynchronous input and output option from IEEE Standard 1003.1-2001. • AIX 5L v.5.2 supports the Universal Disk Format (UDF) v.1.50 file system for the pSeries and RS/6000-supported DVD-RAM and DVD-ROM optical drives. • AIX 5L v.5.2 supports the Common host bus adapter (HBA) API (application program interface) specification revision 1.92, developed through the Storage Networking Industry Association (SNIA) and provides a standard and consistent interface for accessing information Fibre Channel storage area networks (SANs). The Common HBA API includes a set of C programming language library functions, enabling access to Fibre Channel HBA attributes and operating system mapping information.

040-681 IBM pSeries 690 Central Electronics Complex Model 681

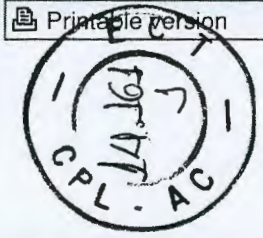
BM U.S. Sales Manual
evised: July 11, 2003.

(11, 16)

Table of contents

Document options

Printable version



M U.S. Product Life Cycle Dates

Type Model	Announced	Available	Marketing Withdrawn	Service Discontinued	Replaced By
-681	2001/10/04	2001/12/14	-	-	-

Back to top

stract

M UNIX systems consist of the IBM eServer pSeries and IBM RS/6000 product lines. Providing unprecedented ue, these innovative systems feature IBM's leading-edge technology and run the top-rated UNIX operating stem, AIX. This broad product line ranges from powerful workstations ideal for mechanical design; to mission-ical symmetric multiprocessing (SMP) servers for ERP, SCM, CRM, transaction processing, and Web serving; to parallel RS/6000 SP systems that can handle demanding scientific and technical computing and business elligence tasks. These platforms provide the power to create change and the flexibility to manage it, with usands of applications that provide real value. More than 1,000,000 systems have shipped to over 135,000 sinesses worldwide.

del Abstract 7040-681

e IBM 7040 Model 681 Central Electronics Complex pSeries 690 provides outstanding 64-bit compute formance for the UNIX environment. It features SOI (silicon on insulator) copper chip technology, mainframe pired logical partitioning (LPAR) and self-managing capabilities.

Back to top

del Highlights 7040-681

Innovative Technology -- A top performing UNIX server featuring

- IBM SOI/copper chip technology
- Mainframe-inspired LPAR and self-managing capabilities
- Cost-efficient growth path to the future
  - 64-bit system scalability:
    - 8-way, 16-way, 24-way, or 32-way -- packaged on four Multi-Chip Modules (four or eight POWER4 or POWER4+ processors per MCM)
    - 1.1 GHz or 1.3 GHz POWER4 processors
    - 1.5 GHz or 1.7 GHz POWER4+ processors
    - 128 MB of L3 ECC cache per MCM
  - DDR System memory expandable from 8 GB to 512 GB

service action requests are forwarded from the operating system partitions to a Service Focal Point (SFP) application running on the Hardware Management Console (HMC). The service focal point application analyzes the potentially duplicate reported failures from the various logical partitions, attempts to determine the root cause of the fault, and upon identifying the cause, initiates call-home requests to IBM support utilizing the HMC modem and the Service Agent application program. This enables IBM service representatives to have available needed replacement hardware components when a service call is placed, thus minimizing system repair time.

Availability -- Backup and Replication

Power and Cooling Subsystem

The pSeries 690 brings new a level of availability features and functions to the Enterprise Server. Within the CEC Rack, the N+1 power and cooling subsystem can provide complete redundancy in case of failures in the bulk or regulated power supplies, the power controllers and the cooling units. Concurrent repair is supported on all of the power and cooling components.

The p690 also features redundant Internal Battery Features (IBF) to hold the system up during brown-out conditions. For full power loss protection, the p690 supports optional uninterruptible power supply (UPS) systems in addition to, or in place of, the IBF features.

In the I/O drawers, N+1 power and cooling is provided with the capability for concurrent repair of the power components and deferred repair of the cooling units.

Constant power monitoring hardware assists in detection of early loss of source power, and is designed to notify the operating system to effect an orderly shutdown. This same power monitoring hardware can detect the loss of redundant bulk power supplies, regulators, fans, and blowers and report them to the operating system for entry in the system error log and for maintenance notification.

CEC Subsystem

RAS features such as ECC on the L1 data cache and L2 data and directory caches can provide dynamic detection and correction of hard or soft array cell failures. Dynamic de-allocation functions include:

- L3 cache line detect and L2 cache de-allocation
- Individual L3 cache memory bypass
- L2 cache and CPU de-allocation
- Redundant bit steering in L1 and L2 caches and L2 and L3 directory arrays

Building on the robust features of the processor complex, the p690 system has enhanced error detection and prevention capabilities. These processor RAS features are called Dynamic Processor De-allocation and Persistent Processor De-allocation. Predictive failure analysis is performed on recoverable processor errors during run-time. If a processor exceeds a threshold of recoverable errors such as on L2 cache accesses, the system is designed to log the event marked and deconfigure the processor from the system while the operating system continues to run. This feature allows the processor to be repaired on a deferred basis while helping prevent an unscheduled system outage.

Persistent Processor De-allocation is designed to ensure that on subsequent reboots, the processor remains out of the system configuration until replaced. The standard memory card has single error-correct and double-error detect ECC circuitry to correct single-bit memory failures. The double-bit detection helps maintain data integrity by detecting and reporting multiple errors beyond what the ECC circuitry can correct. The memory chips are organized such that the failure of any specific memory module should only affect a single bit within an ECC word (bit scattering), thus allowing for error correction and continued operation in the presence of a complete chip failure (Chipkill recovery).

This memory card also utilizes memory scrubbing and thresholding to determine when spare memory modules within each bank of memory should be used to replace ones that have exceeded their threshold value (dynamic bit steering). Memory scrubbing is the process of reading the contents of memory during idle time and checking and correcting any single-bit errors that have accumulated. These single-bit failures could be either solid (chnology failures) or soft failures (intermittent errors caused by noise or other cosmic effects). If an error is detected, the system is designed to correct it by passing the data through the ECC logic that corrects the fault and writing the corrected contents back to its memory address location.

To prevent an uncorrectable memory error from causing a system outage, the service processor is designed to initiate a deferred maintenance request on memory cards that have used their spare bits and are experiencing additional correctable errors (memory predictive failure analysis).

DASD predictive failure analysis is designed to detect an imminent disk failure and report the findings through the AIX log. Then the disk can be replaced either immediately or scheduled at a later time, depending on the configuration of the DASD subsystem. With the hot-plug disk design, normal operation can continue in the absence of a failed disk and a concurrent repair can be performed while the application continues uninterrupted.

Availability - UE Error Handling

Some events in the processor, cache, and memory subsystems sometimes cause errors that exceed the error correction capability, and become Uncorrectable Errors (Ues). In other systems, these result in immediate checkstop with the offending component fully identified by the run time diagnostics. In the p690 system, is designed not to cause a checkstop of the system. Instead, the corrupted data is specially marked until used by a processor, at which time a new synchronous machine check interrupt allows AIX to localize the effect to a single LPAR partition or a software process. This provides the capability of localizing a global system resource to affecting only the partition utilizing the resource instead of checkstopping all system partitions. The affected partition can then be rebooted with significantly reduced boot time as compared to a full system reboot.

RIO Subsystem

The interface from the processor to the I/O is through the Remote I/O (RIO) link. This link uses a loop interconnect technology to provide redundant paths to I/O drawers. There is a maximum of 1 I/O drawer on each loop path, with a total of 8 I/O drawers per system. RIO availability features include CRC checking on the RIO interface with packet retry on bus timeouts. In addition, if a RIO link fails, the hardware is designed to automatically initiate a RIO bus reassignment to route the data through the alternate path to its intended destination.

Availability - PCI Bus Error Recovery

- 8.0 bels (operating/idling with slim line covers)

- Sound Pressure:
  - 58 dBa (operating/idling with acoustic covers)
  - 66 dBa (operating/idling with slim line covers)

- Maximum Altitude:
  - 1.1, 1.5, and 1.7GHz Processors: 3,040 meters (10,000 ft)
  - 1.3GHz Processors: 2,134 meters (7,000 ft)
  - Maximum altitude with DVD-R, DVD-R/W/CD-R, or CD-R/W media in the rear positions of the Media Drawer (#8692) is 2134 meters (7,000 ft).

ower Requirements

- Operating voltage @ 50/60 Hz: (3-phase)
  - 200 to 240 V AC
  - 380 to 415 V AC
  - 480 V AC

- Electrical output: 15,400 watts (maximum)

- Power source loading: 15.0 kVA (maximum configuration)

- Thermal Output: 15,550 joules/sec (53,390 Btu/hr) (maximum configuration, 32-way CEC with eight I/O drawers)

nformance Classification

his equipment is subject to FCC rules and it shall comply with the appropriate FCC rules before final delivery to ıe buyer or centers of distribution.

- U.S. - FCC CFR47 Part 15 Class A
- Europe - CISPR 22 Class A; "CE" Mark of Conformity
- Japan - VCCI-1
- Korea - Korean Requirement Class A

omologation: Telecom Environmental Testing (Safety and EMC)

omologation approval for specific countries has been initiated with the IBM Homologation and Type Approval IT&A) organization in LaGaude.

ıis IBM pSeries model and applicable features meet the environmental testing requirements of the country ELECOM and have been designed and tested in compliance with the Full Quality Assurance Approval (FQAA) ocess as delivered by the British Approval Board for Telecom (BABT), the U.K. Telecom Regulatory authority.

roduct Safety/Country Testing/Certification

- U.S.: UL
- Canada: CNL (CSA or cUL)
- Germany/Europe: GS Mark (Safety, TUV, EN60 950)

eneral Requirements

ıe pSeries 690 is in compliance with IBM Corporate Bulletin C-B 0-2594-000 Statement of Conformity of IBM oduct to External Standard (Suppliers Declaration).

ns

eries 690 Central Electronics Complex (CEC) (7040-681)

- The pSeries 690 CEC (7040-681) is a 17U-tall, 24-inch, rack-mounted device. It houses the system processors, memory, system support processor, I/O drawer connection capability, and associated components. It is installed with the bottom of the drawer at placement indicator (#4418), the 18U position of the 7040-61R rack.

- The p690 is powered by one to four multi-chip processor modules. Each Multi-Chip Module (MCM) contains either four or eight processors. The p690 is available in the following configurations:
  - 8-and 16-way 1.3 GHz, POWER4, HPC option processors (4 processors per MCM)
  - 8-, 16-, 24-, 32-way 1.1 GHz, POWER4 processors (8 processors per MCM)
  - 8-, 16-, 24-, 32-way 1.3 GHz, POWER4, Turbo option processors (8 processors per MCM)
  - 8-, 16-, 24-, 32-way 1.5 GHz, POWER4+ processors (8 processors per MCM)
  - 8-, 16-, 24-, 32-way 1.7 GHz, POWER4+ Turbo option processors (8 processors per MCM)

- All processors in a p690 must operate at the same speed.

- Supports all major CD-ROM formats including Mode 1, Mode 2, XA, CDDA and audio
- Contains headphone output and line output for audio

Limitations:

- DVD video is not supported.
- Attributes provided: 4.7GB 2X DVD (2705 KB/Sec) DVD-RAM
- Attributes required: 1 half high media bay and one SCSI address
- For 7040-681: (#2623)
    - Minimum required: 0
    - Maximum allowed: 4 (Initial order maximum: 4)
    - OS level required: AIX 5.1 or later
    - Initial Order/MES/Both/Supported: Both

Note: One device capable of reading CD media is required per 7040-681. This DVD RAM may be mounted in the rear bays of the #8962 media drawer only if the operating environment is maintained at 24 degrees C (75.2 degrees F) or below. This device is allowed in the rear bays of the #8692 media drawer on systems installed at 2134 meters (7,000 ft) or below.

(#2624) 32X (Max) SCSI-2 CD-ROM Drive

The 32X (Max) SCSI-2 Internal CD-ROM Drive is a tray loading CD-ROM drive providing up to 4800KB/sec maximum media data transfer rate. It is a 5.25 inch half-high form factor, single ended, 8 bit, multi-session capable, CD-ROM drive which provides state of the art performance and supports existing 600MB CD-ROM discs.

Characteristics:

- Media Data Transfer Rate: 4800 KB/sec (Max)
- Interface: SCSI-2 8 bit Single Ended (SE)
- Avg. Random Access Time: 90ms (typical)
- Buffer Memory: 512KB
- Media capacity: Greater than 600MB
- Multisession capable (Reads CDR & CDRW media)
- 5.25-inch half-high form factor
- Operates in either vertical or horizontal positions
- Interface supports standard and extended XA formats
- Loading tray supports 12cm and 8cm disks
- Attributes provided: 600MB 32X (max)(up to 4800KB/sec) CDROM
- Attributes required: 1 half high media bay and 1 SCSI-2 internal SE 8-bit address
- For 7040-681: (#2624)
    - Minimum required: 0
    - Maximum allowed: 4 (Initial order maximum: 4)
    - OS level required: AIX 5.1 or later.
    - Initial Order/MES/Both/Supported: Both

Note: One device capable of reading CD media is required per 7040-681.

(#2634) 16X/48X(max) IDE DVD-ROM Drive

The 16X/48X(max) IDE DVD-ROM Drive is an internal tray loading DVD-ROM drive providing up to 7200KB/sec (CD-ROM) and 22.16MB/sec (DVD-ROM) data transfer rates. It is a 5.25 inch half-high form factor multi-session capable, DVD-ROM drive which provides state of the art performance and supports existing 650MB CD-ROM, 4.7 GB DVD-ROM, and 9.4 GB DVD-ROM (double-sided) discs. This drive also reads Type II (removable from cartridge) DVD-RAM discs at DVD-ROM speeds. System boot and install functions are supported with CD-ROM and DVD-RAM media.

Characteristics:

- Media Data Transfer Rate: CD-ROM=7200 KB/sec (max): DVD-ROM=22.16MB/sec (max)
- Interface: IDE/ATAPI
- Avg. Random Access Time: CD-ROM=90ms(typical); DVD-ROM=135ms(typical)
- Buffer Memory: 256KB
- Media capacity: CD-ROM=650MB; DVD-ROM= 4.7 GB(single sided); 9.4 GB(double-sided)
- Multisession capable (Reads CD/R & CD-R/W media)
- 5.25-inch half-high form factor
- Operates in either vertical or horizontal positions
- Interface supports standard and extended XA formats
- Loading tray supports 12cm and 8cm disks

Limitations:

- DVD video is not supported.
- This DVD-ROM drive is limited to reading only CD-type formatted media when running with AIX 5.1 software.
- Attributes provided: 16X/48X(max) IDE DVD-ROM Drive
- Attributes required: 1 half-high media bay

  The 16X/48X(max) IDE DVD-ROM Drive (#2634) requires a SCSI-to-IDE Interface Bridge (#4253) when installed in this system.

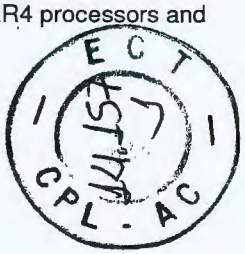
  The (#2634) 16X/48X(max) IDE DVD-ROM Drive is allowed in the rear bays of the media drawer only if it

- Initial Order/MES/Both/Supported: Both

(#5254) 8-Way POWER4 Turbo Processor Option

This Turbo Option feature is a multi-chip module (MCM) which provides eight 1.3GHz POWER4 processors and incorporates 5.6MB of shared Level 2 cache.

- Attributes provided: 8-Way POWER4 1.3GHz MCM
- Attributes required: Empty 2nd, 3rd, or 4th processor position
- For 7040-681: (#5254)
  - Minimum required: 0
  - Maximum allowed: 3 (Initial order maximum: 3)
  - OS level required: AIX 5.1 or later
  - Initial Order/MES/Both/Supported: Both



(#5257) Processor Bus Pass Through Module

The Processor Bus Pass Through Module provides processor bus interconnection through processor positions which do not contain processor modules.

- Attributes provided: Processor bus interconnection
- Attributes required: Empty Processor Module position
- For 7040-681: (#5257)
  - Minimum required: 0
  - Maximum allowed: 2 (Initial order maximum: 2)
  - OS level required: AIX 5.1 or later
  - Initial Order/MES/Both/Supported: Both

Note: One #5257 Processor Bus Pass Through Module must be installed in each empty processor position on 7040-681 systems equipped with two or more processor modules. Processor Bus Pass Through Modules are not required on systems equipped with only one processor module.

(#6120) IBM 80/160 GB Internal Tape Drive with VXA Technology

The IBM 80/160 GB Internal Tape Drive with VXA** Technology is a 5.25-inch, half-high, Ultra2 LVD 16-bit tape drive, which provides a high capacity for save/restore and achieve functions. This tape drive uses VXAtape** data cartridges and is compression capable, providing a capacity of up to 160 GB - a significant increase in capacity over the previous internal tape drives.

Characteristics:

- Capacity: 80 GB native mode, 160 GB (typical) compression mode
- Form Factor: 5.25-inch half high
- Media: uses VXAtape data cartridges
- Technology: Helical scan, rotating head
- Operation: Streaming
- Data Transfer Rate: 6MBps native mode, 12MBps (typical) compression
- Interface: SCSI-2 (LVD/SE) asynchronous/synchronous
- Compatability: 80 GB mode (Read/Write), 160 GB compression (Read/Write)
- Attributes provided: One 80/160 GB internal tape drive
- Attributes required: One 1.6-inch (41mm) half-high media bay and one SCSI-2 internal 16-bit address

The IBM 80/160 GB Internal Tape Drive with VXA Technology (#6120) is limited to systems without Primary Integrated Battery Backup (#6200) or Redundant Integrated Battery Backup (#6201) installed, Media Drawer (#8692) front bay locations only, and a maximum system ambient operating temperature of 28 C (82.4 F) at a maximum operating altitude of 2134 m (7000 ft). Lower altitudes have higher maximum ambient operating temperatures. Refer to the 7040 System Planning Guide for additional details.

- For 7040-681: (#6120)
  - Minimum required: 0
  - Maximum allowed: 1 (Initial order maximum: 1)
  - OS level required: AIX 5.1 or later, AIX 5.2 or later
  - Initial Order/MES/Both/Supported: Both
  - CSU: No
  - Return parts MES: No

(#6158) 20/40GB 4mm Internal Tape Drive

The 20/40 GB 4-mm Internal Tape Drive is a 5.25-inch, half-high, single-ended 16-bit tape drive, which provides a high capacity for save/restore and achieve functions. This tape drive uses IBM 4-mm data cartridges and is compression capable, providing a capacity of up to 40 GB - a significant increase in capacity over the previous 12/24 4-mm internal tape drives (when using DDS-4 media).

Characteristics:

- Capacity: 20 GB native mode, 40 GB (typical) compression mode
- Form Factor: 5.25-inch half high
- Media: IBM 4-mm DDS-4 data cartridge

5765-E62 IBM AIX 5L for POWER V5.2

IBM U.S. Sales Manual
Revised: June 24, 2003.

Table of contents

Document options

Printable version

IBM U.S. Product Life Cycle Date

Program Number	VRM	Announced	Available	Marketing Withdrawn	Service Discontinued	Replaced By
5765-E62	5.02.0	2002/10/08	2002/10/18	-	2007/07/31	-

↑ Back to top

Abstrac

AIX 5L represents the next generation of AIX. Built on a proven code base, AIX 5L is designed to exploit advanced 64-bit system and software architectures while introducing:

- Logical partitioning
- Improved workload management
- Integrated Linux affinity
- Network performance improvement
- System security enhancements
- Reliability, availability, and serviceability (RAS) enhancements and performance-tuning tools
- Cluster Systems Management

AIX 5L V5.2 moves the operating system into the next stage of IT infrastructure self-management with innovative scalability technology while continuing to offer application flexibility with Linux, tools that simplify systems management, leadership security mapping between heterogeneous platforms, and affinity with pSeries focus market segments. The addition of dynamic logical partitioning and keyed Capacity Upgrade on Demand significantly improves flexibility, workload management, and system resource use in the datacenter.

AIX 5L V5.2 reliability and scalability, combined with application binary compatibility across all AIX V5 releases and concurrent 32/64-bit functionality, make it the best choice for customers who:

- Require a robust platform for business-critical applications
- Want to leverage their IT investments in technology and skills
- Have network interoperability requirements with heterogeneous systems
- Need components and tools to build tailored solutions
- Want to reduce the cost of computing through improved systems and network management
- Need security at all levels of their operating, application and network environments
- Deploy applications worldwide requiring multilingual support

↑ Back to top

Highlight:

AIX 5L V5.2 offers:

- Dynamic logical partitioning for processors, memory, and I/O
- Dynamic Capacity Upgrade on Demand
- Enhancements to Scalability and Workload Manager
- Enhancements to Enterprise Storage Management
- Cluster Systems Management for monitoring and administering multiple machines (both AIX and Linux) from a single point of control
- Advanced RAS features
- Additional security features and enhancements
- Network enhancements including Mobile IPv6, SNMP V3, and upgrade to BIND V9
- APIs from the latest C language and single UNIX specification standards

↑ Back to top

Descriptio

Scalability and Resource Management

- Dynamic logical partitioning adds and removes processors, real memory, and I/O from active logical partitions without rebooting the systems. Processors, memory, and I/O slots can be assigned via the Hardware Management Console.
- Dynamic Capacity Upgrade on Demand enables you to order and install POWER4 systems with additional hardware resources (processors) than what is currently required and keep these resources in reserve until they are required as future business application workloads dictate. To enable the additional resources, the system administrator can dynamically turn on the resources using DLPAR services without having to bring down the system. This function is well suited for those who have unpredictable application workload requirements.
- Dynamic CPU Guard automatically and dynamically removes failing processors from a system image before they cause a system failure. If spare processors are available on the systems, they can automatically replace the failing processors.
- Memory affinity support may improve the performance of memory-access- intensive, high-performance computing jobs running on multichip module p690 and p670 systems.
- The POWER4 processor in the p690 system supports 4 KB and 16 MB virtual page sizes.
  The large page provides performance improvements to high-performance computing applications. AIX V5.2 supports large page use for both 32-and 64-bit applications and on both 32-bit and 64-bit kernels.
- Enhanced Workload Manager (WLM) gives system administrators more control of resources. Functions such as time-based setting make changes to configuration easier. A set of processors may be associated with a WLM class. Jobs assigned to such a WLM class run only on the processors associated with the WLM class.
- The existing per-process file descriptor limit is increased from 32K to 64K under both 32-bit and 64-bit kernels.
- Enhanced journaled file system, JFS2, increases file and file system sizes to 16 terabytes (TB) with the 64-bit kernel. The 32-bit kernel continues to support 1 TB. Larger file systems created under the 64-bit kernel can be mounted only with the 64-bit kernel.

- AIX V5.2 includes support for the Universal Disk Format (UDF) V1.50 file system for the pSeries and RS/6000-supported DVD-RAM and DVD-ROM optical drives.
  With the UDF file system you can back up and restore AIX files and backup images. You can also start the system and install from disks created using the mkcd command with DVD-RAM media. Software vendors and other users can create DVD distribution media for programs and data. AIX creates and supports file names only in 8-bit OSTA compressed UNICODE format.

Reliability, Availability, and Serviceability

- With the improved system dump estimation mechanism, system administrators have a more accurate measure of the storage required for a complete system dump. As a result, the probability of losing a crash dump due to space overflow is reduced.

- Core dumps are generated without stopping and restarting applications. The core dumps can be sent to IBM support for further analysis. This function, combined with the snapshot backup, yields easier problem determination.

- Hang conditions on I/O devices can be detected and recovered without bringing systems to a slow halt. Based on a user-defined timeout threshold, lost I/O is detected and the system alerts the user. Users can also configure the system for an automatic reboot.

- More information is displayed on the second line of LED display panel, if one is available. The extra information corresponds to the LED code that is displayed and helps system operators monitor the boot process.

- Automated dump analysis tool, adump, is enhanced to execute custom Perl scripts for dump analysis.

- AIX V5.2 isolates the damage caused by uncorrectable data corruptions to a user process. This can help avoid more severe situations such as an entire partition reboot or a complete system reboot if it is not partitioned.

Enterprise Storage Management

- An industry-standard programming interface, Common Host Bus Adapter (HBA) API, accesses management information in Fibre Channel HBAs. Storage area network (SAN) developers can use HBA to manage, monitor, and deploy a SAN.

- Logical Volume Manager (LVM) enhancements:
  - The alignment and size restrictions of I/O to the LVM device driver are removed, helping to improve large unaligned I/O performance by not requiring that the I/O devices be divided into several smaller aligned I/O devices.
  - LVM enables a RAID to increase the size of a logical unit number (LUN) up to 1 TB. After a varyoffvg and varyonvg cycle completes, the new disk size becomes effective and LVM can use the additional disk space.
  - LVM supports splitting one or more disks from an active mirrored volume group into a new temporary volume group so that a backup of the volume group can be made. The temporary volume can be disbanded and the split disk reincorporated into the original volume group. Stale partitions are automatically synchronized. Only partitions that are written to while the temporary volume group is in place need to be marked as stale and synchronized when the disks are reincorporated.

- A snapshot feature enables a point-in-time backup of a JFS2 file system.

- System administrators can use SMIT to specify file system sizes in blocks of 512 bytes, 1 MB, or 1 GB during creation or modification of a file system.

Cluster Systems Management (CSM)

- CSM for AIX can manage multiple machines from one single point of control. This solution for distributed systems management allows a system administrator to install and set up a cluster that can include pSeries servers, xSeries servers, or both. The system administrator can control the cluster by using remote parallel command execution, file synchronization, hardware control, and distributed monitoring with automated responses.

- CSM for AIX enables xSeries servers running CSM V1.3 for Linux to join the cluster and be managed along with pSeries servers from the same single point of control.

MANUAL 18 (2.1 – 2.8)

Cáculo para Comprovação de Performance (Equipamentos RISC)

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

SPECjbb2000 solicitado = 260.000
SPECjbb2000 expansível = 330.000

Equipamento auditado: IBM eServer pSeries 690 modelo 681 POWER4+ Turbo (1.7 GHz)

SPECjbb2000 auditado: 553.480
Nr. de CPU auditadas: 32
Nr. de CPU ofertadas: 16

Cálculo (ANEXO 1-B, item 2, subitem 2.1):

SPECjbb2000 estimado = SPECjbb2000 auditado * (no de CPU ofertadas / no CPU auditadas)
SPECjbb2000 estimado = 553.480 * (16 / 32)
SPECjbb2000 estimado = 553.480 * 0.5
SPECjbb2000 estimado = 276.740

AIX 5L Version 5.2

System User's Guide: Operating System and Devices

The basic type of file system is called the *Journaled File System (JFS)*. This file system uses database journaling techniques to maintain its structural consistency. This prevents damage to the file system when the system is halted abnormally.

Some of the most important system management tasks have to do with file systems, specifically:

- Allocating space for file systems on logical volumes
- Creating file systems
- Making file system space available to system users
- Monitoring file system space usage
- Backing up file systems to guard against data loss if the system fails
- Maintaining file systems in a consistent state

These tasks should be performed by your system administrator.

File System Types

The operating system supports multiple file system types. These include:

Journaled File System (JFS)	The basic file system type, it supports the entire set of file system commands.
Enhanced Journaled File System (JFS2)	The basic file system type, it supports the entire set of file system commands.
Network File System (NFS)	A file system type that permits files residing on remote machines to be accessed as though they reside on the local machine.
CD-ROM File System (CDRFS)	A file system type that allows the contents of a CD-ROM to be accessed through the normal file system interfaces (open, read, and close).

File System Structure

On standalone machines, the following file systems reside on the associated devices by default:

/File System	/Device
/dev/hd1	/home
/dev/hd2	/usr
/dev/hd3	/tmp
/dev/hd4	/(root)
/dev/hd9var	/var
/proc	/proc
/dev/hd10opt	/opt

The file tree has the following characteristics:

- Files that can be shared by machines of the same hardware architecture are located in the **/usr** file system.
- Variable per-client files, for example, spool and mail files, are located in the **/var** file system.
- The **/(root)** file system contains files and directories critical for system operation. For example, it contains
  - A device directory (**/dev**)
  - Mount points where file systems can be mounted onto the root file system, for example, **/mnt**

AIX 5L Version 5.2

Installation Guide and Reference

SC23-4389-01

Chapter 17. Network Installation Management Introduction

This chapter provides an introduction to AIX Network Installation Management (NIM) and the operations you can perform to manage the installation of the Base Operating System (BOS) and optional software on one or more machines.

The types of machines you can manage are *standalone*, *diskless*, and *dataless*. A *standalone* machine is one that can boot (start up) by itself. Diskless and dataless systems cannot boot by themselves. They must use remote resources to boot. *Diskless* systems have no disk drive. *Dataless* systems have a local disk drive but they cannot boot from it. This section provides concepts and procedures for setting up the NIM environment, initiating the installation of standalone machines, and initializing resources for diskless and dataless machines.

Using NIM, you can install a group of machines with a common configuration or customize an installation for the specific needs of a given machine. The number of machines you can install simultaneously depends on the throughput of your network, the disk access throughput of the installation servers, and the platform type of your servers.

The NIM environment comprises client and server machines. A *server* provides resources (for example, files and programs required for installation) to another machine. A machine that is dependent on a server to provide resources is known as a *client*. In this guide and reference, any machine that receives NIM resources is a client, although the same machine can also be a server in the overall network environment.

All operations on clients in the NIM environment require one or more resources. NIM resource objects represent files and directories that are used to support some type of NIM operation. Because NIM resources are ordinary file system objects in the AIX operating system, most of them are provided to clients with standard Network File System (NFS) software. This means that many resources must reside locally on the servers providing these resources, because NFS can only export file system objects that are stored on local media in the machines from which they are exported.

Most installation tasks in the NIM environment are performed from one server, called the *master*. A set of installation tasks can also be performed from NIM clients. Once the network installation setup is complete, users of standalone clients can, from the client, install software that is available on NIM servers.

The machines you want to manage in the NIM environment, their resources, and the networks through which the machines communicate are all represented as *objects* within a central database that resides on the master. Network objects and their attributes reflect the physical characteristics of the network environment. This information does not affect the running of a physical network but is used internally by NIM for configuration information.

Each object in the NIM environment has a unique name that you specify when the object is defined. The NIM name is independent of any of the physical characteristics of the object it identifies and is only used for NIM operations. The benefit of unique names is that an operation can be performed using the NIM name without having to specify which physical attribute should be used. NIM determines which object attributes to use. For example, to easily identify NIM clients, the host name of the system can be used as the NIM object name, but these names are independent of each other. When an operation is performed on a machine, the NIM name is used, and all other data for the machine (including the host name) is retrieved from the NIM database.

For more information about NIM concepts, see Chapter 24, "Network Installation Management Concepts", on page 239. For information on a particular NIM task, refer to Chapter 18, "NIM Task Roadmap", on page 169.

'65-E54 IBM High Availability Cluster Multi-Processing for AIX I.5.0 (HACMP)

I U.S. Sales Manual
/ised: June 24, 2003.

ble of contents

Document options

Printable version

I U.S. Product Life Cycle Dates

Program [illegible]ber	VRM	Announced	Available	Marketing Withdrawn	Service Discontinued	Replaced By
[illegible]E54	4.05.0	2002/06/18	2002/07/12	2003/12/31	2004/12/31	5765-F62
5765-E54	4.04.1	2001/06/26	2001/07/13	2003/06/30	2003/12/31	-
5765-E54	4.04.0	2000/06/20	2000/06/23	2001/07/13	2003/12/31	-

Back to top

stract

r IBM US, No Longer Available as of December 31, 2003)
r IBM US, Program Services Discontinued as of December 31, 2004)
l customers with mission-critical environments can better protect their multiprocessing systems with the High ilability Cluster Multi-Processing for AIX 5L, V4.5.0 (HACMP V4.5). HACMP is designed to detect system ures and manage fallover to a recovery node, providing continuous application availability. HACMP 4.5.0 rs improved usability and performance, easier configuration, and additional hardware and software support IBM eServer Cluster 1600, pSeries, and RS/6000 customers with mission-critical applications.
v features include:

- Reduced Fallover Time through parallel processing of resources
- [illegible]tegration with AIX Workload Manager (WLM) for better operational performance after fallover
- Streamlined configuration process via automated Network Discovery
- Improved security for cluster administration via HAView and HATivoli
- Persistent IP address support for applications (such as Tivoli) which require invariant node addresses
- Expanded WAN and X.25 support
- Cluster status information in a Web Browser
- Enhanced Custom Pager Notification support

ditionally, in Enhanced Scalability (ES) and ES/Concurrent Resource Manager (ESCRM):

- Easier configuration of AIX Enhanced Concurrent Mode to define concurrent volume groups on any disk device
- New Application Availability Analysis Tool for customer measurement of system and application "up time"
- Tighter integration with GPFS V1.5 Cluster Filesystem

Manual 26

Xseries (Servidores Intel)

IBM @server xSeries Education

xSeries Reference (xREF)

including

IBM @server™

IntelliStation™ / xSeries™ / BladeCenter™

July 1, 2003

IBM @server xSeries Education

IBM @server™ xSeries™ 440 (November 2002)

xREF by eServer Field Skills Enablement Team

IBM® Type-model	Qty x Processor	L3 cache	L4 cache	Memory	Disk	SCSI controller	Mech-anical	Slots x bays	SMP/RXE Exp Ports	Hot-swap pwr supplies	Mgmt adapter	Available date
8687-4RX	2 x Xeon™ MP 1.5GHz	1MB	32MB	2GB Chipkill™	None	2xUltra160	4U[4] rack	6x4	3/1	Two redundant	PCI	Nov 2002
8687-5RX	2 x Xeon MP 1.9GHz	1MB	32MB	2GB Chipkill	None	2xUltra160	4U rack	6x4	3/1	Two redundant	PCI	Nov 2002
8687-6RX	4 x Xeon MP 1.9GHz	1MB	32MB	4GB Chipkill	None	2xUltra160	4U rack	6x4	3/1	Two redundant	PCI	Nov 2002
8687-7RX	4 x Xeon MP 2.0GHz	2MB	32MB	2GB Chipkill	None	2xUltra160	4U rack	6x4	3/1	Two redundant	PCI	Nov 2002

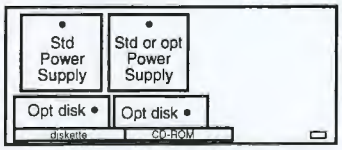
Positioning	*Up to 8-way power for high-end databases, server consolidation and mission-critical business applications*
Processors	**2 or 4 x Intel® Xeon™ Processor MP 1.5, 1.9, or 2.0GHz**[1] with 400MHz frontside bus / supports Hyper-Threading technology
L2 cache	**512KB** each processor / on die of processor / at processor speed
L3 cache	**1MB** or **2MB** each processor / on die of processor / at processor speed
L4 cache	**32MB XceL4™ Server Accelerator Cache** (up to **64MB** with optional SMP Expansion Module) / 32MB in each SMP Expansion Module / ECC / 64-bit 400MHz bus from Cache and Scalability Controller
Processor upgrade	**4-way SMP** (up to **8-way SMP** with optional SMP Expansion Module)
SMP Expansion Module	**One SMP Expanion Module std** / two max / each contains four Intel 603-pin micro-PGA ZIF sockets for Xeon MP, 32MB L4 cache, sixteen DIMM sockets, three SMP Expansion Ports (second module connected via one or two SMP Expansion Ports) / each SMP Expansion Module activates one RXE Expansion Port (only one RXE Expansion Port supported)
Additional boards	One I/O Board (PCI-X Host Bridge, SCSI, ethernet, graphics, South Bridge, Super I/O, slot for Mgmt Adapter), one PCI Board (PCI-X Host Bridge, six PCI-X slots), one Midplane Board (connects SMP Exp Modules, I/O Board, PCI Board)
Memory	**2GB** or **4GB** std / **16GB** max[13] (up to **32GB** with optional SMP Expansion Module) / four DIMMs installed (512MB or 1GB) / 16 DIMM gold-connector slots / must install four indentical DIMMs at same time / 4-way interleaving / PC133-compliant / 3.3v registered 168-pin SDRAM RDIMMs / 133MHz / **Error Checking and Correcting (ECC) and Chipkill™ via Memory ProteXion™** (1, 2, 3, or 4-bit errors on same chip; up to two chips at once; redundant bit steering) / **Active Memory™** via memory mirroring (memory mirroring supported with any OS)
SCSI disk controller	Adaptec® AIC-7899W / Wide Ultra160 SCSI (LVD 160MB/sec) / dual channel / 64-bit 66MHz PCI / integrated on I/O Board
SCSI implementation	First channel to internal 2-port SCSI backplane for internal hot-swap disks (16-bit LVD cable to SCSI backplane) / second channel to one external .8mm VHDCI 68-pin connector (16-bit LVD cable from I/O Board to ext connector) / one standard (longer) 16-bit LVD cable included for attaching an optional ServeRAID adapter to the two-bay backplane
IDE controller	Enhanced IDE ATA-100 controller in South Bridge / one one-drop IDE cable to backplane for diskette and CD-ROM
Disk - capacity/bays	No disks standard / supports up to 15K rpm SCSI disks / two hot-swap bays / converged tray / 80-pin SCA-2 connectors
Mechanical	**EIA 19" rack models (4U[4])** x 28" deep / supported in NetBAY™ Racks (such as NetBAY42 SR, NetBAY42 ER)
Chipset	**IBM XA-32™ chipset** / IBM Cache and Scalability Controller with L4 cache controller and three SMP Expansion Ports / IBM Memory I/O Controller with two remote I/O ports (each to a IBM PCI-X Host Bridge) / each IBM PCI-X Host Bridge provides three peer PCI buses / PCI 2.2 Bus E supports graphics, adapter slot with Remote Supervisor Adapter, VIA® 82C686B South Bridge (IDE ATA-100, USB, Super I/O PC97317VUL [keyboard, mouse]) / PCI 2.2 Bus F supports SCSI, ethernet / PCI-X Bus A, B, C, D support PCI-X slots / designed to the PCI-X 1.0 specification
Slots (Active™ PCI-X)	Six hot-swap PCI-X 1.0 slots[10] available with power and attention indicator lights (optical sensors control power to slot) / **hot replace, hot upgrade, hot expansion** /separated by insulative plastic dividers
RXE Expansion Port	**One port to support up to 12 additional PCI-X slots via an optional IBM RXE-100 Remote Expansion Enclosure**
CD-ROM / diskette	24X-10X[6] CD-ROM / 3.5" 1.44MB diskette drive / both removable from Ultrabay™ 2000 bays / supports CD-RW, DVD
Ethernet	Broadcom® 5700 10/100/1000 ethernet controller / on I/O Board / full duplex / 64-bit 66MHz PCI bus / Wake on LAN®
Graphics controller	SVGA / S3® Savage4 Pro / on I/O Board / 8MB SDRAM 125MHz std/max / up to 1280x1024 at 64K colors at 85Hz
Ports	*Rear:* RXE-100 Expansion Port (to connect optional RXE-100), RXE Management Port, two USB (Vers 1.1), keyboard, mouse, analog DB-15 graphics, ethernet / no serial or parallel ports / *Front:* one USB (Vers 1.1)
Security	Power-on and administrator passwords / unattended boot / selectable boot
Systems mgmt	**Remote Supervisor Adapter** / PCI adapter / includes 10/100 ethernet, RJ-11, and serial connectors / provides remote console and mgmt / power on/off system / monitors power status, op system, temperature, disks, fans, power supplies
Diagnostics	**Light Path Diagnostics™** / primary indicator on information panel with LEDs associated with failing components / IBM Real Time Diagnostics (operated through IBM Director) available even while server running
Software	**ServerGuide™** (CD-ROM installation and configuration utilities), IBM Director, and others
Keyboard / mouse	None standard (because rack-based)
Power supplies	*Std:* two; *max:* two / hot-swap / 1050 watts at 220v or 550 watts at 110v / redundant at 220v with two power supplies / front access / worldwide / voltage-sensing / auto-restart / fans in each power supply / PFA
Cooling fans	Four hot-swap, redundant, multi-speed fans / one additional fan in each power supply / PFA

xSeries SMP Expansion Module	59P5188
512MB PC133 ECC SDRAM RDIMM	33L3324
1GB PC133 ECC SDRAM RDIMM	31P8300
Xeon MP 1.5GHz/1MB L3 Cache Proc Upg	59P5171
Xeon MP 1.9GHz/1MB L3 Cache Proc Upg	59P5172
Xeon MP 2.0GHz/2MB L3 Cache Proc Upg	59P5173
IBM 73.4GB 10K Ultra160 SCSI Hot-Swap	06P5756
IBM ServeRAID™-4H Ultra160 SCSI Adapter	37L6889
8X/4X/24X Max CD-RW Ultrabay 2000	22P9101
IBM T540 15" Flat Panel Color Monitor (black)	9511AG4

Other options at **ibm.com**/pc/us/accessories

Six available 3.3 volt Active PCI-X slots:

Slot 1: fullsize, 64-bit 66MHz PCI-X, hot-swap Bus A
Slot 2: fullsize, 64-bit 66MHz PCI-X, hot-swap Bus A
Slot 3: fullsize, 64-bit 100MHz PCI-X, hot-swap, Bus B
Slot 4: fullsize, 64-bit 100MHz PCI-X, hot-swap, Bus B
Slot 5: fullsize, 64-bit 133MHz PCI-X, hot-swap, Bus C
Slot 6: fullsize, 64-bit 133MHz PCI-X, hot-swap, Bus D
Slot: used by Remote Supervisor Adp, 32-bit 33MHz



4U Rack

Bay ① 3.5", 0.5", access, diskette (Ultrabay 2000)
Bay ② 3.5", 0.5", access, CD-ROM (Ultrabay 2000)
Bay ③ 3.5", SL 1", access, hot-swap
Bay ④ 3.5", SL 1", access, hot-swap

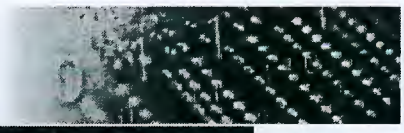
- Dimensions: H7.0" x W19.0" x D27.5"
  Dimensions: H178mm x W483mm x D699mm
- Max weight: 110 lbs; 50kg
- Stealth black color
- Tool-free serviceability
- Access processors, memory, adapters, and SMP Expansion Module from top
- Access power supplies and disks from front
- Setup Program by pressing F1 at startup
- Diagnostics (PC-Doctor) by pressing F2 at startup
- SCSISelect by pressing Ctrl+A at startup
- Information LED panel and front-accessible pull-out Light Path panel (1st and 2nd level diagnostics without removing cover)
- Predictive Failure Analysis® alerts on processors, XceL4 Server Accelerator Cache, memory, fans, power supplies, and optional disks with IBM Director

All models: Maximum internal disk capacity: 146.8GB with two 73.4GB[2] hot-swap SCSI disks

LIMITED WARRANTY[3]

- **1 year parts and labor**
- **International Warranty Service[3]**
- **On site, 24 hr x 7 day coverage, same day response time[7]**
- **1 year on site warranty service upgrade option (in eligible locations):[7]**
  - **24 hr x 7 day coverage, 2 hour response time** (No ServicePac available)
- **Post warranty maintenance services available**
- **24x7[14] toll-free support for warranty questions during the warranty period[3]**

See footnotes for important warranty information
US models announced November 5, 2002
• = Hot-swap



TPC Transaction Processing Performance Council

The TPC defines transaction processing and database benchmarks and delivers trusted results to the industry.

- Home
- Results
- Benchmarks
  - TPC-C
  - **- Results**
  - - Description
  - - FAQ
  - TPC-H
  - TPC-R
  - TPC-W
  - Obsolete
  - - TPC-A
  - - TPC-B
  - - TPC-D
- Technical Articles
- Related Links
- What's New
- About the TPC
- Who We Are
- Member Login

TPC-C Result Highlights

IBM eServer xSeries 440 c/s 8p

Benchmark Stats

Result ID:	103040401
Result Status:	In Review
TPC-C Rev:	5.1
Report Date:	04/04/03

System Information

Total System Cost	781,556 US $
TPC-C Throughput	119,115
Price/Performance	6.56 US $
Availability Date	10/04/03
Database Manager	Microsoft SQL Server 2000 Enterprise Ed. SP3
Operating System	Microsoft Windows Server 2003 Datacenter Edition
Transaction Monitor	Microsoft COM+

Server Information

CPU:	Intel Xeon MP 2.0 GHz
# of CPUs:	8
Cluster:	N

Client Information

# of clients:	4
CPU:	Intel Xeon DP 2.4GHz
CPUs per client:	8

- Executive Summary (148 KB)
- Full Disclosure Report (2513 KB)

top

Home Results Benchmarks Technical Articles Related Links What's New
About the TPC Who We Are Privacy Policy About Pricing

xSeries 2.0GHz 2MB L3 Cache Upgrade with Xeon Processor MP

IBM Web Price
$6,599.00*
Availability: **Within 2 weeks****

Add to cart

eserver

This 2.0GHz server processor based on the new Intel NetBurst microarchitecture provides fast processing speeds, a new integrated 1MB L3 cache architecture, a high-bandwidth 400MHz system bus and advanced features for availability and manageability. It also includes a revolutionary new Hyper-Threading technology which helps improve system performance by simultaneously processing software threads in parallel.

Features and Benefits:

Available in 1.5GHz, 1.9GHz and 2.0GHz speeds and 1MB and 2MB L3 cache sizes
400MHz system bus enables increased data throughput, thereby delivering up to 3.2GB of data per second in and out of the processor
The winning combination of NetBurst microarchitecture, Hyper-Threading technology and the integrated L3 cache architecture provide enhanced performance, greater system bandwidth and scalable headroom for compute, database, directory, security, middleware and collaboration applications
This new Intel Xeon Processor MP delivers outstanding throughput and performance headroom for large server workloads resulting in support for more end-users
2MB integrated Level-3 cache further improves application performance by allowing more instructions to reside in high-speed memory on the processor core

General	
Model name	59P5173
Description	xSeries 2.0GHz 2MB L3 Cache Upgrade with Xeon Processor MP
IBM Web Price*	$6,599.00
Compatibility	
Hardware prerequisites (System unit)	xSeries 440
Product approvals/certifications	FCC, UL, CE, CSA, EN
Characteristics	
Processor (CPU)	Intel® Xeon ™ MP
Processor internal clock speed	2.00 GHz
Processor manufacturer	Intel®
Processor	
Planar clock speed	400 MHz

Add to cart

*Price does not include tax or expedited shipping and is subject to change without notice. Reseller prices may vary. IBM does not warrant non-IBM products. PCs shown here, except for Servers and Network Stations, ship with an operating system. All offers subject to availability. IBM reserves the right to alter product offerings and specifications at any time without notice. IBM is not responsible for photographic or typographic errors.

** An estimated ship date will be included with your order confirmation e-mail. Availability does not determine when your order will ship since inventory status may change before your order is final (following the receipt of any credit or payment authorization) as other orders are processed. "In stock" indicates we currently have at least one of the item in stock. Orders are normally held until all the products on the order are in inventory. "Within 2 weeks" indicates that the product should be available in inventory within 2 weeks. "Within 2-4 Weeks" indicates that the product should be available in inventory in 2-4 weeks. To obtain the latest information about the availability of a specific part number, please call 1-883-SHOP-IBM

IBM United States

Search

Home | Products & services | Support & downloads | My account | Call 1-888-SHOP-IBM

Select a country

- ← Personal computing
- Accessories & upgrades
- Services
- Support
- ThinkVantage Technologies
- Presentations
- News & awards
- Library
- Request a Catalog

Shopping help

- Warranty info
- Shop by part number
- View cart
- Open saved carts
- Estimate shipping
- Estimate leasing
- Order status
- Returns policy
- Shopping guarantee

Related links:

- Home / home office
- Small & Medium Business
- Government
- Education

Your TeleWeb Hotline!

888-SHOP-IBM x 7000

Call for express sales service!

xSeries SMP Expansion Module

IBM Web Price
$5,199.00*
Availability: **Within 2 weeks****

Add to cart

eserver

This option module is installed on the x440 centerplane next to the standard module. It is compatible with all Intel Xeon Processor MP models of the x440. This option module must be used for installation of the 1.5GHz (part# 59P5171), 1.9GHz (part# 59P5172) and 2.0GHz (part# 59P5173) processor options. Prior to installation, the standard SMP expansion module must be fully populated with four Intel Xeon Processors MP of the same type and speed.

Features and Benefits:

Four additional CPU connectors
32MB of L4 system cache
16 memory connectors supporting an additional 16GB of system memory
Three SMP expansion ports

General	
Model name	59P5188
Description	xSeries SMP Expansion Module
IBM Web Price*	$5,199.00
Compatibility	
Hardware prerequisites (System unit)	xSeries 440
Product approvals/certifications	CE, UL, FCC, EN, CSA
Warranty	
Limited Warranty period	One year
Type of Service	Customer Carry-in Repair, Customer Carry-in Exchange

Add to cart

*Price does not include tax or expedited shipping and is subject to change without notice. Reseller prices may vary. IBM does not warrant non-IBM products. PCs shown here, except for Servers and Network Stations, ship with an operating system. All offers subject to availability. IBM reserves the right to alter product offerings and specifications at any time without notice. IBM is not responsible for photographic or typographic errors.

** An estimated ship date will be included with your order confirmation e-mail. Availability does not determine when your order will ship since inventory status may change before your order is final (following the receipt of any credit or payment authorization) as other orders are processed. "In stock" indicates we currently have at least one of the item in stock. Orders are normally held until all the products on the order are in inventory. "Within 2 weeks" indicates that the product should be available in inventory within 2 weeks. "Within 2-4 Weeks" indicates that the product should be available in inventory in 2-4 weeks. To obtain the latest information about the availability of a specific part number, please call 1-888-SHOP-IBM.

Important Legal Information

IBM United States

Search

Home | Products & services | Support & downloads | My account | Call 1-888-SHOP-IBM

Select a country

← Personal computing

Accessories & upgrades

Services

Support

ThinkVantage Technologies

Presentations

News & awards

Library

Request a Catalog

Shopping help

Warranty info

Shop by part number

View cart

Open saved carts

Estimate shipping

Estimate leasing

Order status

Returns policy

Shopping guarantee

Related links:

Home / home office

Small & Medium Business

Government

Education

512MB PC133 CL3 ECC SDRAM RDIMM

IBM Web Price
$499.00*
Availability: **In stock****

Add to cart

Upgrade your standard system memory capacity with this IBM memory option, improving your overall system performance. SDRAM enables faster performance than either traditional fast page mode or hyper-page mode memory. Adding additional IBM Memory is a cost-effective way to improve your system's performance.

Features and Benefits:

Fast access time -- synchronous to processor's front-side bus clock
168-pin DIMM with gold-plated leads
Serial presence detect/decode functions

General	
Model name	33L3324
Description	512MB PC133 CL3 ECC SDRAM RDIMM
IBM Web Price*	$499.00
Compatibility	
Hardware prerequisites (System unit)	xSeries 232, xSeries 342, xSeries 343, xSeries 440
Product approvals/certifications	CE Mark (EN 55024:1998)
Characteristics	
Memory capacity	512 MB
Memory type	PC133 SDRAM
Average access time	133
Form factor	DIMM
Height	5.25 inches
Width	.15 inches
Depth	1.7 inches
Warranty	
Limited Warranty period	Three year
Type of Service	Customer Carry-in Exchange

Add to cart

*Price does not include tax or expedited shipping and is subject to change without notice. Reseller prices may vary. IBM does not warrant non-IBM products. PCs shown here, except for Servers and Network Stations, ship with an operating system. All offers subject to availability. IBM reserves the right to alter product offerings and specifications at any time without notice. IBM is not responsible for photographic or typographic errors.

** An estimated ship date will be included with your order confirmation e-mail. Availability does not determine when your order will ship since inventory status may change before your order is final (following the receipt of any credit or payment authorization) as other orders are processed. "In stock" indicates we currently have at least one of the item in stock. Orders are normally held until all the products on the order are in inventory. "Within 2 weeks" indicates that the product should be available in inventory within 2 weeks. "Within 2-4 Weeks" indicates that the product should be available in inventory in 2-4 weeks. To obtain the latest information about the availability of a specific part number, please call 1-888-SHOP-IBM.

Important Legal Information

Features and specifications

The following table provides a summary of the features and specifications for each xSeries 440.

Microprocessor:

- Supports the following microprocessors (depending on your configuration):
  - Up to 8 Intel™ Xeon MP microprocessors

    OR
  - Up to 4 Intel Xeon DP microprocessors

  Note: Use the Information in BIOS to determine the type and speed of the microprocessors installed in your server.
- IBM XA-32 chip set with integrated memory, I/O, system cache, and remote I/O controllers

Memory:

- Minimum: 2 GB
- Maximum: 32 GB (depending on your configuration)
- Type: 4-way interleaved PC133 MHz, ECC SDRAM, registered DIMMs only
- Supports 512 MB and 1GB dual inline memory modules (DIMMs)
- XceL4 Server Accelerator Cache (up to 64 MB depending on your configuration)

Drives:

- Diskette: 1.44 MB
- CD-ROM: 24X IDE
- Supports up to two internal Ultra160 SCSI hard disk drives

Active™ PCI-X expansion slots:

Six 64-bit Active PCI-X expansion slots:

- Two 66 MHz PCI-X slots
- Two 100 MHZ PCI-X slots
- Two 133 MHZ PCI-X slots
- Additional PCI-X slots available in an optional remote I/O expansion enclosure (models 1RX, 2RX, 3RX, 4RX, 5RX, 6RX, 7RX, 3RY, 4RY only)

Power supply:

Two hot-swap power supplies (550 watts at 110 V ac or 1050 watts at 220 V ac)

Cooling:

Four hot-swap fans

- Two 150 mm x 51 mm redundant fans
- Two 150 mm x 38 mm fans

Video:

- S3 Savage4 Pro video on system board
- PCI bus interface
- Compatible with SVGA
- 8 MB SDRAM video memory at 125 MHz

Size (4U):

- Height: 17.8 cm (7 inches, 4U)
- Depth: 69.85 cm (27.5 inches)
- Width: 48.3 cm (19 inches)
- Maximum weight: 50 kg (110 lb) depending on your configuration

Integrated functions:

- Broadcom 5700 10/100/1000 Ethernet controller
- Light path diagnostics
- Adaptec 7899W Dual Ultra160 SCSI controller
- Remote Supervisor Adapter (service processor)
  - ASM interconnect (peer-to-peer) port
  - Ethernet port
  - Serial port
- IDE controller
- RXE Management Port
- Three USB ports
- Keyboard port
- SCSI port
- Mouse port
- Symmetrical multiprocessor (SMP) Expansion Ports (up to six ports depending on your configuration)
- Two remote I/O expansion enclosure (RXE) Expansion Ports

Acoustical noise emissions:

- Sound power, idling: 6.2 bel maximum
- Sound power, operating: 6.2 bel maximum

Environment:

- Air temperature:
  - Server on: 10° to 35°C (50.0° to 95.0°F). Altitude: 0 to 914 m (2998.7 ft)
  - Server on: 10° to 32° C (50.0° to 89.6° F). Altitude: 914 m (2998.7 ft) to 2133 m (6998.0 ft)
  - Server off: -40° to 60° C (-104° to 140° F). Maximum altitude: 2133 m (6998.0 ft)
- Humidity:
  - Server on: 8% to 80%
  - Server off: 5% to 100%

Heat output:

Approximate heat output in British thermal units (Btu) per hour

- Minimum configuration: 855 Btu (250 watts)
- Maximum configuration: 2726 Btu (800 watts)

Electrical input:

- Sine-wave input (47-53 or 57-63 Hz) required
- Input voltage low range:
  - Minimum: 100 V ac
  - Maximum: 127 V ac
- Input voltage high range:
  - Minimum: 200 V ac
  - Maximum: 240 V ac
- Input kilovolt-amperes (kVA) approximately:
  - Minimum: 0.250 kVA
  - Maximum: 0.800 kVA

13

Locator light: This blue light indicates the primary and secondary servers. This light blinks on the primary server. If the light remains solid, it indicates that server is the secondary server. See "Identifying problems using the light path diagnostics feature" on page 52 for the exact location of this light.

CD-ROM drive eject button: Push this button to release a CD-ROM drive from the server.

CD eject button: Push this button to release a CD from the drive.

CD-ROM drive activity light: When this light is on, it indicates that the CD-ROM drive is in use.

Diskette drive eject button: Push this button to release a diskette drive from the server.

Diskette eject button: Push this button to release a diskette from the drive.

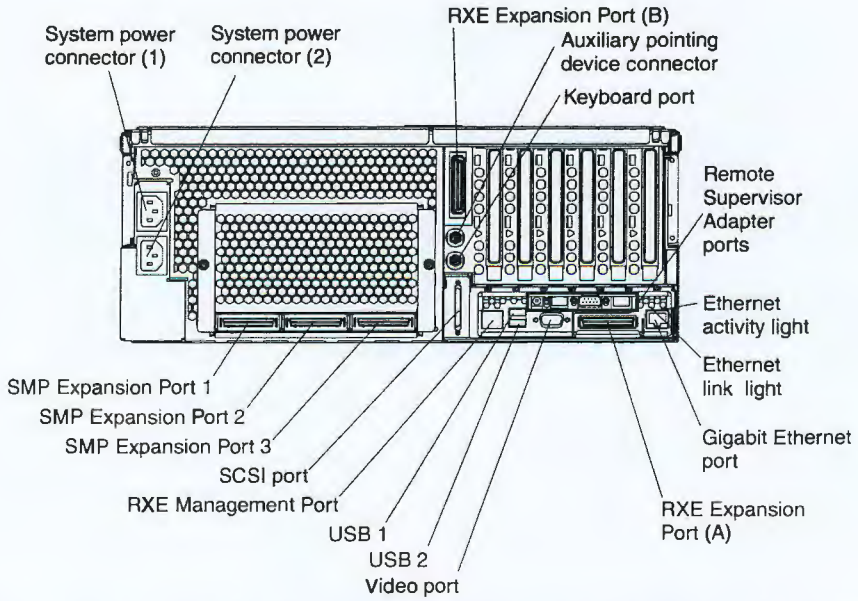
Diskette drive activity light: When this light is on, it indicates that the diskette drive is in use.

Power supply latch: This latch is used to secure the power-supply in place.

Reset button: Press this button to reset the server and run the power-on self-test (POST). You might need to use a pen or the end of a straightened paper clip to press the button.

Power button: Press this button to manually turn the server on or off.

Rear view



System power connectors (1 and 2): The system power cords are connected to these two connectors to provide power to the system.

RXE Expansion Port (B): Use this port to connect the server to a remote I/O enclosure (models 1RX, 2RX, 3RX, 4RX, 5RX, 6RX, 7RX, 3RY, 4RY only) when two SMP Expansion Modules are installed.

15

IBM @server xSeries Education

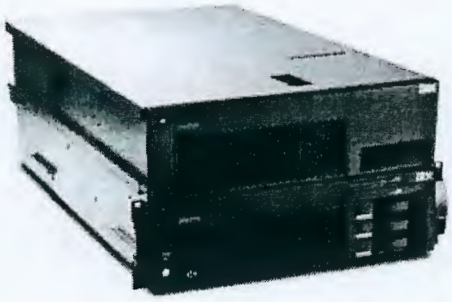
xSeries Reference (xREF)

including

IBM @server™

IntelliStation™ / xSeries™ / BladeCenter™

July 1, 2003



IBM @server xSeries Education

17

IBM @server™ xSeries™ 360 (November 2002)

xREF by eServer Field Skills Enablement Team

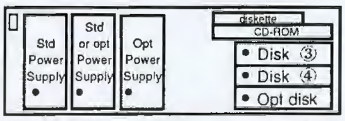
IBM® Type-model	Qty x Processor	L3 cache	Memory	Disks	SCSI controller	Mechanical	Slots bays	RXE Exp Ports	Hot-swap pwr supplies	Mgmt adapter	Available date
8686-7RX	1 x Xeon™ MP 1.5GHz	1MB	1GB Chipkill™	None	Ultra160	3U[4] rack	6x5	One	One (not redun)	PCI	Dec 2002
8686-8RX	2 x Xeon MP 1.9GHz	1MB	2GB Chipkill	None	Ultra160	3U rack	6x5	One	Two redundant	PCI	Dec 2002
8686-9RX	2 x Xeon MP 2.0GHz	2MB	2GB Chipkill	None	Ultra160	3U rack	6x5	One	Two redundant	PCI	Dec 2002

Positioning	*Space efficient 4-way, 3U, rack-dense server with ground breaking Enterprise X-Architecture™ technology*
Processors	**1 or 2 x Intel® Xeon™ Processor MP 1.5, 1.9, or 2.0GHz**[1] with 400MHz frontside bus / Hyper-Threading technology
L2 cache	**512KB** / on die of processor / at processor speed
L3 cache	**1MB** or **2MB** / on die of processor / at processor speed
Processor upgrade	**4-way SMP** / up to four Xeon Processors MP (same speed/cache size)
Implementation	Systemboard contains four Intel 603-pin micro-PGA ZIF sockets, one memory board slot, six Active™ PCI-X slots, and integrated SCSI, ethernet, graphics
Memory	**1GB** or **2GB** std / 16GB max[12,13] / two (1GB model) or four (2GB models) 512MB DIMMs installed / 1.7-inch tall / one memory board standard with 8 DIMM gold-connector slots / DIMMs must be installed in matched pairs / 128-bit simultaneous transfer from two DIMMs / PC1600 200MHz registered 184-pin DDR-SDRAM RDIMMs / **Error Checking and Correcting (ECC)** via **16-bit Checksum Chipkill™** (corrects 1, 2, 3, or 4-bit errors on same chip and detects 2- through 8-bit errors contained in two chips)
SCSI disk controller	Adaptec® AIC-7892 / Wide Ultra160 SCSI (LVD 160MB/sec) / single channel / 64-bit 33MHz PCI / integrated on planar
SCSI connectors	Controller hard-wired to SCSI backplane (no cable) / no external SCSI connector
SCSI cabling	One standard 16-bit LVD cable included for attaching an optional ServeRAID adapter to the three-bay backplane; SCSI RAID adapter 68-pin connector on systemboard for this cable to get signals to three-bay backplane
IDE controller / cabling	Enhanced IDE ATA-33 controller in OSB4 South Bridge
Disk - capacity	None standard / supports up to 15,000 rpm disks
Disk - bays	Three hot-swap bays / converged tray / 80-pin SCA-2 connectors
Mechanical	**EIA 19" rack models (3U[4])** x 28" deep / supported in NetBAY™ Racks (such as NetBAY42 SR, NetBAY42 ER)
Chipset	**IBM XA-32™ chipset** / IBM Memory I/O Controller (improved performance from earlier models) with two remote I/O ports (one to IBM PCI-X Host Bridge; one to RXE Expansion Port) / IBM PCI-X Host Bridge provides three peer PCI buses (two PCI-X 1.0, one PCI 2.2) / PCI 2.2 Bus 0 supports SCSI, graphics, ethernet, adapter slot with Remote Supervisor Adapter, and ServerWorks® OSB4 South Bridge (IDE, USB, ISA bus for Super I/O NS PC97317VUL [diskette, keyboard, mouse])
Slots (Active™ PCI-X)	Six hot-swap PCI-X 1.0 slots[10] available with power and attention indicator lights (optical sensors control power to slot) / **hot replace, hot upgrade, hot expansion** / separated by insulative plastic dividers
RXE Expansion Port	**One port to support up to 12 additional PCI-X slots via an optional IBM RXE-100 Remote Expansion Enclosure**
CD-ROM / diskette	24X-10X[6] CD-ROM / 3.5" 1.44MB diskette drive
Ethernet	Intel 82559 10/100 ethernet controller / on systemboard / full duplex / 32-bit PCI / Wake on LAN® / Alert on LAN™ 2
Graphics controller	SVGA / S3® Savage4 LT / on systemboard / 8MB SDRAM std/max / up to 1280x1024 at 64K colors at 85Hz
Ports	*Rear:* RXE-100 Expansion Port (to connect optional RXE-100), RXE Management Port (to manage optional RXE-100), two USB (Ver 1.1), keyboard, mouse, analog DB-15 graphics, ethernet / no serial or parallel ports / *Front:* one USB (Ver 1.1)
Security	Power-on and administrator passwords / unattended boot / selectable boot
Systems management	**Remote Supervisor Adapter** / PCI adapter / includes 10/100 ethernet, RJ-11, and serial connectors / provides remote console and mgmt / power on/off system / monitors power status, op system, temperature, disks, fans, power supplies
Diagnostics	**Light Path Diagnostics™** / primary indicator on information panel with LEDs associated with failing components / IBM Real Time Diagnostics (operated through IBM Director) available even while server running
Software	**ServerGuide™** (CD-ROM installation and configuration utilities), IBM Director, and others
Keyboard / mouse	None standard (because rack-based)
Power supplies	*Std:* one or two 370 watt hot-swap; *Max:* three hot-swap / redundant with two power supplies (some configurations) / worldwide / voltage-sensing / auto-restart / fans in each power supply / PFA
Cooling fans	Six hot-swap, redundant, multi-speed fans / one additional fan in each power supply / PFA / fan failure signals Diagnostic LED and mgmt processor

RXE-100 Remote Expansion Enclosure	86841RX
512MB PC1600 ECC DDR SDRAM RDIMM	33L3283
1GB PC1600 ECC DDR SDRAM RDIMM	33L3285
2GB PC1600 ECC DDR SDRAM RDIMM[12]	33L3287
Xeon MP 1.5GHz/1MB L3 Cache Proc Upg	59P6815
Xeon MP 1.9GHz/1MB L3 Cache Proc Upg	59P6816
Xeon MP 2.0GHz/2MB L3 Cache Proc Upg	59P6817
370 watt Hot-Swap Redundant Power Supply	31P6108
IBM ServeRAID™-4Mx Ultra160 SCSI Adapter	06P5736
IBM 73.4GB 10K Ultra160 SCSI Hot-Swap SL	06P5756
IBM NetBAY42 Standard Rack (SR)	9306420
IBM Integrated xSeries Adapter for iSeries	1519100
IBM T541 15" Flat Panel Color Monitor (black)	9512AB1

Other options at **ibm.com**/pc/us/accessories

Six available 3.3 volt Active PCI-X slots:
- Bus 2 (B) with two slots supports (slots 1, 2):
  - one fullsize, 64-bit, 133MHz PCI-X, hot-swap
  - or two fullsize, 64-bit, 100MHz PCI-X, hot-swap
  - or two fullsize, 64-bit, 66MHz PCI-X, hot-swap
  - or two fullsize, 64-bit, 66MHz PCI, hot-swap
  - or two fullsize, 64-bit, 33MHz PCI, hot-swap
- Bus 1 (A) with four slots supports (slots 3, 4, 5, 6):
  - four fullsize, 64-bit, 66MHz PCI-X, hot-swap
  - or two fullsize, 64-bit, 66MHz PCI, hot-swap
  - or four fullsize, 64-bit, 33MHz PCI, hot-swap
- Bus 0 with one slot supports:
  - only for standard Remote Supervisor Adapter halfsize, 64-bit, 33MHz PCI, not hot-swap



3U Rack

Bay ① 3.5", 0.5", access, diskette
Bay ② 3.5", 0.5", access, CD-ROM
Bay ③ 3.5", SL 1", access, hot-swap
Bay ④ 3.5", SL 1", access, hot-swap
Bay ⑤ 3.5", SL 1", access, hot-swap

- Dimensions: H5.25" x W17.4" x D27.6"
  Dimensions: H133.4mm x W442.0mm x D701mm
- Weight: 58.4 to 70lbs; 24.9 to 31.8kg
- Stealth black color
- Tool-free serviceability
- Access adapters, processors, memory, and systemboard from top
- Access power supplies and disks from front
- Setup Program by pressing F1 at startup
- Diagnostics (PC-Doctor) by pressing F2 at startup
- SCSISelect by pressing Ctrl+A at startup
- Top cover Light Path Diagnostics (level 2 diagnostic panel) for outside view of potential problem without removing cover
- Information LED panel, diagnostic LED panel, and component LEDs give visual indications of system well-being
- Predictive Failure Analysis[3] alerts on disks, power supplies, memory, processors, VRMs, and fans with IBM Director

All models: Maximum internal disk capacity: 220.2GB with three 73.4GB[2] hot-swap SCSI disks

LIMITED WARRANTY[3]

- **3 year parts and labor**
- **International Warranty Service**[3]
- **On site, 8 am - 5 pm, Mon - Fri coverage excluding holidays, next business day response time**[7]
- **On site service upgrade options (in eligible locations):**[7]
  - **3 year IOR 24x7, 4 hr avg response** (ServicePac® part num 96P2253)
  - **3 year IOR 24x7, 2 hr avg response** (ServicePac part num 96P2254)
  - **4 year IOR 9x5, NBD response** (ServicePac part num 96P2255)
  - **5 year IOR 9x5, NBD response** (ServicePac part num 96P2259)
  - **Other ServicePac options at ibm.com/services/its/us/source/wamemxeu.pdf**
- **24x7**[14] **toll-free support for warranty issues during the warranty period**[3]

See footnotes for important warranty information
US models announced November 5, 2002
• = Hot-swap

TPC Transaction Processing Performance Council

The TPC defines transaction processing and database benchmarks and delivers trusted results to the industry.

- Home
- Results
- Benchmarks
  - TPC-C
  - **Results**
  - Description
  - FAQ
  - TPC-H
  - TPC-R
  - TPC-W
  - Obsolete
  - TPC-A
  - TPC-B
  - TPC-D
- Technical Articles
- Related Links
- What's New
- About the TPC
- Who We Are
- Member Login

TPC-C Result Highlights

IBM eServer xSeries 360/2.0GHz/4p

Benchmark Stats

Result ID:	103022802
Result Status:	In Review
TPC-C Rev:	5.1
Report Date:	02/28/03

System Information

Total System Cost	226,504 US $
TPC-C Throughput	52,587
Price/Performance	4.31 US $
Availability Date	04/30/03
Database Manager	Microsoft SQL Server 2000 Enterprise Ed. SP3
Operating System	Microsoft Windows Server 2003 Enterprise Server
Transaction Monitor	Microsoft COM+

Server Information

CPU:	Intel Xeon MP 2.0 GHz
# of CPUs:	4
Cluster:	N

Client Information

# of clients:	2
CPU:	Intel Xeon DP 2.4GHz
CPUs per client:	1

- Executive Summary (216 KB)
- Full Disclosure Report (1433 KB)

top

Home Results Benchmarks Technical Articles Related Links What's New
About the TPC Who We Are Privacy Policy About Pricing

IBM United States

Home | Products & services | Support & downloads | My account | Call 1-888-SHOI

Select a country

← Personal computing
Accessories & upgrades
Services
Support
ThinkVantage Technologies
Presentations
News & awards
Library
Request a Catalog

Shopping help
Warranty info
Shop by part number
View cart
Open saved carts
Estimate shipping
Estimate leasing
Order status
Returns policy
Shopping guarantee

Related links:
Home / home office
Small & Medium Business
Government
Education

xSeries 2.0GHz/2MB L3 cache upgrade with Xeon Processor MP

eserver

intel inside XEON

Your TeleV
888-S
Call for exp

IBM Web Price
$5,749.00*
Availability: **In stock****

Add to cart

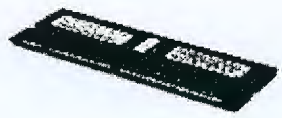
This 2.0GHz server processor based on the new Intel NetBurst microarchitecture provides fast processing speeds, a new integrated 2MB L3 cache architecture, a high-bandwidth 400MHz system bus and advanced features for availability and manageability. It also includes a revolutionary new Hyper-Threading technology which helps improve system performance by simultaneously processing software threads in parallel.

Features and Benefits:

Available in 1.5GHz, 1.9GHz and 2.0GHz speeds and 1MB and 2MB L3 cache sizes
400MHz system bus enables increased data throughput, thereby delivering up to 3.2GB of data per second in and out of the processor
The winning combination of NetBurst microarchitecture, Hyper-Threading technology and the integrated L3 cache architecture provide enhanced performance, greater system bandwidth and scalable headroom for compute, database, directory, security, middleware and collaboration applications
This new Intel Xeon Processor MP delivers outstanding throughput and performance headroom for large server workloads resulting in support for more end-users
2MB integrated Level-3 cache further improves application performance by allowing more instructions to reside in high-speed memory on the processor core

General	
Model name	59P6817
Description	xSeries 2.0GHz/2MB L3 cache upgrade with Xeon Processor MP
IBM Web Price*	$5,749.00
Compatibility	
Hardware prerequisites (System unit)	xSeries 255
Product approvals/certifications	UL, FCC, EN, CSA, CE
Characteristics	
Processor (CPU)	Intel® Xeon™ MP
Processor internal clock speed	2.00 GHz
Processor manufacturer	Intel®
Processor	
Planar clock speed	400 MHz

512MB PC1600 ECC DDR SDRAM RDIMM



IBM Web Price
$325.00*
Availability: **In stock****

Add to cart

This memory option features a new high-speed, double data rate (DDR) SDRAM Registered DIMM that enables the memory data transfer rate to increase without increasing the system processor front-side bus clock speed. This double data rate is accomplished by delivering data on both the rising and falling edge of the processor clock signal once the data transfer begins. This will enable the doubling of the memory transfer rate for the PC100 to 200MHz without increasing the 100MHz front-side bus clock speed. This option features two-way memory interleaving that expands the memory bandwidth and improves the system's overall performance.

Features and Benefits:

These memory data transfer rate enhancements translate into 6 to 8 percent improvements for typical applications. In some server applications where large contiguous blocks of data are transferred, significantly greater performance improvements will be achieved.
Chipkill memory technology increases overall system and data reliability and corrects many soft memory errors automatically without any software intervention

General	
Model name	33L3283
Description	512MB PC1600 ECC DDR SDRAM RDIMM
IBM Web Price*	$325.00
Compatibility	
Hardware prerequisites (System unit)	xSeries 360, xSeries 255
Product approvals/certifications	CE Mark (EN 55024:1998)
Characteristics	
Memory type	PC1600 DDR SDRAM

Add to cart

*Price does not include tax or expedited shipping and is subject to change without notice. Reseller prices may vary. IBM does not warrant non-IBM products. PCs shown here, except for Servers and Network Stations, ship with an operating system. All offers subject to availability. IBM reserves the right to alter product offerings and specifications at any time without notice. IBM is not responsible for photographic or typographic errors.

** An estimated ship date will be included with your order confirmation email. Availability does not determine when your order will ship since inventory status may change before your order is final (following the receipt of any credit or payment authorization) as other

25

xSeries 370W Hot Swap Redundant Power Supply

eserver

IBM Web Price
$249.00*
Availability: **In stock****

Add to cart

This 370-watt, auto-sensing power supply option can be installed in the IBM eServer (logo) xSeries 360 server to support robust configurations where redundancy is a requirement.

General

Model name	31P6108
Description	xSeries 370W Hot Swap Redundant Power Supply
IBM Web Price*	$249.00

Compatibility

Hardware prerequisites (System unit)	xSeries 360

Add to cart

*Price does not include tax or expedited shipping and is subject to change without notice. Reseller prices may vary. IBM does not warrant non-IBM products. PCs shown here, except for Servers and Network Stations, ship with an operating system. All offers subject to availability. IBM reserves the right to alter product offerings and specifications at any time without notice. IBM is not responsible for photographic or typographic errors.

** An estimated ship date will be included with your order confirmation e-mail. Availability does not determine when your order will ship since inventory status may change before your order is final (following the receipt of any credit or payment authorization) as other orders are processed. "In stock" indicates we currently have at least one of the item in stock. Orders are normally held until all the products on the order are in inventory. "Within 2 weeks" indicates that the product should be available in inventory within 2 weeks. "Within 2-4 Weeks" indicates that the product should be available in inventory in 2-4 weeks. To obtain the latest information about the availability of a specific part number, please call 1-888-SHOP-IBM.

Important Legal Information

Features and specifications

The following table provides a summary of the specifications and features for the xSeries 360 server.

Microprocessor:

- Intel® Xeon™ Processor MP (frequency varies with server model, each MP processor functions as two logical processors)
  - — Minimum: One
  - — Maximum: Four
- Level-3 cache size varies with model
- 100 MHz front-side bus (FSB)

Chipset:

IBM XA-32™ Chipset with integrated memory, I/O controller, and remote I/O controller.

Memory:

- DDR registered SDRAM DIMMs with ECC and Chipkill™ memory
  - — Minimum: 512 MB
  - — Maximum: 8 GB
- Slots: Interleaved, 8 slots

Drives standard:

- Slim diskette: 1.44 MB
- Slim CD-ROM: 24X-10X IDE

Hard disk drives:

- Slim-high hot-swap drives. (number of drives and drive capacity vary with model)
- Maximum: Three

Active™ PCI-X expansion slots:

- Two 100 MHz/64-bit PCI-X
- Four 66 MHz/64-bit PCI-X

Hot-swap power supplies:

370 W (115-230 V ac)

- Minimum: One
- Maximum: Three

Hot-swap cooling:

Six hot-swap fans

Video:

- S3 video controller
- Compatible with SVGA 4
- 8 MB SDRAM video memory

Size (3 U)

- Height: 134 mm (5.28 in.)
- Depth: 720 mm (28.35 in.)
- Width: 440 mm (17.32 in.)
- Weight: 25 kg (55 lb) to 31.7 kg (70 lb) depending upon configuration

Integrated functions:

- Light Path Diagnostics™
- Ultra160 SCSI controller
- One 10BASE-T/100BASE-TX Intel Ethernet controller
- Remote Supervisor Adapter (service processor)
  - — ASM interconnect (peer-to-peer) port
  - — RXE expansion port
  - — RXE management port
  - — Ethernet port
  - — Serial port
- Three universal serial bus ports
- Keyboard port
- Mouse port
- Video port

Acoustical noise emissions:

- Sound power, idling: 6.3 bel maximum
- Sound power, operating: 6.3 bel maximum
- Sound pressure, operating: 47 dBa maximum

Environment:

- Air temperature:
  - — Server on: 10° to 35°C (50° to 95°F). Altitude: 0 to 914 m (3000 ft)
  - — Server on: 10° to 32°C (50° to 89.6°F). Altitude: 914 m (3000 ft) to 2133 m (7000 ft)
  - — Server off: 10° to 43°C (50° to 110°F). Maximum altitude: 2133 m (7000 ft)
- Humidity:
  - — Server on: 8% to 80%
  - — Server off: 8% to 80%

Heat output:

Approximate heat output in British thermal units (Btu) per hour

- Minimum configuration: 1232 Btu (0.36 kilowatts)
- Maximum configuration: 3566 Btu (1.045 kilowatts)

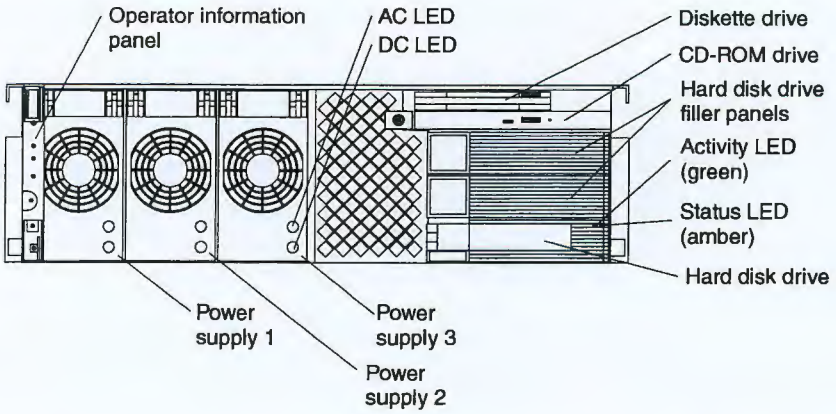
Electrical input:

- Sine-wave input (50-60 Hz) required
- Input voltage low range:
  - — Minimum: 100 V ac
  - — Maximum: 127 V ac
- Input voltage high range:
  - — Minimum: 200 V ac
  - — Maximum: 240 V ac
- Input kilovolt-amperes (kVA) approximately:
  - — Minimum: 0.08 kVA (ac power connected, server off)
  - — Minimum: 0.38 kVA (dc power on, server idle)
  - — Maximum: 1.1 kVA

- Customer support center 24 hours a day, 7 days a week[2]

Server controls and indicators

The following illustration shows the controls and indicators on the front of the server.



Operator information panel: This panel, also known as the front LED panel, contains controls, indicators, and one of the three USB ports. See "Operator information panel" on page 7 for details.

AC LED: Each hot-swap power supply has an ac power LED to indicate that ac power is available to the power supply.

DC LED: Each hot-swap power supply has a dc power LED to indicate that the power supply is active.

Diskette drive: The server contains one standard 3.5 diskette drive with an LED to indicate when it is active.

CD-ROM drive: The server contains one standard IDE CD-ROM drive with an LED to indicate when it is active.

Hard disk drive filler panels: A filler panel is used to cover empty hard disk drive bays. A filler panel must be installed in each empty bay to ensure proper system cooling.

Activity LED: Each hot-swap hard disk drive has an activity LED, which flashes if the drive is being accessed.

Status LED: Each hot-swap hard-disk drive has a status LED. If this amber LED is on continuously, the drive has failed. If an optional IBM ServeRAID™ adapter is installed in the server and the LED flashes slowly (one flash per second), the drive is being rebuilt. If the LED flashes rapidly (three flashes per second), the controller is identifying the drive.

Hard disk drive: The server supports a maximum of three hot-swap hard disk drives.

Power supplies 1, 2, and 3: The server comes with a minimum of one hot-swap power supply and supports a maximum of three hot-swap power supplies.

2.Service availability will vary by country. Response time will vary depending on the number and nature of incoming calls.

IBM @server xSeries Education

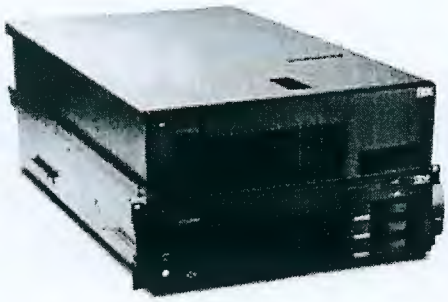
xSeries Reference (xREF)

including

IBM @server™

IntelliStation™ / xSeries™ / BladeCenter™

July 1, 2003



IBM @server xSeries Education

IBM @server™ xSeries™ 235 (February 2003)

xREF by Field Skills Enablement Team

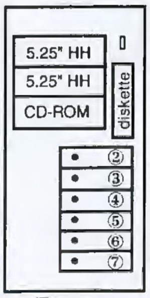
IBM® Type-model	Qty x Processor	L2 cache	FSB MHz	Memory	Disk	SCSI controller	Mechanical	Slots x bays (hot-swap bays)	Power supply	Ethernet	Available date
8671-61X	1 x Xeon® 2.67GHz	512KB	533Mhz	512MB	None	2 x Ultra320	Tower	6x10 (6 hot-swap std; 9 max)	1 fixed	Gigabit	Mar 2003
8671-6AX	1 x Xeon 2.67GHz	512KB	533Mhz	512MB	None	2 x Ultra320	Tower	6x10 (6 hot-swap std; 9 max)	2 hot-swp	Gigabit	Mar 2003
8671-71X	1 x Xeon 2.8BGHz	512KB	533Mhz	512MB	None	2 x Ultra320	Tower	6x10 (6 hot-swap std; 9 max)	1 fixed	Gigabit	Mar 2003
8671-7AX	1 x Xeon 2.8BGHz	512KB	533Mhz	512MB	None	2 x Ultra320	Tower	6x10 (6 hot-swap std; 9 max)	2 hot-swp	Gigabit	Mar 2003
☞ 8671-81X	1 x Xeon 3.06GHz	512KB	533Mhz	512MB	None	2 x Ultra320	Tower	6x10 (6 hot-swap std; 9 max)	1 fixed	Gigabit	May 2003
☞ 8671-8AX	1 x Xeon 3.06GHz	512KB	533Mhz	512MB	None	2 x Ultra320	Tower	6x10 (6 hot-swap std; 9 max)	2 hot-swp	Gigabit	May 2003

Positioning	*Universal server; two-way server using the Xeon processor to provide power and performance at an affordable price*
Processor(s)	**1 x Intel® Xeon™ Processor 2.67, 2.8B or 3.06 GHz** with 533MHz frontside bus / Hyper-Threading technology
L2 cache	**512KB** / on die of processor / at processor speed (no L3 cache)
SMP support	**2-way SMP** / up to two Xeon Processors (same speed/cache size)
Implementation	Systemboard contains two Intel 603-pin micro-PGA ZIF sockets, six memory gold-connector DIMM slots, six PCI slots (two hot-swap Active™ PCI slots), and integrated SCSI, ethernet, graphics
Memory	**512MB** std / 12GB max / two slots used / four slots available **PC2100** 266MHz registered 184-pin ECC DDR-SDRAM DIMMs DIMMs must be installed in matched pairs [a bank] / 2-way memory interleave / dual channel / memory bus runs at 2x100MHz / **Error Checking and Correcting (ECC)** via **16-bit Checksum Chipkill™** (corrects 1, 2, 3, or 4-bit errors on same chip and detects 2- through 8-bit errors contained in two chips) / Chipkill requires all 256MB or higher x4 DIMMs
SCSI disk controller	**LSI Logic® 53C1030 / dual channel Ultra320 SCSI controller** (LVD 320MB/sec) / on planar / 64-bit 100MHz PCI-X / supports **RAID-1 mirroring** with up to one hot-spare disk / shared with optional IBM ServeRAID™-5i Controller for low-cost RAID 0, 1, 1E, 5, 00, 10, 1E0, 50 (installed only in Slot 4)
SCSI channels	Two 16-bit channels / *SCSI Channel A:* 16-bit 68-pin LVD cable from controller to backplane; *Channel B:* 16-bit 68-pin interface for Bay 8 and 9 (may require a cable) or with optional 3-Pack Kit (cable included); supports external SCSI devices via external SCSI knockout in rear (cable req 32P8164) or via opt ServeRAID adapter with external connector(s)
IDE controller / cable	Enhanced IDE ATA-100 controller in CSB5 South Bridge / one connector on planar / one 1-drop IDE cable (CD-ROM)
Disk - capacity	None standard / supports 7200-15000 rpm disks / one backplane / all disk bays Ultra320-enabled
Disk - bays	Six hot-swap / 80-pin SCA-2 connectors / three additional hot-swap bays with Kit 33P2751 for up to nine 15K rpm disks
Mechanical	Tower / conversion to or EIA 19" Rack (5U[4]) via optional kit for support in IBM NetBAY™ Racks
Chipset	**ServerWorks® Grand Champion™ 4.0 LE** / CMIC LE Host Bridge (memory controller and I/O Bridge) / two CIOB-X2 I/O Bridges (IMB2 bus to Host Bridge for PCI-X 1.0 Bus B with slots 2, 3, 4 and Ultra320 and ethernet controllers; IMB2 bus to Host Bridge for PCI-X 1.0 Bus C with slots 5 and 6) / CSB5 South Bridge (Thin IMB to Host Bridge for PCI 2.2 bus A with slot 1 and graphics controller, EIDE, USB, SMBus, LPC bus to Super I/O) / NS PC87417 Super I/O
Ethernet controller	10/100/1000 gigabit / Broadcom® BCM 5703 / on planar / PCI-X 64-bit 100MHz / full duplex / Wake on LAN® / Alert Standard Format
CD-ROM / diskette	48X-20X[6] CD-ROM / IDE / 1.6" HH; *Diskette:* 3.5" 1.44MB diskette drive / dust cover
Rear ports	*Rear:* two USB (Vers 1.1), keyboard, mouse, parallel, **two** serial (9-pin),graphics (DB-15), ethernet (RJ-45), two RJ-45 (sys mgmt)
Front port / graphics	*Front:* one USB (Vers 1.1); *Graphics:* SVGA / ATI® Rage XL / on planar / 8MB SDRAM std/max / 32-bit 33MHz PCI 2.2 Bus
Security	Power-on password / administrator password / hinged and lockable front door to cover disk bays, power button, and reset button / unattended boot / selectable boot
Systems mgmt	**IBM Integrated system management processor** (ISMP) / H8S2148 / on planar / provides system and environmental monitoring such as temp, optional disks, fans, power supp / supports optional Remote Supervisor Adapter with 20-pin connector on planar for continuous power (no ext pwr reqd)
Diagnostics	**Light Path Diagnostics™** panel providing LED map to failing part (under side cover) / Information LED Panel in front
Software	**ServerGuide™** (CD-ROM installation and configuration utilities), IBM Director, others
Keyboard / mouse	IBM 101-key keyboard / IBM mouse (both black)
Power supply	*8xX:* std/max: one/two 660 watt (3.06Ghz Procs Only) *Rest:* std/max: one/two 560 watt *All:* voltage-sensing / auto-restart / fan in each power supp
Fans	Four fans and two blowers / variable speed / hot-swap / redundant / PFA / fan in each power supply

Xeon 2.67GHz/512KB L2 Cache Proc Upg	71P8966
Xeon 2.8BGHz/512KB L2 Cache Proc Upg	71P8967
Xeon 3.06GHZ/512KB L2 Cache Proc Upg	02R1988
256MB PC2100 CL2.5 ECC DDR-SDRAM DIMM	33L5037
512MB PC2100 CL2.5 ECC DDR-SDRAM DIMM	33L5038
1GB PC2100 CL2.5 ECC DDR-SDRAM RDIMM	33L5039
2GB PC2100 CL2.5 ECC DDR-SDRAM RDIMM	33L5040
IBM ServeRAID-5i Controller (adapter for slot 4)	25P3492
IBM Remote Supervisor Adapter (PCI adapter)	09N7585
IBM T541 15" Flat Panel Color Monitor (black)	9512AB1
36.4GB 15K-2 80 Ultra320 SCSI Hot-Swap SL HDD	06P5776
3-Pack Ultra320 Hot-Swap Expansion Kit	33P2751
IBM 560W Hot-Swap Power Upgrade Kit*	02R1874
IBM 660W Hot-Swap Power Upgrade Kit (3.06 Only)	02R2015

Other options at **ibm.com**/pc/us/accessories
*Not backward compatible with 400Mhz FSB x235

Slot 1: full, 32-bit 33MHz 5v PCI 2.2, Bus A
Slot 2: full, 64-bit 100MHz 3.3v PCI-X, not hot, Bus B
Slot 3: full, 64-bit 100MHz 3.3v PCI-X, not hot, Bus B
Slot 4: full, 64-bit 100MHz 3.3v PCI-X, not hot, Bus B*
Slot 5: full, 64-bit 133MHz 3.3v PCI-X, hot-swap, Bus C
Slot 6: full, 64-bit 133MHz 3.3v PCI-X, hot-swap, Bus C
* Extended slot for opt IBM ServeRAID-5i Controller



Tower

Bay ① 3.5", SL 1", access, diskette
Bay ② 3.5", SL 1", access, hot-swap
Bay ③ 3.5", SL 1", access, hot-swap
Bay ④ 3.5", SL 1", access, hot-swap
Bay ⑤ 3.5", SL 1", access, hot-swap
Bay ⑥ 3.5", SL 1", access, hot-swap
Bay ⑦ 3.5", SL 1", access, hot-swap
Bay ⑧ 5.25", HH 1.6" access, open**
Bay ⑨ 5.25", HH 1.6" access, open**
Bay ⑩ 5.25", HH 1.6" access, CD-ROM

Bays 2 through 7 support 6 SL disks via SCA-2 connectors.
**Bays 8 and 9 support three 3.5" disks via 3-Pack Kit 33P2751

- Quick release adapter slots (no screws)
- Configuration/Setup Utility invoked by pressing F1 at startup
- LSI Logic Configuration Utility near startup by pressing CTRL+C
- Diagnostics (PC-Doctor™) by pressing F2 at startup
- ACPI 2.0-compliant
- Operator Information Panel (in front)
- Predictive failure analysis on disk options, memory, processors, VRMs, power supplies, and fans in conjunction with IBM Director can alert the system administrator of an imminent component failure
- Tower: H 17.31" x W 8.5" x D 27.6"
- 74 to 101 pounds
- Stealth black color

All models: Max int disk capacity: 1.321TB[2] with nine 146.8GB SL disks with 3-Pack Ultra160 Hot-Swap Expansion Kit

LIMITED WARRANTY[3]

- **3 year parts and labor**
- **International Warranty Service[3]**
- **On site, 8 am - 5 pm, Mon - Fri coverage excluding holidays, next business day response time[7]**
- **3 year on site warranty service upgrade options (in eligible locations):[7]**
  - **9 hour coverage, Mon-Fri excluding holidays, 4 hour average response** (ServicePac® part num 21P2083)
  - **24 hr x 7 day coverage, 4 hour average response** (ServicePac part number 21P2084)
  - **24 hr x 7 day coverage, 2 hour average response** (ServicePac part number 21P2085)
- **24x7[14] toll-free support for warranty issues during the warranty period[3]**

See footnotes for important warranty information • = Hot-swap
☞ US models announced May 13, 2003; others February 18, 2003

35

TPC Transaction Processing Performance Council

The TPC defines transaction processing and database benchmarks and delivers trusted results to the industry.

- Home
- Results
- Benchmarks
  - TPC-C
  - **Results**
  - Description
  - FAQ
  - TPC-H
  - TPC-R
  - TPC-W
  - Obsolete
  - TPC-A
  - TPC-B
  - TPC-D
- Technical Articles
- Related Links
- What's New
- About the TPC
- Who We Are
- Member Login

TPC-C Result Highlights

IBM eServer xSeries 235 1P c/s

Benchmark Stats

Result ID:	103071001
Result Status:	In Review
TPC-C Rev:	5.1
Report Date:	07/10/03

System Information

Total System Cost	46,539 US $
TPC-C Throughput	18,936
Price/Performance	2.46 US $
Availability Date	07/10/03
Database Manager	Microsoft SQL Server 2000 Standard Ed.
Operating System	Microsoft Windows Server 2003 Standard Edition
Transaction Monitor	Microsoft COM+

Server Information

CPU:	Intel Xeon DP 3.06GHz
# of CPUs:	1
Cluster:	N

Client Information

# of clients:	1
CPU:	Intel Xeon DP 2.4GHz
CPUs per client:	1

- Executive Summary (242 KB)
- Full Disclosure Report (1492 KB)

top

Home Results Benchmarks Technical Articles Related Links What's New

About the TPC Who We Are Privacy Policy About Pricing

United States

Select a country

← Personal computing
Accessories & upgrades
Services
Support
ThinkVantage Technologies
Presentations
News & awards
Library
Request a Catalog

Shopping help
Warranty info
Shop by part number
View cart
Open saved carts
Estimate shipping
Estimate leasing
Order status
Returns policy
Shopping guarantee

Related links:
Home / home office
Small & Medium Business
Government
Education

IBM xSeries 3.06GHz/533MHz - 512 KB L2 Cache Xeon Processor

@server

IBM Web Price
$1,099.00*
Availability: **Within 2 weeks****

Add to cart

This 3.06GHz Intel Xeon processor with 533MHz front-side bus speed helps deliver processing power, throughput and headroom for peak performance to your application-intensive xSeries systems. It features the new Intel NetBurst microarchitecture, which helps increase overall throughput via a 533MHz system bus and enhanced 512KB Level 2 cache. It also features new Hyper-Threading technology which allows it to execute more than one thread per processor. These advances increase the throughput of your server applications and enable outstanding scalability for Internet infrastructure and mail servers. These enhancements can add up to faster response times, support for more simultaneous users and increased transaction workloads. This processor is designed to provide performance headroom for unpredictable server workloads and escalating computing needs. Coupled with DDR memory, this processor delivers the processing power and headroom to accommodate unexpected peaks in server workloads.

Features and Benefits:

Allows your IT the capability to expand the number of processors on a system as the workload and number of users grows
Targeted for middleware applications that power e-businesses and data centers
533MHz system bus transfers information from the processor to the rest of the system at a rate up to four times faster than the 133MHz system bus used on Pentium III processors. Also, provides increased bandwidth to route traffic on front end of Internet, preventing the bus from becoming a bottleneck.
NetBurst microarchitecture and Hyper-Threading technology help provide enhanced performance, throughput and scalability for multiprocessing server applications on xSeries servers

General	
Model name	02R1988
Description	IBM xSeries 3.06GHz/533MHz - 512 KB L2 Cache Xeon Processor
IBM Web Price*	$1,099.00
Compatibility	
Product approvals/certifications	UL-1950, NOM 018, ICES-003 Class A (Canada), FCC Class A - Part 15, CSA C22.2 No. 950
Characteristics	
Processor (CPU)	Intel® Xeon™
Processor internal clock speed	3.06 GHz
Processor manufacturer	Intel®

Add to cart

*Price does not include tax or expedited shipping and is subject to change without notice. Reseller prices may vary. IBM does not warrant non-IBM products. PCs shown here, except for Servers and Network Stations, ship with an operating system. All offers subject to availability. IBM reserves the right to alter product offerings and specifications at any time without notice. IBM is not responsible for photographic or typographic errors.

** An estimated ship date will be included with your order confirmation e-mail. Availability does not determine when your order will ship since inventory status may change before your order is final (following the receipt of any credit or payment authorization) as other orders are processed. "In stock" indicates we currently have at least one of the item in stock. Orders are normally held until all the products on the order are in inventory. "Within 2 weeks" indicates that the product should be available in inventory within 2 weeks. "Within 2-4 Weeks" indicates that the product should be available in inventory in 2-4 weeks. To obtain the latest information about the availability of a specific part number, please call 1-888-SHOP-IBM.

Important Legal Information

40

IBM 512 MB PC2100 CL2.5 ECC DDR SDRAM DIMM

IBM Web Price
$305.00*
Availability: **In stock****

Add to cart

This Double Data Rate (DDR) memory option allows you to execute up to twice the number of operations per cycle than traditional SDRAM memory. This can effectively double the data exchange rate between memory and processors, allowing customers to retrieve and process information faster and more efficiently.
Faster speed memory does not necessarily mean faster system performance, especially when combined with the latest Intel Xeon processor technology. For example, the new Intel Xeon processors require 400MHz memory data transfer rates, but the 400MHz transfer rate is actually performed using dual 100MHz double data rate clocks. The technique of combining dual 100MHz clocks and double data rate transfers delivers 400MHz data transfer rates. DDR memory is typically used for servers that require high-density packaging to optimize rack space.

Features and Benefits:

Optimizes customer floor space requirements when used in a high-density server package
Performs two operations per clock speed while DRAM performs one operation per clock speed
Yields about a 6-8% performance gain over SDRAM memory

General	
Model name	33L5038
Description	IBM 512 MB PC2100 CL2.5 ECC DDR SDRAM DIMM
IBM Web Price*	$305.00
Compatibility	
Hardware prerequisites (System unit)	xSeries 235, xSeries 345, xSeries 225, IntelliStation Z Pro (6221)
Characteristics	
Memory capacity	512 MB
Memory type	PC2100 DDR SDRAM
Form factor	DIMM
Warranty	
Limited Warranty period	Three year
Type of Service	Customer Carry-in Exchange

Add to cart

41

*Price does not include tax or expedited shipping and is subject to change without notice. Reseller prices may vary. IBM does not warrant non-IBM products. PCs shown here, except for Servers and Network Stations, ship with an operating system. All offers subject to availability. IBM reserves the right to alter product offerings and specifications at any time without notice. IBM is not responsible for photographic or typographic errors.

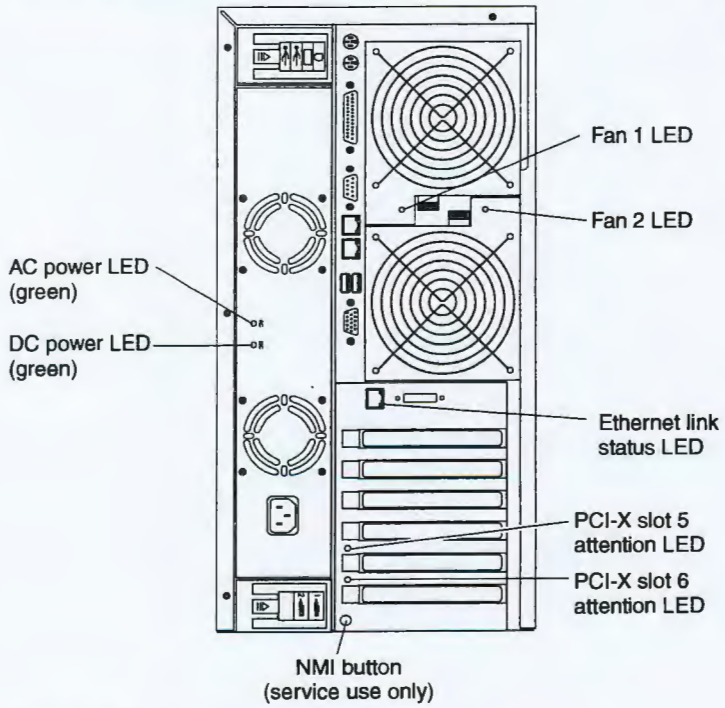
** An estimated ship date will be included with your order confirmation e-mail. Availability does not determine when your order will ship since inventory status may change before your order is final (following the receipt of any credit or payment authorization) as other orders are processed. "In stock" indicates we currently have at least one of the item in stock. Orders are normally held until all the products on the order are in inventory. "Within 2 weeks" indicates that the product should be available in inventory within 2 weeks. "Within 2-4 Weeks" indicates that the product should be available in inventory in 2-4 weeks. To obtain the latest information about the availability of a specific part number, please call 1-888-SHOP-IBM.

Important Legal Information

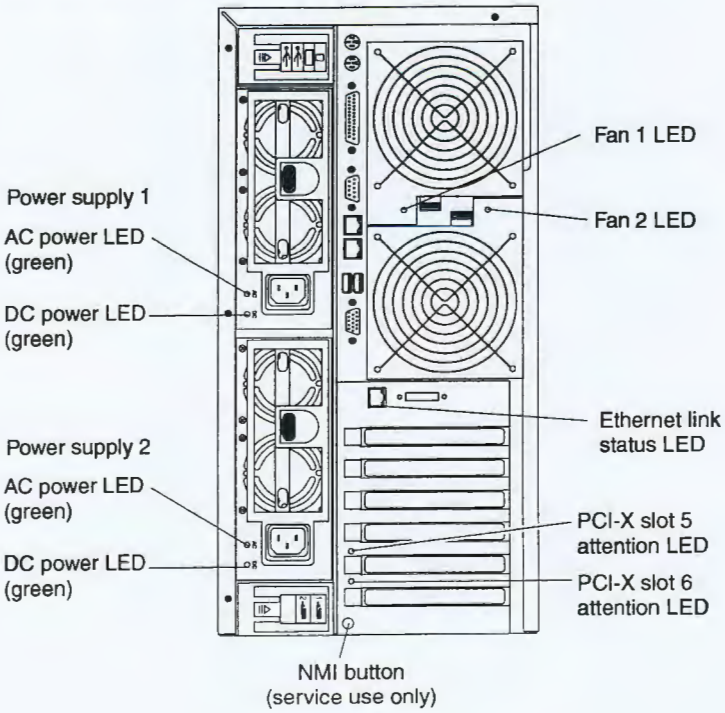
Rear view

This section identifies the indicators on the rear of your server. The following illustrations contain most of these indicators. The remaining indicators are illustrated in the "Working with adapters" section in the *Option Installation Guide* on the IBM *xSeries Documentation* CD.

Server with fixed power supply



Server with hot-swap power supplies



Features and specifications

The Table 1 provides a summary of the features and specifications for your server.

Table 1. Features and specifications

Microprocessor:
- Intel Xeon™, 1.8 GHz or higher depending on server model
- 512 KB (minimum) Level-2 cache
- 400 MHz or 533 MHz front-side bus (FSB) depending on server model
- Support for up to two microprocessors
  Note: You can use the Configuration/Setup program in your server to determine the specific type of microprocessor on your system board.

Memory:
- Standard: 256 MB or 512 MB, depending on server model, expandable to 6 GB
- Type: 133 MHz/266 MHz, registered, ECC, double data rate, SDRAM
- Sizes: 128 MB, 256 MB, 512 MB, or 1 GB, in pairs
- Connectors: two-way interleaved, six dual inline memory module (DIMM) connectors
- Maximum: Three pairs of DIMMs

Drives standard:
- Diskette: 1.44 MB
- CD-ROM: IDE

Expansion bays:
- Six open hot-swap, slim-high, 3.5-inch drive bays
- Three 5.25-inch bays (CD-ROM drive installed in one bay)
- One 3.5-inch removable-media drive bay (diskette drive installed)

PCI expansion slots:
- Two Active PCI-X™ (hot-plug) 133 MHz/64-bit
- Three PCI-X non-hot-plug 100 MHz/64-bit
- One PCI non-hot-plug, 33 MHz/32-bit

Upgradeable microcode:
BIOS, diagnostics, and IBM integrated system management upgrades (when available) can update EEPROMs on the system board

Predictive Failure Analysis® (PFA) alerts:
- Power supplies
- Fans
- Memory
- Hard disk drives
- Microprocessors
- Voltage regulator modules (VRMs)

Integrated functions:
- IBM integrated system management processor (ISMP)
  - Service processor with Light Path Diagnostics™
  - RS-485 (ASM interconnect)
  - Support for IBM Remote Supervisor Adapter
- Broadcom 5703 10/100/1000 Ethernet controller (one port, controller on system board)
- One serial port
- One parallel port
- Two internal Ultra320 SCSI ports (dual-channel integrated SCSI controller with RAID capabilities on the system board)
- Three Universal Serial Bus (USB) v1.1 ports (one on the front and two on the rear of the enclosure)
- Keyboard port
- Mouse port
- ATI Rage XL video (controller on system board)
  - Compatible with SVGA and VGA
  - 8 MB video memory

Security features:
- Door and side cover lock
- Power-on and administrator passwords
- Remote-control security settings
- Selectable drive startup
- Keyboard password
- System-management security
  - User login password
  - Read-only or read/write access
  - Dial-in call-back

Power supplies:
- Hot-swap (some models)
  - Standard: Two 560 watts (115-230 V ac) for redundancy
  - Redundant/nonredundant indicator on diagnostic LED panel
- Non-hot-swap (some models)
  - Standard: One 560 watts (115-230 V ac)
  - Upgradeable to two hot-swap power supplies

Acoustical noise emissions:
- Sound power, idle: 6.5 bel
- Sound power, operating: 6.5 bel
- Bystander sound pressure, idle: 49 dBa
- Bystander sound pressure, operating: 49 dBa

Redundant cooling:
Six hot-swap fans

Electrical input:
- Sine-wave input (50-60 Hz) required
- Input voltage range automatically selected
- Input voltage low range:
  - Minimum: 100 V ac
  - Maximum: 127 V ac
- Input voltage high range:
  - Minimum: 200 V ac
  - Maximum: 240 V ac
- Input kilovolt-amperes (kVA) approximately:
  - Minimum: 0.1 kVA
  - Maximum: 0.8 kVA

Power available for drives:
- +5 V dc
- +12 V dc

Heat output:
Approximate heat output in British thermal units (Btu) per hour
- Minimum configuration: 341 Btu (100 watts/hour)
- Maximum configuration: 2600 Btu (760 watts/hour)

Environment:
- Air temperature:
  - Server on: 10° to 35°C (50° to 95°F) Altitude: 0 to 2134 m (7000 ft)
  - Server off: -40° to +60°C (-40° to 140°F) Maximum altitude: 2133 m (7000 ft)
- Humidity:
  - Server on: 8% to 80%
  - Server off: 8% to 80%

Size (tower model):
- Height: 440 mm (17.3 in.)
- Depth: 700 mm (27.5 in.)
- Width: 221 mm (8.7 in.)
- Weight: 33.5 kg (74 lb) to 45.8 kg (101 lb) depending upon configuration

Size (5 U) (rack configuration):
- Height: 216 mm (8.5 in.)
- Depth: 674 mm (26.5 in.)
- Width: 440 mm (17.3 in.)
- Weight: 33.5 kg (74 lb) to 45.8 kg (101 lb) depending upon configuration

IBM United States

Search

Home | Products & services | Support & downloads | My account | Call 1-888-SHOP-IBM

Select a country

← Personal computing

Accessories & upgrades

Services

Support

ThinkVantage Technologies

Presentations

News & awards

Library

Request a Catalog

Shopping help

Warranty info

Shop by part number

View cart

Open saved carts

Estimate shipping

Estimate leasing

Order status

Returns policy

Shopping guarantee

Related links:

Home / home office

Small & Medium Business

Government

Education

73.4GB 10K Ultra 160 SCSI Hot Swap SL HDD

IBM Web Price
$639.00 *
Availability **In stock****

eserver

Add to cart

Your TeleWeb Hotline!
888-SHOP-IBM x 7000
Call for express sales service!

Take advantage of IBM's latest SCSI hard disk drive (HDDs) technology with optional high- speed, high-density 10,000rpm Ultra160 SCSI slim-line HDDs in hot-swap xSeries servers and IntelliStation workstations.
These 3.5-inch, hot-swap HDD options can double xSeries storage capacities for those who need high-speed data storage for demanding enterprise server and workstation applications. These HDDs store a tremendous amount of data in a slim-line form factor. This optimizes the storage capacities of supported servers, while providing excellent storage subsystem performance.

Features and Benefits:

10,000rpm HDDs -- Deliver solid reliability and excellent performance
Ultra160 SCSI interface -- wide bandwidth for streaming data transfers
Available in hot-swap version:
- Converged hot-swap drive tray -- Supports xSeries servers,
Netfinity servers, IntelliStation workstations, and EXP storage units with hot-swap bays
Predictive Failure Analysis (PFA) -- Can alert you of a problem before it occurs

General	
Model name	06P5756
Description	73.4GB 10K Ultra 160 SCSI Hot Swap SL HDD
IBM Web Price*	$639.00
Compatibility	
Hardware prerequisites (System unit)	xSeries 220, xSeries 330, xSeries 232, xSeries 225, xSeries 230, xSeries 240, xSeries 250, xSeries 340, xSeries 342, xSeries 350, xSeries 360, xSeries 370, xSeries 440, xSeries 235, xSeries 255, xSeries 345
Characteristics	
Predictive failure monitor	Yes
Drive interface type	Ultra160 SCSI
Storage capacity	73.4GB
Buffer size	8 KB
Seek time	4.9 ms
Platter RPM	10000
Interface bus	SCSI
Form factor	SL
Weight	1.3 lbs
Height	1 inches
Width	4 inches
Depth	5.75 inches
Hard disk	
Average latency	2.99 ms
Warranty	
Limited Warranty period	--
Type of Service	--

47

Add to cart

*Price does not include tax or expedited shipping and is subject to change without notice. Reseller prices may vary. IBM does not warrant non-IBM products. PCs shown here, except for Servers and Network Stations, ship with an operating system. All offers subject to availability. IBM reserves the right to alter product offerings and specifications at any time without notice. IBM is not responsible for photographic or typographic errors.

** An estimated ship date will be included with your order confirmation e-mail. Availability does not determine when your order will ship since inventory status may change before your order is final (following the receipt of any credit or payment authorization) as other orders are processed. "In stock" indicates we currently have at least one of the item in stock. Orders are normally held until all the products on the order are in inventory. "Within 2 weeks" indicates that the product should be available in inventory within 2 weeks. "Within 2-4 Weeks" indicates that the product should be available in inventory in 2-4 weeks. To obtain the latest information about the availability of a specific part number, please call 1-888-SHOP-IBM

Important Legal Information

Select a country

Select a language

Personal computing support

Search PC support

Warranty

Automated solutions

Online assistant

Submit a question

Discussion forums

Support phone list

Site feedback

Site help

Related links:

Business Partner support

IBM PC Institute

IBM Publications Center

Find a Business Partner

IBM Supports Microsoft Service Packs

ServeRAID-4Mx, -4Lx Ultra160 SCSI Controllers - Overview

Applicable countries and regions

Printable

- ServeRAID Files & Drivers

At a glance

The advanced ServeRAID-4Mx and -4Lx Ultra160 SCSI controllers, updated to 66MHz PCI bus performance, deliver excellent performance, scalability, and control for mid- and entry-range storage environments.

- New offerings join the popular ServeRAID-4 family to provide:
  - Compatibility with current line
  - Same ease-of-use and setup features
  - Common support requirements across the enterprise
- High-performance features include:
  - Wide band-width
  - Supports 64- or 32-bit PCI installations
  - High-speed, 66 MHz PCI bus performance
  - Supports Ultra160 SCSI technology - 160 MB/s data transfers
- Industry-leading RAID support - levels 0, 00, 1, 1E, 1E0, 5, 50, 5E, and 10
- IBM X-architected Active PCI
- Supports clustering and failover
- Excellent price/performers for basic- to moderate- RAID data storage
- Three-year, limited warranty

Warranty

- 3 year Customer Carry-In/Exchange

This product replaces

- Not applicable

This product was replaced by

- Not applicable

Packaging

You will receive one box containing the following items:

- Controller card assembly
- ServeRAID support CD-ROM
- ServeRAID User's Guide/Warranty

Product marketing and replacement part numbers (FRU)
Worldwide

Description	Marketing part number	Replacement part number(FRU)
ServeRAID 4Mx	06P5736	Adapter - 06P5737 Battery - 37L6903
ServeRAID 4Mx (Japan)	06P5738	Adapter - 06P5739 Battery - 00N9561
ServeRAID 4Lx	06P5740	Adapter - 06P5741

Product dates
Worldwide

- Announce date: 22 May 2001
- Planned availability date: 30 May 2001
- Withdrawal date: N/A
- Effective withdrawal date: N/A

Technical specifications
Physical, environmental, and compatibility specifications as known at time of announcement

- ServeRAID-4Mx Ultra160 SCSI Controller:
  - Up to 66 MHz PCI bus speed
  - 64-bit, full-length PCI adapter card
  - Two VHDCI .8 mm external connectors
  - Two internal, industry standard, 68-pin connectors
  - Two RAID channels
  - Supports Ultra160 SCSI (160 MB/s)
- ServeRAID-4Lx Ultra160 SCSI Controller:
  - Up to 66 MHz PCI bus speed
  - 64-bit, half-length PCI adapter card
  - One VHDCI .8 mm external connector
  - One internal, industry standard, 68-pin connector
  - One RAID channel
  - Supports Ultra160 SCSI (160 MB/s)

The above Ultra160 SCSI controllers are backward compatible with legacy SCSI modes:

- Wide Ultra2 SCSI (80 MB/s)
- Wide Ultra SCSI (40 MB/s)
- Fast/Wide SCSI (20 MB/s)

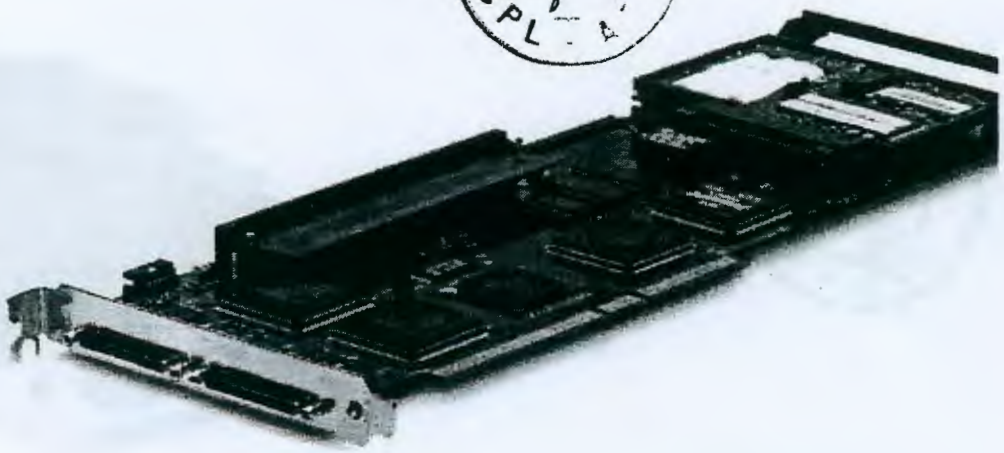
Operating temperature

- Between 10 to 35 degrees C (50 to 95 degrees F) at 0m to 914m (0 to 3,000 ft.)
- Between 10 to 32 degrees C (50 to 90 degrees F) at 914m to 2,133m (3,000 to 7,000 ft.)

Relative humidity

- Operating: between 8% and 80%

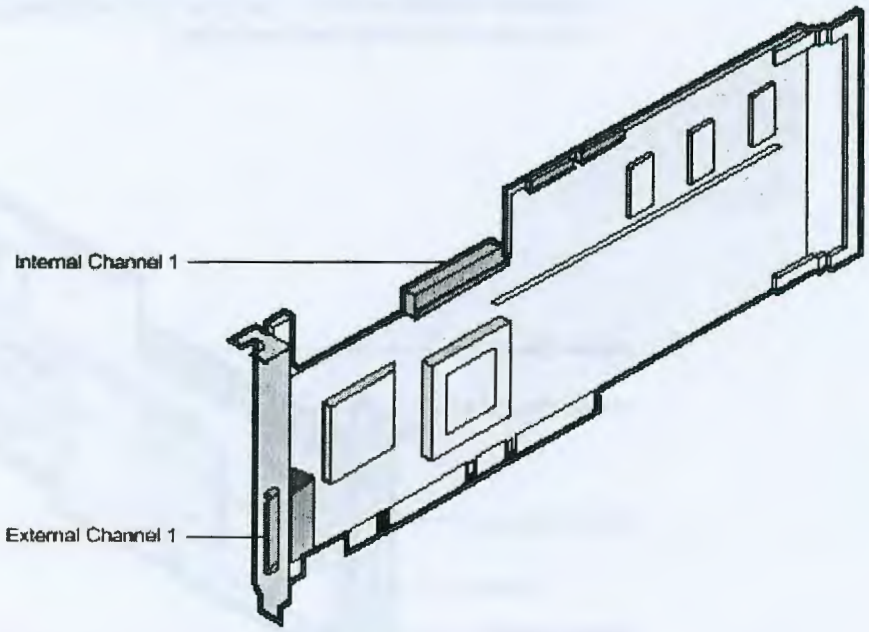
50



ServeRAID-4L (part 37L6091, 2000)

Key identifiers:

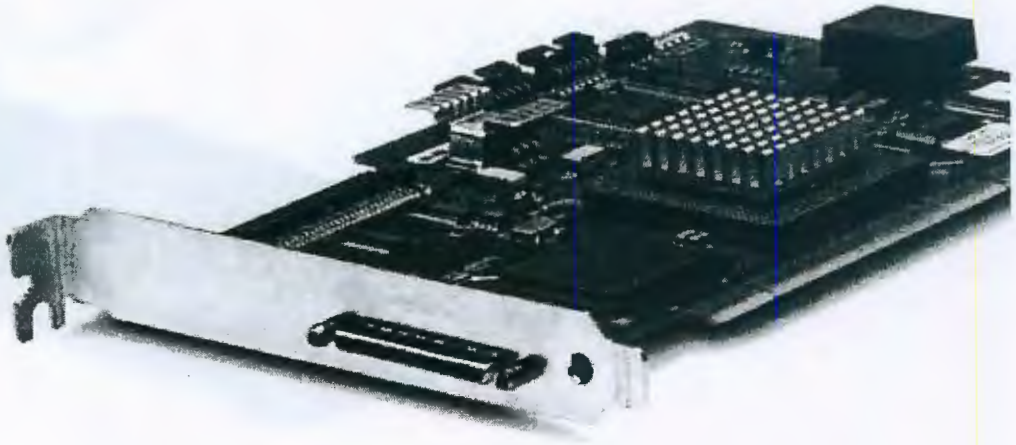
- One external VHDCI connector
- One internal 68-pin industry-standard SCSI connector
- Space for two internal connectors, but only one present (same circuit board as tl



ServeRAID-4Lx (part 06P5740, 2001)

Key identifiers:

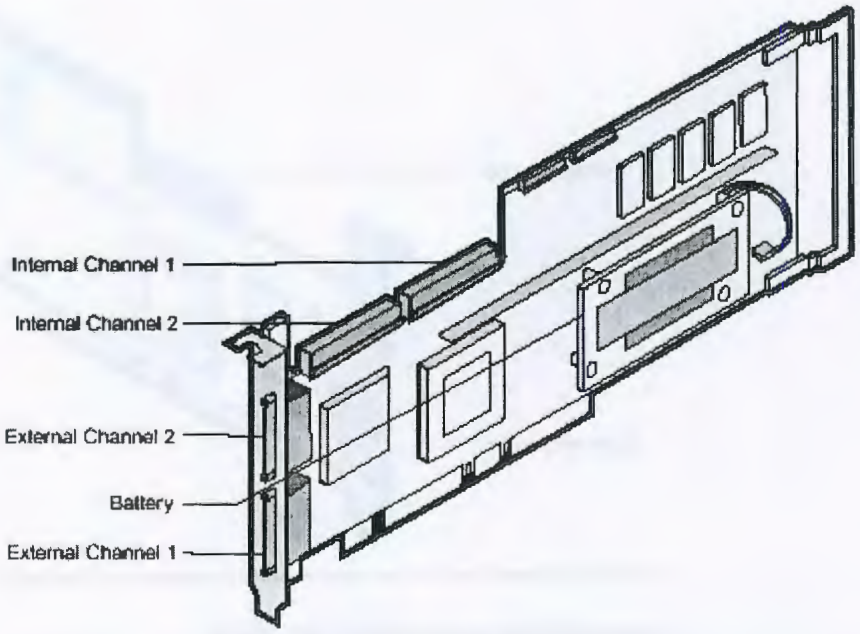
- Half-length card
- Square heat sink in the middle of the card
- One external VHDCI connector
- One internal 68-pin industry-standard SCSI connector
- 64-bit PCI connector (long)



ServeRAID-4M (part 37L6080, 2000)

Key identifiers:

- Two external VHDCI connectors
- Two internal 68-pin industry-standard SCSI connector
- Battery integrated into a daughter card lengthwise along card, near handle
- No heat sinks (4Mx has heat sinks)

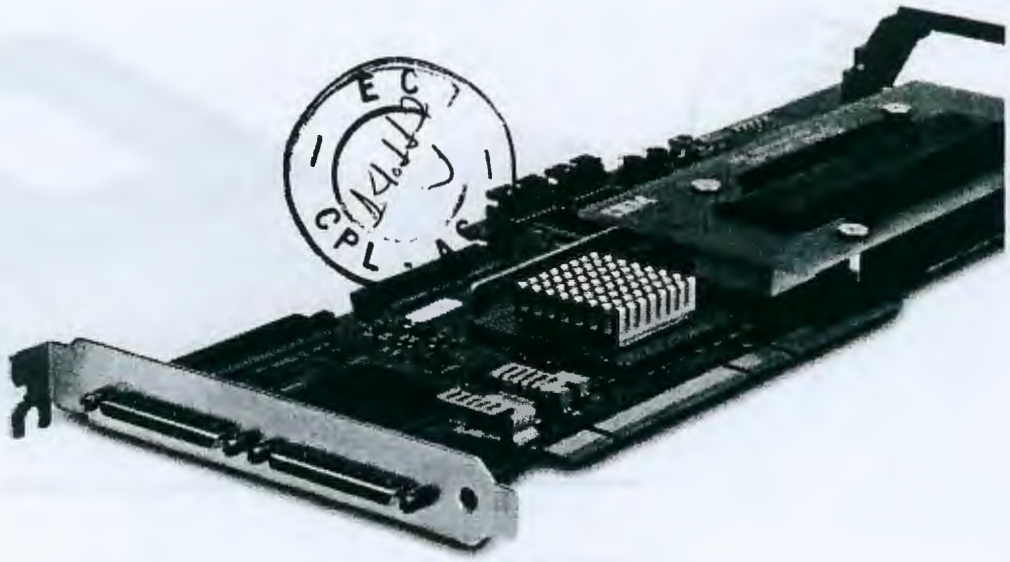


ServeRAID-4Mx (part 06P5736, 2001)

Key identifiers:

- Similar to ServeRAID-4M (check for heat sinks)
- Two external VHDCI connectors

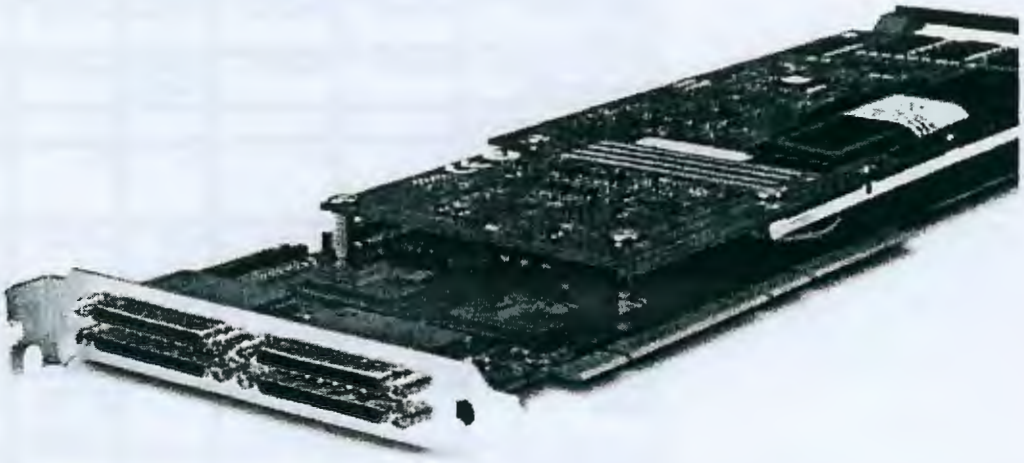
- Two internal 68-pin industry-standard SCSI connector
- Battery integrated into a daughter card lengthwise along card, near handle
- Heat sink on central chip and smaller chip near PCI connector



ServeRAID-4H (part 37L6889, 2000)

Key identifiers:

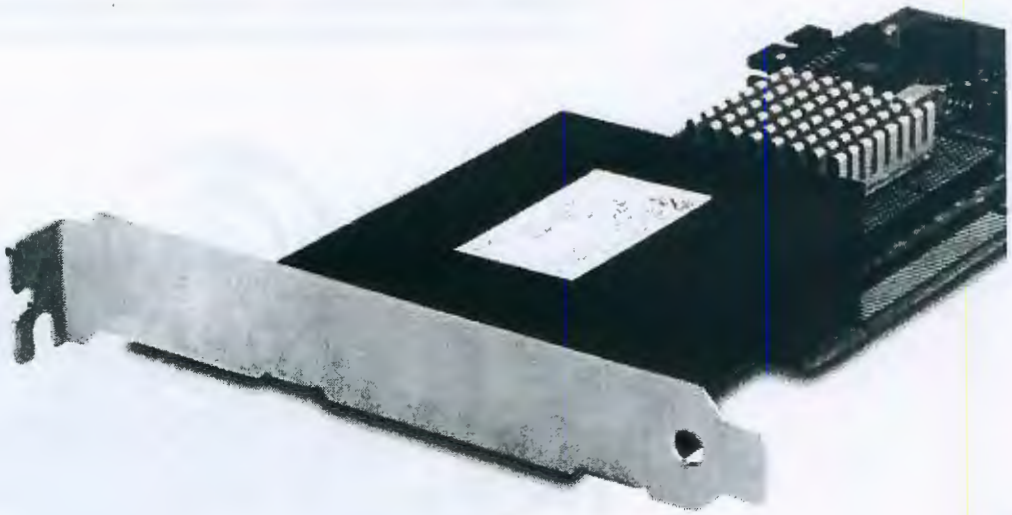
- Four external VHDCI connectors
- Two internal 68-pin industry-standard SCSI connectors
- Large daughter card with battery attached to the main board



ServeRAID-5i (part 25P3492, 2002)

Key identifiers:

- No internal or external SCSI connectors (uses the server's onboard SCSI)



Feature comparison

The following table provides a comparison of features between the members of the Se

Feature	SR	SR-II	SR-3L	SR-3H	SR-3HB	SR-4L	SR-4Lx	SR-4M
Codename	Copperhead	Copperhead Refresh	Clarinet Lite	Clarinet	Clarinet	Morpheus Lite	Neo Lite	Morpheu
First available	1996	1997	1998	1998	1999	2000	2001	2000
US Announcement Letter	196-134	197-256	198-232	198-232	199-152	100-099	101-146	100-099
Marketing part number	70G8489	76H3584	01K7364	01K7207	37L6086	37L6091	06P5740	37L608(
FRU part number (adapter only)	06H9334	76H3587	37L6083 01K7352	01K7396	01K7396	09N9540	06P5741	37L725E
Internal connectors	3	3	1	1	1	1	1	2
External connectors (std/max)	1/1	2/3	1/1	2/3	2/3	1/1	1/1	2/2
Cable for extra external connector	None	Optional 76H5400	None	Included	Included	None	None	None
External connector type	68 pin	VHDCI	VHDCI	VHDCI	VHDCI	VHDCI	VHDCI	VHDCI
Cache	4 MB	4 MB	4 MB	32 MB	32 MB	16 MB	32 MB	64 MB
Battery backup for cache	No	Optional 76H5401 28L1003	No	Optional 28L1003 (Poseidon)	Yes (Poseidon)	No	No	Yes
SCSI channels	3	3	1	3	3	1	1	2
Disks per channel	15	15	15	15	15	15	14	15
SCSI level	SCSI F/W	Ultra	Ultra2	Ultra2	Ultra2	Ultra160	Ultra160	Ultra160
PCI bus speed	33 MHz	33 MHz	33 MHz	33 MHz	33 MHz	33 MHz	66 MHz	33 MHz
PCI bus width	32 bit	32 bit	32 bit	64 bit	64 bit	64 bit	64 bit	64 bit
PCI bus voltage	5V	5V	5V	5V	5V	3.3 or 5V	3.3 or 5V	3.3 or 5V
Autosync	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
"Optimal" SCSI	No	No	Yes	Yes	Yes	Yes	Yes	Yes

setting								
LVDS support	No	No	Yes	Yes	Yes	Yes	Yes	Yes
I_2O enabled	No	No	Yes	Yes	Yes	Yes	Yes	Yes
Active PCI support	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Usable in a fault tolerant pair	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Data scrubbing	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Flashcopy	No	No	Yes	Yes	Yes	Yes	Yes	Yes
RAID-0, 1, 1E, 5 support	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
RAID-5E support	No	No	Yes	Yes	Yes	Yes	Yes	Yes
RAID-00 support	No	No	No	No	No	Yes	Yes	Yes
RAID-10 support	No	No	No	No	No	Yes	Yes	Yes
RAID-1E0 support	No	No	No	No	No	Yes	Yes	Yes
RAID-50 support	No	No	No	No	No	Yes	Yes	Yes

Special Notices

← Servers
Intel processor-based servers
Rack-optimized
Universal
High-performance scalable
Blade servers
Storage
Systems Management
Accessories & upgrades
Services
Support
Certification
Education and training
News and awards
Literature
HW/SW compatibility
Solutions

Shopping help
Warranty info
Shop by part number
View cart
Open saved carts
Estimate shipping
Estimate leasing
Order status
Returns policy
Shopping guarantee

Related links:
Home / home office
Small & Medium Business
Government
Education

IBM TotalStorage FC2-133 Host Bus Adapter

eserver

IBM Web Price
$1.485.00*
Availability: **In stock****

Add to cart

This host bus adapter option is a 64-bit, low-profile adapter that supports auto-sensing for 1Gbps or 2Gbps operations on point-to-point FC-AL-2 and switched fabric topologies with FC SCSI (FCP) and IP protocols. It provides a full 133 MHz, PCI-X based solution incorporating improved storage interoperability, broad heterogenous host and NOS support. This option attaches FAStT Storage Servers to IBM eServer xSeries and other Intel-based servers.

Features and Benefits:

Features integrated adapter management software
Implements the latest 2Gb and PCI-X technologies
Operates in any PCI or PCI-X slot
Backward compatible with previous generations of FAStT host bus adapters

General	
Model name	24P0960
Description	IBM TotalStorage FC2-133 Host Bus Adapter
IBM Web Price*	$1,485.00
Compatibility	
Hardware prerequisites (System unit)	xSeries 250, xSeries 300, xSeries 330, xSeries 340, xSeries 350, xSeries 370
Memory	
Memory (RAM) std	--
Power management	
Sound emissions	
Warranty	
Limited Warranty period	Three year
Type of Service	Customer Carry-In Exchange

Add to cart

*Price does not include tax or expedited shipping and is subject to change without notice. Reseller prices may vary. IBM does not warrant non-IBM products. PCs shown here, except for Servers and Network Stations, ship with an operating system. All offers subject to availability. IBM reserves the right to alter product offerings and specifications at any time without notice. IBM is not responsible for photographic or typographic errors.

** An estimated ship date will be included with your order confirmation e-mail. Availability does not determine when your order will ship since inventory status may change before your order is final (following the receipt of any credit or payment authorization) as other orders are processed. "In stock" indicates we currently have at least one of the item in stock. Orders are normally held until all the products on the order are in inventory. "Within 2 weeks" indicates that the product should be available in inventory within 2 weeks. "Within 2-4 Weeks" indicates that the product should be available in inventory in 2-4 weeks. To obtain the latest information about the availability of a specific part number, please call 1-888-SHOP-IBM.

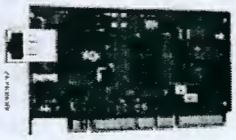
Important Legal Information

57

NetXtreme 1000 T Ethernet Adapter

$139.00 IBM List Price

Part Number: **31P6301**



This single-port Ethernet adapter option helps deliver high-performance network connections for your IBM eServer xSeries server and is designed to help reduce system I/O bottlenecks in high-performance networking applications. This adapter offers a low-profile form factor for 2U servers and the latest 133MHz PCI-X interface to help achieve higher throughput and lower CPU utilization

Features & Benefits:

- Support for Full Smart Load Balancing for optimized bandwidth and failover for fault tolerant environments
- Flexible architecture, which matches the hardware behavior to the operating system, is designed to help allow higher data throughput and increased CPU performance.
- Higher data throughput offers better utilization of the whole network and contributes to lower latencies for the applications.
- Lower CPU utilization enables the server to execute applications faster when communicating over the network.

Technical Details

Characteristics

Interface bus:	PCI-X
Adapter/Device form factor:	Halfsize
Data rates:	
Wiring type(s):	CAT-5
Connectors:	RJ45
Status LED:	Yes
Supported standards:	IEEE 802.3u, IEEE 802.3, IEEE 802.1p, IEEE 802.1Q VLAN Tagging, IEEE 802.3x, DMI 2.X, Wired for Management (WfM) baseline 2.0, Wired for Management (WfM) baseline 1.1, SNMP, PCI 2.1, IEEE 802.3z, IEEE 802.3x FCOFDL, PXE 2.X, SMBus 2.X, PCI-X, PCI 2.2, IEEE 802.3ad, IEEE 802.3ab
Supported protocols:	NETBEUI, Collision Sense Multiple Access/Collision Avoidance, 802.2 NetBios, IPX/SPX, IPX, IP, TCP/IP
SMP:	Yes
LAN Client:	Yes
Wake on LAN:	Yes
Full duplex:	Yes
Remote program load (RPL):	Yes
Cables:	
Compatible networks:	Gigabit Ethernet
Data/address width:	64bit
Data transfer rates (Burst):	
Other Information:	

Compatibility

Restrictions:	
Hardware prerequisites:	
System Units	
_ IBM Systems:	
_ Non-IBM systems:	
Operating system requirements:	

Adapters:	
Mounting kit etc.:	
Supported software:	
Product approvals/certifications4:	BSMI (Taiwan), VCCI, UL, MIC (Korea), FCC, CE, C-Tick
Energy Star Compliant:	No

Warranty [3]

Limited Warranty period and type:	Three year Customer Carry-in Exchange

Weight & Dimensions [6]

Weight:	.167lbs
Travel weight:	--
Height:	6.6in
Width:	2.54in
Depth:	.55in
Operating Temperature (C) (low; high):	0; 55
Relative Humidity (%) (low; high):	5; 95
Ship Information	--
Box 1	
Weight:	
Height:	--
Width:	--
Depth:	--
Box 2	--
Weight:	
Height:	--
Width:	--
Depth:	--
Special ship information:	

▶ Important Legal Information

- TBI (SERDES style) Transceiver interfaces
- Jumbo frames (9KB) – BCM5705 and Netware 5.1 do not support Jumbo Frames
- Layer 2 Priority Encoding (802.1P)
- Dual, High–Speed On–Chip RISC Processors
- Adaptive interrupt frequency
- Programmable rule checking and frame classification
- Up to 16 classes of service (CoS) (4 if no external memory)
- Up to 16 Distribution Rings (4 if no external memory)
- Integrated 96KB Frame Buffer Memory
- GMI/MII Management Interface
- 16M external SSRAM address space
- Selectable memory protection for external (on–board) memory
- Statistics for SNMP MIB II, Ethernet like MIB, and Ethernet MIB (802.3z, Clause 30)
- Four unique MAC unicast addresses
- Support for multicast addresses via 128 bits hashing hardware function
- Serial EEPROM (5703 uses Flash)
- Support for PXE available (tested against the following programs: Linux Red Hat PXE server, Windows 2000, Intel APITEST, DOS UNDI, 3Com boot server)
- JTAG support
- PCI v2.2 32/64–Bit, 33/66 MHz Bus Interface (5700, 5701, 5703)
- PCI–X v1.0 64–bit 100 MHz Bus Interface (5701, 5703)
- PCI Power Management Interface (v1.1)
- PCI Hot Plug (IBM, Compaq, Dell, and Microsoft)
- ACPI and Wake–on–LAN Support
- 64 Bit BAR support
- 3.3 V/1.8 V CMOS with 5V tolerant I/Os

Back to Top

Physical Description

The faceplate on the 10/100/1000BASE–T adapter provides an RJ–45 connector for connecting the adapter to another network device.

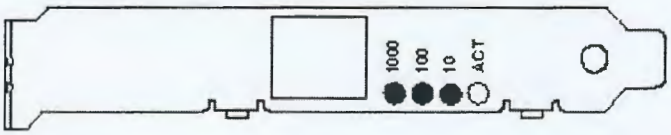


Figure 5. Broadcom NetXtreme™ Gigabit Ethernet Adapter Faceplate

The adapter faceplate has four LEDs, one for each port speed option (10 Mbps, 100 Mbps, and 1000 Mbps), and one for Activity. The three port speed LEDs indicate active links, and the ACT LED indicates data transfer status. Once the adapter is installed and the cables are connected properly, the appropriate speed LED is lit and the ACT LED is on if data traffic is present.

Once the adapter hardware has been properly installed on your system, the LEDs indicate the following adapter states:

NetBAY42 Enterprise Rack Cabinet

IBM Web Price
$2,649.00 *
Availability: **In stock****

Add to cart

New NetBAY rack cabinets provide a comprehensive selection of rugged, rack solutions tailored for "deep" servers and high-density installations. Cabinet provides 42U of rack space with depth capacity to support "deep" servers up to 28 inches. All models feature a perforated-steel front door to optimize cooling while maintaining security by lock and key. These NetBAY rack cabinets support all current rack-mountable IBM eServer xSeries and Netfinity servers.

Features and Benefits:

Includes side panels and a stabilizer kit
Robust design allows shipping with preconfigured servers
Perforated front door provides improved air flow for a fan-free environment
Lockable front and rear doors maximize security
Provides the most room of all NetBAY racks for cable management

General	
Model name	930842S
Description	NetBAY42 Enterprise Rack Cabinet
IBM Web Price*	$2,649.00
Compatibility	
Restrictions	When servicing or sliding devices out of the NetBAY42 ER or EX, it is required that the front stabilizer plate be used in accordance with the instructions included in the installation/safety publications.
Hardware prerequisites (System unit)	Netfinity 4500R, Netfinity 4500R Rack Mounted models, Netfinity 5100, Netfinity 5100 Rack Mounted models, Netfinity 5000, Netfinity 5000 Rack Mounted models, Netfinity 5500, Netfinity 5500 M10, Netfinity 5500 M10 Rack Mounted models, Netfinity 5500 M20,
Hardware prerequisites (Mounting kit etc.)	Cable requirements are dependent upon the devices installed in the NetBAY42 ER cabinets.
Product approvals/certifications	CSA C22.2 No. 950 Third Edition, IEC-950/EN 60950 Second Edition, UL-1950 Third Edition
Characteristics	
Space	42
Type of cabinet	Type A 19" (EIA standard 310-D)
Memory	
Memory (RAM) std	--
Power management	
Sound emissions	
Dimensions	
Weight	575 lbs
Height	79.5 inches
Width	25.5 inches
Depth	43.3 inches
Security	

Security features	Lockable front/rear door, Lockable side panels
Warranty	
Limited Warranty period	Three year
Type of Service	Customer Carry-in

Add to cart

*Price does not include tax or expedited shipping and is subject to change without notice. Reseller prices may vary. IBM does not warrant non-IBM products. PCs shown here, except for Servers and Network Stations, ship with an operating system. All offers subject to availability. IBM reserves the right to alter product offerings and specifications at any time without notice. IBM is not responsible for photographic or typographic errors.

** An estimated ship date will be included with your order confirmation e-mail. Availability does not determine when your order will ship since inventory status may change before your order is final (following the receipt of any credit or payment authorization) as other orders are processed. "In stock" indicates we currently have at least one of the item in stock. Orders are normally held until all the products on the order are in inventory. "Within 2 weeks" indicates that the product should be available in inventory within 2 weeks. "Within 2-4 Weeks" indicates that the product should be available in inventory in 2-4 weeks. To obtain the latest information about the availability of a specific part number, please call 1-888-SHOP-IBM.

Important Legal Information

NetBAY42 Rack Standard Expansion Cabinet

eserver

IBM Web Price
$1,439.00 *
Availability: **Within 2 weeks****

Add to cart

This 42U NetBAY rack option joins the IBM family of rugged, heavy-duty rack solutions to meet your requirements from entry to advanced-enterprise environments. It provides an excellent solution for creating rack suites to economically support multiple servers and supporting devices. This rack option contains the same features as the NetBAY42 Standard Rack with the exception that as an expansion cabinet it does not require nor include side panels. Instead of side panels, it includes rack attachment hardware as a standard feature.
This 19-inch, industry-standard rack option supports rack-mountable IBM eServer xSeries and Netfinity servers.

Features and Benefits:

Locking front and rear doors provide security
Perforated front door provides improved air flow for a fan-free environment
Improved cable management system--cable channel runs from top to bottom
Standard depth does not require purchase of a rack extension kit
Includes side panels and a stabilizer kit

General	
Model name	9306421
Description	NetBAY42 Rack Standard Expansion Cabinet
IBM Web Price*	$1,439.00
Compatibility	
Hardware prerequisites (System unit)	xSeries 200, xSeries 230, xSeries 232, xSeries 235, xSeries 255, xSeries 240, xSeries 250, xSeries 300, xSeries 340, xSeries 342, xSeries 345, xSeries 350, xSeries 360, xSeries 370, xSeries 440, IntelliStation R Pro (6851)
Product approvals/certifications	CSA C22.2 No. 950 Third Edition, IEC-950/EN 60950 Second Edition, UL-1950 Third Edition
Characteristics	
Space	25
Type of cabinet	Type A 19" (EIA standard 310-D)
Memory	
Memory (RAM) std	--
Power management	
Sound emissions	
Dimensions	
Weight	205 lbs
Height	81.7 Inches
Width	23.6 Inches
Depth	40.9 Inches
Security	
Security features	Lockable front/rear door
Warranty	

Limited Warranty period	Three year
Type of Service	Limited warranty

Add to cart

*Price does not include tax or expedited shipping and is subject to change without notice. Reseller prices may vary. IBM does not warrant non-IBM products. PCs shown here, except for Servers and Network Stations, ship with an operating system. All offers subject to availability. IBM reserves the right to alter product offerings and specifications at any time without notice. IBM is not responsible for photographic or typographic errors.

** An estimated ship date will be included with your order confirmation e-mail. Availability does not determine when your order will ship since inventory status may change before your order is final (following the receipt of any credit or payment authorization) as other orders are processed. "In stock" indicates we currently have at least one of the item in stock. Orders are normally held until all the products on the order are in inventory. "Within 2 weeks" indicates that the product should be available in inventory within 2 weeks. "Within 2-4 Weeks" indicates that the product should be available in inventory in 2-4 weeks. To obtain the latest information about the availability of a specific part number, please call 1-800-SHOP-IBM.

Important Legal Information

E74 17.0-inch (16.0-inch viewable) MPRII Color Monitor (6332) - Parts Information

The parts information matrix provides a listing of marketing part numbers, FRU replacement part numbers, and additional part numbers applicable to your monitor. For additional information, such as user's guides, downloadable files, technical specifications and images select the hot-linked description to view an overview document for this product.

- Description: A description of the product.
- Machine type/model number: The machine type (the four characters before the hyphen) and the model number (the three characters after the hyphen) used to identify the product.
- Marketing part number: The marketing part number is the part number used for purchasing the product.
- Replacement part number (FRU): The service part number for the product or one of the product's components.
- Geography: The geography where the product is available.

Monitor Part Numbers

Description	Machine type/model number	Marketing part number	Replacement part number (FRU)	Geography
E74 17.0-inch (16.0-inch viewable) Color Monitor (6332) (Stealth Black)	6332-4LE	31P8136	31P8138	Brazil, Paraguay, Uruguay
E74 17.0-inch (16.0-inch viewable) Color Monitor (6332) (Stealth Black)	6332-4LE	31P8137	31P8138	Argentina

Miscellaneous Part Numbers

Description	Replacement part number (FRU)	Used with the following machine type/model numbers
E74 Tilt/Swivel Stand (Stealth Black)	31P8139	6332-4LE

Applicable countries and regions

Argentina, Brazil, Paraguay, Uruguay

Back to top

Documen
Product ca
Hardwa
Monitor
CRT Mo
E Series
6332
4LE
Version:
1IHT16\
Reference
MIGR-4
IBM Group
PSG Su
Service
Modified d
2002-07

Does this
provide y
informati
Yes
Is the lan
understa
Yes
Please pr
comments
improve t

Document id: MIGR-42789
Last modified: 2002-07-02

we cannot site.

E74 17.0-inch (16.0-inch viewable) MPRII Color Monitor (6332) Latin America - Overview

Related links:

IT product training

IBM Redbooks

Sales manual

Announcement letters

Software support handbook

Developers

IBM Business Partners

- Parts Information
- Publications
- Files
- Images

At A Glance

Features:

- Stealth black version
- A 17.0-inch FST (Flatter Squarer Tube) CRT with a viewable image size of 16.0 inches (406 mm), incorporating a 0.27 mm diagonal dot pitch and a 0.23 mm horizontal dot pitch
- A maximum horizontal frequency of 70 kHz for flicker-free operation at a recommended addressability of 1024 x 768 pels at 85 Hz with a maximum addressability of 1280 x 1024 pels at 60 Hz
- Video Electronics Standards Association (VESA) Display Data Channel (DDC) capability for plug and play and asset tracking for DDC-enabled attaching system unit hardware and software
- Meets the ENERGY STAR guidelines for energy efficiency
- Timings for the VESA 85 Hz refresh rate display modes for 640 x 480, 720 x 400, 800 x 600, and 1024 x 768 addressabilities
- Minimum Swedish MPR-II compliance

Warranty

3 year Limited - customer carry-in exchange

This product was replaces:

A70 17.0-inch FST Color Monitor (6632-0AE and 6632-4AE)

Packaging

You will receive one box containing the following items:

- E74 monitor with attached video signal cable
- Tilt-swivel stand
- Power cord
- Setup Guide
- Warranty and Safety Booklet
- Compact Disk containing E74 Users Guide and monitor installation files

Product dates

Documen
Product ca
Hardwa
Monitor
CRT Mo
E Series
6332
4LE
Version:
1IHT16V
Reference
MIGR-4
IBM Group
PSG Su
Service
Modified d
2002-07

Does this provide y informati

Yes

Is the lan understa

Yes

Please pr comments improve tl

Your respo to improve content. Re assistance submitted normal sup

we cannot site.

Worldwide

- Announce date: 04 Jun 2002
- Planned availability date: June 2002

Technical specifications

Physical, environmental, and compatibility specifications as known at time of announcement

Weight

- 31.8 lbs (unpacked)
- 14.4 kg (unpacked)
- 37.5 lbs (packed)
- 17.0 kg (packed

Height

- 15.6 inches (unpacked) *
- 395 mm (unpacked) *
- 18.3 inches (packed)
- 465 mm (packed)

Width

- 15.7 inches (unpacked)
- 400 mm (unpacked)
- 19.5 inches (packed)
- 496 mm (packed)

Depth

- 16.5 inches (unpacked)
- 420 mm (unpacked)
- 22.6 inches (packed)
- 573 mm (packed)

* Includes tilt/swivel stand

Power requirements

- Input voltage: 90 to 264 V ac (Universal Voltage)
- Frequency: 50/60 Hz
- Heat dissipation (Maximum): 341 btu/hr
- Power consumption (Maximum): < 100 watts
- Power consumption (Normal Use): < 5 watts
- Maximum earth leakage current: - <3.5 mA at 264 V ac, 50 Hz
- Maximum earth leakage current: - <1.0 mA at 115 V ac, 60 Hz

Actual power consumption depends on the screen mode used, the images displayed, and how user controls are set.

Operating parameters

- Temperature: between 0 degrees Celsius and 40 degrees Celsius

72

IBM Sleek 2-Button Mouse - Stealth Black (PS/2)

IBM Web Price
$14.95*
Availability: **In stock****

Add to cart

The IBM Sleek Mouse provides precision that fits in your hand. This easy-to-install mouse has a simple, natural shape and 400DPI for comfort and control. In modern Stealth Black color, this is the perfect all-purpose mouse.
The IBM Sleek Mouse is fully compatible with IBM-compatible computers with a PS/2 (mini-din)-style mouse port.y

General

Model name	28L3673
Description	IBM Sleek 2-Button Mouse - Stealth Black (PS/2)
IBM Web Price*	$14.95

Compatibility

Restrictions	Does not meet ESD CB-2-0001-024 standard
Hardware prerequisites (System unit)	PC 300, PC 300GL, PC 300PL, PC 300XL, ThinkPad 240, ThinkPad 310, ThinkPad 365, ThinkPad 380, ThinkPad 385, ThinkPad 390, ThinkPad 560, ThinkPad 570, ThinkPad 600, ThinkPad 760, ThinkPad 765, ThinkPad 770, ThinkPad i Series, ThinkPad A Series, ThinkPad T
Hardware prerequisites(Adapters)	--
Hardware prerequisites (Mounting kit etc.)	--
Supported software	Microsoft Windows NT, Microsoft Windows 3.1, Microsoft Windows 95, Microsoft Windows 98, IBM OS/2 3.0 or later, DOS 5.0 or later
Product approvals/certifications	BCIQ, C-Tick, CE, CSA No. 950, EMI (Korea), FCC Class B (US), GS (Germany), ICES-003 Class B (Canada), IEC-801.2-4, IEC-950/EN 60950 Second Edition, MOC, NMB-003 Class B (Canada), NOM 019, UL-1950 Third Edition, VCCI

Characteristics

Type	
Number of keys	2
Keyboard - pointing device	--
Keyboard - connector	PS/2 6-Pin mini-DIN
Weight	.3 lbs
Height	1.44 inches
Width	2.44 inches
Depth	4.5 inches

Warranty

75

Limited Warranty period	One year
Type of Service	Customer Carry-in Exchange (CCE)

Add to cart

*Price does not include tax or expedited shipping and is subject to change without notice. Reseller prices may vary. IBM does not warrant non-IBM products. PCs shown here, except for Servers and Network Stations, ship with an operating system. All offers subject to availability. IBM reserves the right to alter product offerings and specifications at any time without notice. IBM is not responsible for photographic or typographic errors.

** An estimated ship date will be included with your order confirmation e-mail. Availability does not determine when your order will ship since inventory status may change before your order is final (following the receipt of any credit or payment authorization) as other orders are processed. "In stock" indicates we currently have at least one of the item in stock. Orders are normally held until all the products on the order are in inventory. "Within 2 weeks" indicates that the product should be available in inventory within 2 weeks. "Within 2-4 Weeks" indicates that the product should be available in inventory in 2-4 weeks. To obtain the latest information about the availability of a specific part number, please call 1-888-SHOP-IBM.

Important Legal Information

IBM DPI Universal Rack PDU with Nema L5-20P and L6-20P (US lines)

IBM Web Price
$179.00*
Availability: **In stock****

Add to cart

Features and Benefits:

Features connector-linking components rather than country specific hardware
Designed to plug directly into appropriate wall outlets or for use with the innovative DP Interconnect Front-End PDUs.
Breaker-protected outlets help keep loads safe from catastrophic power events

General	
Model name	32P1736
Description	IBM DPI Universal Rack PDU with Nema L5-20P and L6-20P (US lines)
IBM Web Price*	$179.00
Compatibility	
Product approvals/certifications	TUV-GS - ZH/618, UL 1950 First Edition, VCCI Class A (Japan), CISPR-22 Class A, CNS-13438 (Taiwan), CSA C22.2 No. 950, FCC Class A - Part 15, ICES-003 Class A (Canada), IEC-60950 Certificate/Report, NOM 018, TUV-GS - EN60950, BSMI (Taiwan), C-Tick Mark (
Characteristics	
Height	1.63 inches
Width	8.76 inches
Depth	4.51 inches

Add to cart

*Price does not include tax or expedited shipping and is subject to change without notice. Reseller prices may vary. IBM does not warrant non-IBM products. PCs shown here, except for Servers and Network Stations, ship with an operating system. All offers subject to availability. IBM reserves the right to alter product offerings and specifications at any time without notice. IBM is not responsible for photographic or typographic errors.

** An estimated ship date will be included with your order confirmation e-mail. Availability does not determine when your order will ship since inventory status may change before your order is final (following the receipt of any credit or payment authorization) as other orders are processed. "In stock" indicates we currently have at least one of the item in stock. Orders are normally held until all the products on the order are in inventory. "Within 2 weeks" indicates that the product should be available in inventory within 2 weeks. "Within 2-4 Weeks" indicates that the product should be available in inventory in 2-4 weeks. To obtain the latest information about the availability of a specific part number, please call 1-888-SHOP-IBM.

Important Legal Information

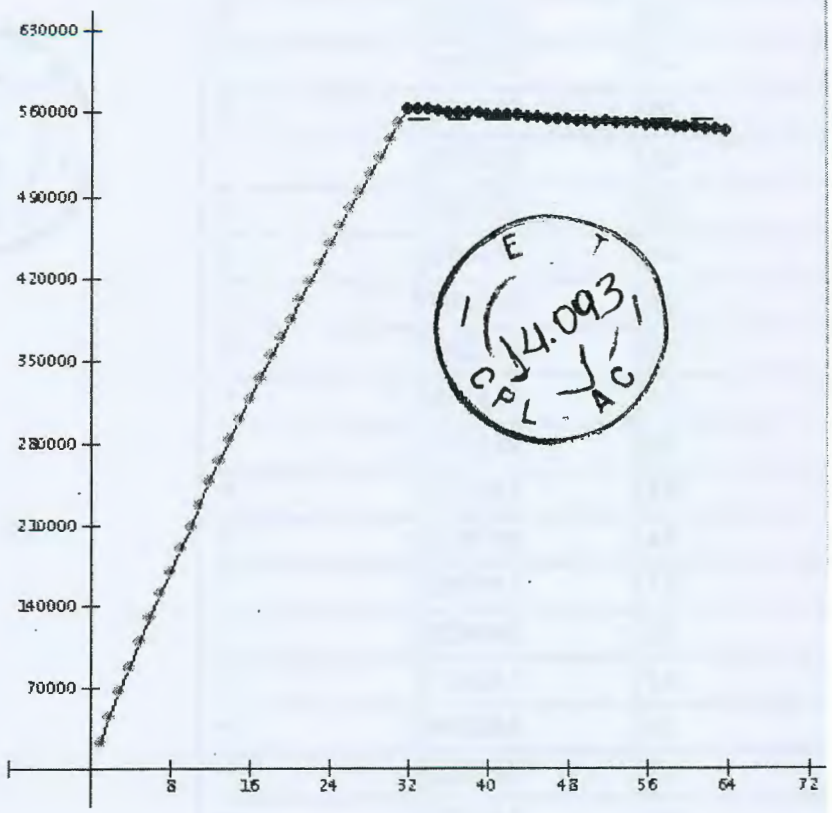
SPECjbb2000

SPECjbb2000 = 553480 ops/s

BM Corporation IBM eServer pSeries 690 Turbo

BM Corporation J2RE 1.4.1 IBM AIX build cadev-20030522 (32 bit JVM)

Warehouses	Ops/s	Incl. in metric
1	22804	
2	44503	
3	66229	
4	87630	
5	108703	
6	128866	
7	149201	
8	169104	
9	189545	
10	207830	
11	227330	
12	246724	
13	264446	
14	282471	
15	300338	
16	316965	
17	334273	
18	352065	
19	367941	
20	383434	
21	399804	
22	416397	
23	431476	
24	447427	
25	463319	
26	478113	
27	493329	
28	508333	
29	521535	
30	536641	
31	551079	
32	563160	*
33	562677	*
34	561633	*
35	561493	*
36	559722	*
37	558643	*



38	558779	*
39	558887	*
40	558134	*
41	557395	*
42	557110	*
43	556617	*
44	555901	*
45	555450	*
46	554050	*
47	553585	*
48	553470	*
49	552807	*
50	552268	*
51	551188	*
52	551713	*
53	550622	*
54	549825	*
55	549963	*
56	549429	*
57	548917	*
58	548396	*
59	547222	*
60	546478	*
61	546342	*
62	544885	*
63	544554	*
64	543511	*
PECjbb2000	**(from 32 to 64)**	**553480 ops/s**

PEC license # 11 | **Tested by:** IBM Corporation | **Test date:** Jun 23, 2003

Hardware	
ardware endor	IBM Corporation
endor RL	http://www.ibm.com
[odel	IBM eServer pSeries 690 Turbo
rocessor	POWER4+
[Hz	1700
of Procs	32
[emory MB)	65536

Software	
Software Vendor	IBM Corporation
Vendor URL	http://www.ibm.com
Java Precompiler Version	
Java Precompiler Command Line	
Java Precompiler Way Of Excluding Classes	
JVM Version	J2RE 1.4.1 IBM AIX build cadev-20030522 (32 bit JVM)
JVM Command Line	java -Xlp -Xcompactexplicitgc -Xgcpolicy:subpool -ms3072m -mx3072m -ss128k spec.jbb.JBBmain -propfile SPECjbb.props

Primary cache	64KBI+32KBD on chip
Secondary cache	1536KB unified on chip
Other cache	128MB unified (off-chip)/MCM, 4 MCMs in SUT
Filesystem	JFS
Disks	1 x 36.4GB SCSI
Other hardware	

JVM Initial Heap Memory (MB)	3072
JVM Maximum Heap Memory (MB)	3072
JVM CLASSPATH	./jbb.jar: ./jbb_no_precompile.jar: ./check.jar: ./reporter.jar
JVM BOOTCLASSPATH	/java/cadev-20030522/jre/lib/core.jar: /java/cadev-20030522/jre/lib/graphics.jar: /java/cadev-20030522/jre/lib/security.jar: /java/cadev-20030522/jre/lib/server.jar: /java/cadev-20030522/jre/lib/xml.jar: /java/cadev-20030522/jre/lib/charsets.jar: /java/cadev-20030522/jre/classes
OS Version	AIX 5L V5.2 APAR IY43549
System state	normal
Other software	

Test Information	
Tested by	IBM Corporation
SPEC license #	11
Test location	Austin, TX
Test date	Jun 23, 2003
H/w available	Jul-2003
JVM available	Oct-2003
OS available	Jul-2003
Other s/w available	

Tuning

Operating system tunings

- SPINLOOPTIME=2000
- vmo -r -o lgpg_regions=256 -o lgpg_size=16777216
- setsched -S rr -P 40 -p $$
- schedtune -t 400 -F 1
- vmtune -S 1

Notes

Details of Runs

Warehouses	Thrput	Total heap (MB)		Thread spread %	% > 120s	transaction type	Count	Time (in seconds)	
		Size	Used					total	max
1	22804	3072	30.8	<0.01%	<0.01	new_order	1189844	65.5	.019
						payment	1189837	20.8	<0.01
						order_status	118984	2.54	<0.01
						delivery	118984	9.06	<0.01
						stock_level	118984	16.2	.018
2	44503	3072	52.4	<0.01%	<0.01	new_order	2321883	130	.029
						payment	2321877	41.8	.029
						order_status	232188	5.11	<0.01
						delivery	232189	18.4	.028
						stock_level	232186	32.6	<0.01
3	66229	3072	74.9	1.15%	<0.01	new_order	3455684	195	.028
						payment	3455691	63.1	.029

						order_status	345569	7.60	.029
						delivery	345568	28.0	.026
						stock_level	345568	48.5	.029
	87630	3072	93.1	2.98%	<0.01	new_order	4572387	260	.028
						payment	4572393	84.8	.028
						order_status	457239	10.2	<0.01
						delivery	457241	36.5	<0.01
						stock_level	457238	65.1	.028
	108703	3072	114	2.07%	.019	new_order	5672563	326	.028
						payment	5672559	106	.027
						order_status	567257	12.7	.026
						delivery	567256	45.8	<0.01
						stock_level	567255	81.0	.028
	128866	3072	134	2.45%	<0.01	new_order	6724004	390	.028
						payment	6724010	127	.028
						order_status	672400	15.3	<0.01
						delivery	672399	55.7	.028
						stock_level	672401	98.1	.028
	149201	3072	156	1.99%	<0.01	new_order	7784639	456	.030
						payment	7784638	148	.030
						order_status	778461	17.8	.028
						delivery	778464	66.2	<0.01
						stock_level	778463	114	.030
	169104	3072	179	2.35%	<0.01	new_order	8823020	520	.031
						payment	8823015	169	.031
						order_status	882300	20.5	<0.01
						delivery	882301	76.5	.031
						stock_level	882304	129	.031
	189545	3072	198	1.61%	<0.01	new_order	9889863	588	.032
						payment	9889850	188	.032
						order_status	988983	22.5	<0.01
						delivery	988987	87.0	.032
						stock_level	988986	144	.032
0	207830	3072	221	1.85%	<0.01	new_order	10844109	654	.034
						payment	10844116	208	.034
						order_status	1084411	25.3	<0.01
						delivery	1084408	97.8	.034
						stock_level	1084412	159	.034
1	227330	3072	242	1.71%	<0.01	new_order	11861800	720	.037
						payment	11861807	228	.036
						order_status	1186181	28.0	<0.01
						delivery	1186179	108	.034

						stock_level	1186181	175	.037
12	246724	3072	260	1.81%	<0.01	new_order	12873649	788	.037
						payment	12873633	248	.037
						order_status	1287362	30.2	.036
						delivery	1287365	119	.037
						stock_level	1287363	189	.037
13	264446	3072	278	1.94%	<0.01	new_order	13798349	854	.039
						payment	13798353	267	.039
						order_status	1379832	32.7	.034
						delivery	1379837	130	.038
						stock_level	1379837	206	.039
14	282471	3072	300	1.25%	<0.01	new_order	14737993	923	.041
						payment	14738003	288	.041
						order_status	1473804	35.0	.041
						delivery	1473801	141	.039
						stock_level	1473798	218	.041
15	300338	3072	319	2.08%	<0.01	new_order	15671101	988	.042
						payment	15671088	307	.042
						order_status	1567109	37.8	.041
						delivery	1567112	153	.042
						stock_level	1567107	234	.042
16	316965	3072	343	2.18%	<0.01	new_order	16538699	1056	.045
						payment	16538696	326	.044
						order_status	1653871	39.8	.043
						delivery	1653865	164	.044
						stock_level	1653867	250	.045
17	334273	3072	361	1.72%	<0.01	new_order	17441805	1121	.046
						payment	17441787	346	.046
						order_status	1744182	42.1	.043
						delivery	1744179	176	.045
						stock_level	1744180	265	.046
18	352065	3072	386	1.94%	<0.01	new_order	18370156	1194	.048
						payment	18370148	364	.048
						order_status	1837015	44.1	.047
						delivery	1837017	186	.048
						stock_level	1837015	278	.049
19	367941	3072	406	1.91%	<0.01	new_order	19198519	1263	.051
						payment	19198513	383	.050
						order_status	1919851	45.9	.048
						delivery	1919851	199	.050
						stock_level	1919848	292	.051
20	383434	3072	428	2.39%	<0.01	new_order	20006116	1328	.052

						payment	20006096	407	.052
						order_status	2000612	48.8	.051
						delivery	2000614	208	.052
						stock_level	2000609	306	.052
1	399804	3072	442	1.70%	<0.01	new_order	20861086	1396	.053
						payment	20861107	426	.053
						order_status	2086104	50.9	.052
						delivery	2086112	220	.052
						stock_level	2086109	320	.053
2	416397	3072	468	1.91%	<0.01	new_order	21725607	1466	.055
						payment	21725601	445	.055
						order_status	2172562	53.5	.050
						delivery	2172553	233	.055
						stock_level	2172559	332	.055
3	431476	3072	486	2.39%	<0.01	new_order	22511974	1536	.058
						payment	22511960	464	.058
						order_status	2251195	55.6	.056
						delivery	2251200	242	.056
						stock_level	2251196	346	.058
4	447427	3072	507	1.92%	<0.01	new_order	23344984	1605	.059
						payment	23344980	482	.059
						order_status	2334502	57.3	.059
						delivery	2334496	251	.058
						stock_level	2334496	363	.059
5	463319	3072	531	2.03%	<0.01	new_order	24173555	1676	.061
						payment	24173538	501	.061
						order_status	2417353	59.9	.059
						delivery	2417351	262	.061
						stock_level	2417359	374	.061
6	478113	3072	545	2.10%	<0.01	new_order	24945443	1742	.062
						payment	24945442	520	.062
						order_status	2494541	62.0	.061
						delivery	2494544	273	.062
						stock_level	2494545	393	.062
	493329	3072	570	2.44%	<0.01	new_order	25739554	1813	.064
						payment	25739543	540	.064
						order_status	2573952	64.5	.064
						delivery	2573956	285	.064
						stock_level	2573949	405	.064
	508333	3072	591	1.56%	<0.01	new_order	26523457	1885	.067
						payment	26523472	557	.067
						order_status	2652346	66.2	.066

						delivery	2652349	294	.066
						stock_level	2652344	419	.066
29	521535	3072	611	1.73%	<0.01	new_order	27211653	1951	.068
						payment	27211646	574	.067
						order_status	2721165	69.0	.067
						delivery	2721161	309	.067
						stock_level	2721163	436	.068
30	536641	3072	629	1.70%	<0.01	new_order	28000974	2025	.069
						payment	28000987	592	.069
						order_status	2800104	70.6	.067
						delivery	2800098	318	.068
						stock_level	2800093	449	.069
31	551079	3072	652	1.78%	<0.01	new_order	28753649	2091	.071
						payment	28753642	611	.071
						order_status	2875362	73.0	.071
						delivery	2875360	329	.069
						stock_level	2875369	466	.071
32	563160	3072	675	2.68%	.031	new_order	29391300	2159	.074
						payment	29391289	629	.073
						order_status	2939132	75.0	.072
						delivery	2939132	341	.074
						stock_level	2939124	480	.074
33	562677	3072	698	3.76%	.741	new_order	29574543	2245	1.69
						payment	29574561	658	.731
						order_status	2957464	76.7	.366
						delivery	2957460	349	.425
						stock_level	2957459	502	1.16
34	561633	3072	706	9.38%	.188	new_order	29357504	2302	1.66
						payment	29357516	680	1.60
						order_status	2935754	80.8	1.35
						delivery	2935749	354	1.71
						stock_level	2935748	510	1.22
35	561493	3072	721	10.7%	.799	new_order	29529395	2368	1.77
						payment	29529400	697	1.76
						order_status	2952942	86.9	1.78
						delivery	2952944	369	1.79
						stock_level	2952944	543	1.83
36	559722	3072	744	9.72%	1.05	new_order	29509509	2444	1.96
						payment	29509504	730	1.97
						order_status	2950951	82.8	1.89
						delivery	2950959	366	1.98
						stock_level	2950952	562	1.95

	558643	3072	756	11.7%	.575	new_order	29314207	2514	2.03
						payment	29314197	758	2.03
						order_status	2931426	85.0	1.95
						delivery	2931419	381	1.91
						stock_level	2931414	557	2.02
3	558779	3072	785	9.09%	.786	new_order	29382787	2557	1.96
						payment	29382751	774	1.95
						order_status	2938280	88.8	1.88
						delivery	2938277	397	1.95
						stock_level	2938278	603	2.02
9	558887	3072	794	11.6%	.615	new_order	29338668	2615	2.05
						payment	29338683	821	1.97
						order_status	2933858	89.7	1.66
						delivery	2933863	403	1.94
						stock_level	2933863	590	2.13
0	558134	3072	818	8.08%	.798	new_order	29352258	2708	[illegible]
						payment	29352285	817	[illegible]
						order_status	2935228	97.0	1.82
						delivery	2935225	414	1.94
						stock_level	2935229	613	1.94
1	557395	3072	833	8.17%	.707	new_order	29287012	2741	1.97
						payment	29287005	871	1.97
						order_status	2928704	97.2	1.77
						delivery	2928699	415	1.96
						stock_level	2928696	645	1.97
2	557110	3072	847	9.45%	.188	new_order	29121103	2827	2.07
						payment	29121097	872	2.09
						order_status	2912107	94.8	[illegible]
						delivery	2912100	421	[illegible]
						stock_level	2912108	641	[illegible]
3	556617	3072	867	11.6%	.883	new_order	29297162	2883	2.04
						payment	29297164	914	1.78
						order_status	2929723	95.9	1.68
						delivery	2929717	420	1.74
						stock_level	2929714	697	1.98
4	555901	3072	888	15.7%	.512	new_order	29151941	2962	3.15
						payment	29151954	932	2.23
						order_status	2915198	97.1	1.67
						delivery	2915195	413	1.71
						stock_level	2915192	705	1.97
5	555450	3072	895	13.0%	.038	new_order	28991113	2937	2.23
						payment	28991109	982	1.94

						order_status	2899110	100	1.84
						delivery	2899113	424	1.74
						stock_level	2899115	753	3.23
5	554050	3072	917	10.4%	.854	new_order	29153898	3120	2.42
						payment	29153898	951	2.02
						order_status	2915380	92.6	1.76
						delivery	2915386	457	1.93
						stock_level	2915387	744	1.97
7	553585	3072	947	17.5%	1.44	new_order	29298372	3125	2.06
						payment	29298387	1048	2.06
						order_status	2929835	99.4	2.07
						delivery	2929841	440	2.03
						stock_level	2929836	810	2.31
3	553470	3072	958	20.7%	.850	new_order	29122102	3220	3.48
						payment	29122153	1026	2.71
						order_status	2912211	89.0	1.98
						delivery	2912216	442	1.90
						stock_level	2912212	803	2.04
9	552807	3072	966	12.2%	.448	new_order	28971186	3290	2.68
						payment	28971160	1019	3.22
						order_status	2897114	92.0	1.85
						delivery	2897107	438	2.29
						stock_level	2897119	862	3.07
0	552268	3072	988	23.7%	1.03	new_order	29111969	3346	3.49
						payment	29111982	1084	2.38
						order_status	2911203	98.4	1.58
						delivery	2911194	446	3.77
						stock_level	2911207	865	3.43
	551188	3072	1003	22.4%	.393	new_order	28870528	3392	3.22
						payment	28870511	1110	2.91
						order_status	2887057	108	2.00
						delivery	2887058	426	2.23
						stock_level	2887040	873	2.36
2	551713	3072	1024	18.5%	.957	new_order	29060396	3435	3.20
						payment	29060427	1143	4.80
						order_status	2906045	108	1.94
						delivery	2906044	421	2.68
						stock_level	2906045	950	2.62
3	550622	3072	1047	18.8%	.203	new_order	2878625[illegible]	[illegible]519	2.67
						payment	2878625[illegible]	4128	3.43
						order_status	2878628	97.2	1.86
						delivery	2878626	436	1.93

						payment	28643431	1455	5.20
						order_status	2864348	105	2.51
						delivery	2864343	446	3.57
						stock_level	2864341	1218	5.40
3	544554	3072	1219	45.2%	1.10	new_order	28724726	4228	8.89
						payment	28724759	1387	11.2
						order_status	2872476	110	3.30
						delivery	2872477	418	2.63
						stock_level	2872479	1246	10.2
4	543511	3072	1237	32.3%	1.93	new_order	28411688	4043	7.73
						payment	28411691	1632	7.24
						order_status	2841167	103	1.83
						delivery	2841170	441	5.15
						stock_level	2841174	1230	3.54

Manual 26

IBM Tivoli Storage Manager for Windows - Storage Agent User's Guide

IBM Tivoli Storage Manager
for Windows

Storage Agent User's Guide

Version 5.2

GC32-0785-01

Chapter 1. Storage Agent Overview

IBM Tivoli Storage Manager for Storage Area Networks is a feature of Tivoli Storage Manager that enables LAN-free client-data movement.

This feature allows the client system to directly write data to, or read data from, storage devices attached to a storage area network (SAN), instead of passing or receiving the information over the network. Data movement is thereby off-loaded from the LAN and from the Tivoli Storage Manager server, making network bandwidth available for other uses. For instance, using the SAN for client data movement decreases the load on the Tivoli Storage Manager server and allows it to support a greater number of simultaneous client connections. See Figure 1. The storage agent, a component of the feature, makes LAN-free data movement possible.

You install the storage agent on the client machine where it shares storage resources with the Tivoli Storage Manager server. A Tivoli Storage Manager server, acting as a library manager, controls the storage devices. This server may be the server working in conjunction with the storage agent or another server in the enterprise. The Tivoli Storage Manager server keeps track of the metadata that the client has stored. The metadata, such as policy information and file name and size, is passed over the LAN connection between the storage agent and server.

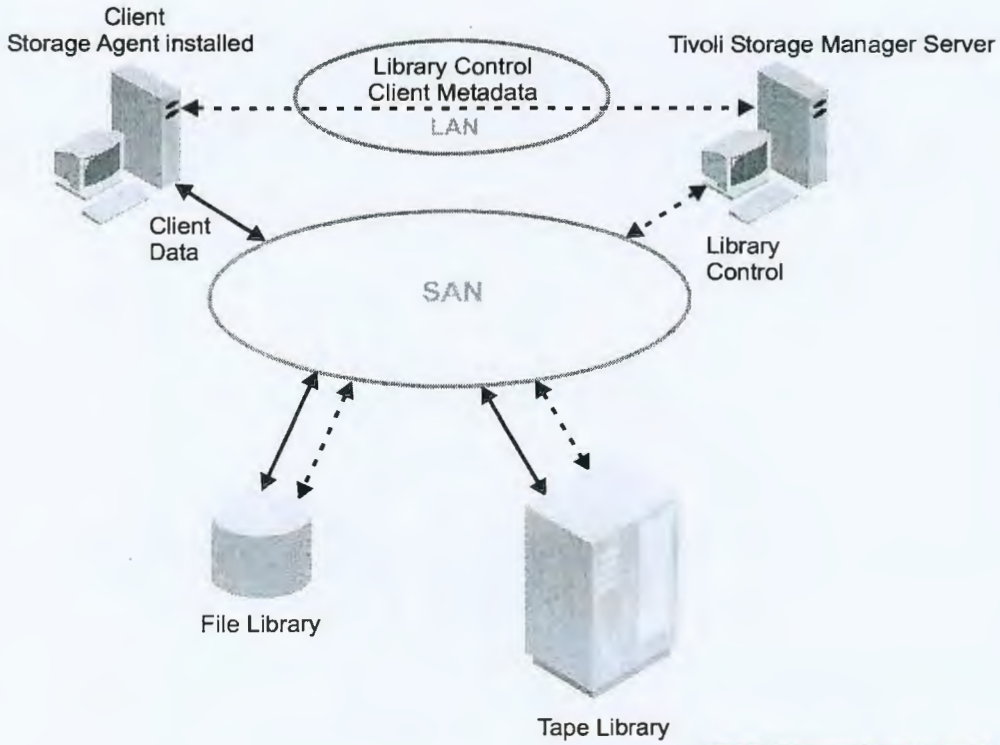


Figure 1. SAN Data Movement. Solid lines indicate data movement. Broken lines indicate movement of control information and metadata.

Manual 27

BlackBox

BLACK BOX®
NETWORK SERVICES

Black Box Corporation • 1000 Park Drive • Lawrence, PA 15055-1018 • Tech Support: 724-746-5500 • **www.blackbox.com** • **e-mail: info@blackbox.com**

SERVSWITCH™ AFFINITY

Affordable many-to-many multiplatform KVM switching.

Key Features

- ***As many as 16 users have keyboard/mouse/video control over as many as 1024 PC, Sun, RS/6000, SGI, HP, and/or Alpha computers.***
- ***With additional converters, also supports Apple computers.***
- ***Easily expandable with plug-in Port Cards and flexible cabling.***
- ***Free lifetime firmware upgrades.***
- ***Supports video resolutions up to 1280 x 1024.***
- ***High levels of security, including passwords and access profiles.***
- ***Controlled through on-screen display, with additional keyboard commands and a terminal-based serial-port options menu.***
- ***Some models have redundant power supplies.***

Is your server room growing by leaps and bounds? Wouldn't it be nice to have a keyboard/video/mouse-switching system that could keep up with all the hardware, all the users, the constant changes, and the realities of your budget?

Our ServSwitch™ Affinity could be the one. It will support most major hardware platforms, including IBM® PS/2®, PC/AT®, and RS/6000®; Sun®; SGI™; HP® 700 and 9000 series; and Compaq® Alpha™. IBM type computers can use any keyboard mode and any of a variety of mouse types. Video can be any of several types at up to 1280 x 1024 resolution. With additional adapters, you can attach Apple® Macintosh® CPUs too—see **"What else you might need"** on page 4.

You can attach as many as 16 computers to a single unit or 1024 computers to a daisychained Affinity system. Either way, you can also attach up to 4, 8, or 16 independent users; more users can be connected, but they'll have to contend for access.

Here's how it works: Each ServSwitch Affinity has four slots for Port Cards. 0 x 4 Port Cards (product code KV1300C) have four CPU (computer) ports and a serial port only; 1 x 4 Cards (KV1301C) also have a KVM (user) port.

The Affinity chassis also has a fifth, top slot used for expansion purposes; the 16-User models have a matching sixth, bottom slot. 4-User models ship with a Terminator Card (KV1304C) installed in the expansion slot; you can swap in a 4-User Expansion Card (KV1305C) if you'll be daisychaining the Affinity. 8- and 16-User models, which are designed to be part of a daisychain, come without anything installed in the expansion slot(s). You need to purchase and install an 8-User Expansion Card (KV1306C) for each slot in order for the unit to work.

The only difference between the three 4-User Affinity models with single power supplies is which Cards they're preinstalled with; see the start of **"Ordering Information"** on page 5 for a list of which Cards come with each model.

You can add capacity to your Affinity system at any time by installing Port Cards in vacant slots or adding more chassis to a daisychain.

The Port Card's serial ports are used for terminal-based initial system configuration; they are also used to upgrade the Affinity's firmware (upgrades are free for the lifetime of the Affinity!).

The ServSwitch Affinity's main controls are its on-screen menus (with a full range of configuration and operating functions). These menus are augmented by a number of keyboard commands.

For added security, the Affinity supports password-protected access groups. Computers can belong to multiple groups, but users can only belong to one. Users will only be able to access the computers in their group.

When users do access computers, they'll have one of four assigned access levels: view only (no keyboard/mouse control), share (view access until current user becomes inactive, then add keyboard and mouse), control (sole control but others can view), or private (sole control, no one else can interrupt or view).

For mission-critical applications, we offer models of the Affinity with dual, redundant power supplies. If one power supply ever fails, the other can take on the entire load until a replacement supply can be installed.

6/26/2001 #22921

Specifications

Hardware Required: Monitor that supports your computers' highest video standard; in multiplatform applications, should be multisync model that can video from either composite sync or separate horizontal/vertical sync signals

Compliance: CE, FCC Part 15 Subpart J Class A, IC Class/ classe A

Standards:
- With original Serv cabling: VGA (color or monochrome/page white) video;
- With original Serv cabling (minimal) or coaxial cabling (recommended): SVGA and (with KV99MA adapter) Mac video;
- With coaxial cabling: XGA (color or monochrome), Sun, RS/6000, or SGI video

Interfaces:
- On CPU ports and user ports of Port Cards and IN 1 and OUT 1 ports of primary Expansion Cards:
  - Proprietary composite of:
    - IBM PS/2, PC/AT, or Sun compatible keyboard;
    - PS/2, RS-232 serial (except on user ports), or Sun compatible mouse; and
    - Video (see **Standards** above);
  - With the KV99MCON converter, also supports ADB (Mac compatible) keyboard and mouse ports;
  - IN 1 and OUT 1 also carry system-control signals;
- On Expansion Cards' other IN and OUT ports: Proprietary video composite (see **Standards** above);
- On serial ports of Port Cards: EIA/TIA RS-232 proprietarily pinned on RJ-12 ("6-wire RJ-11") connectors, DTE

Resolution: Up to 1280 x 1024, but will depend on the length of CPU and User Cables in your system

Serial (RS-232) Characteristics:
- Protocol: Asynchronous;
- Data format: 8 data bits, 1 stop bit, no parity (fixed);
- Data rate: 9600 or 57,600 bps

Maximum Distance:
- 20 ft. (6.1 m) of CPU or User Cable—possibly as much as 100 ft. (30.5 m) if Cable is coaxial, depending on CPUs, monitor, and video resolution—from any Affinity Port Card to any device attached to it;
- 100 ft. (30.5 m) of Expansion Cable between any two Affinity units;
- 50 ft. (15.2 m) of serial cable from the RS-232 port of any Affinity Port Card to a computer's serial port

User Controls:
- For system: Keyboard commands and on-screen menus;
- On Affinity chassis: Rear-mounted ON/OFF rocker switch(es);
  - KV13xDA models: (2);
  - All other models: (1);
- On all Expansion Cards (KV1305C and KV1306C): Board-mounted BUS/RING jumper;
- On 8-User Expansion Cards (KV1306C): (2) Board-mounted jumper blocks for user-port numbering

Indicators:
- All models: ON/OFF switch(es) are dark when ServSwitch Affinity is OFF, backlit when Affinity is ON;
- KV13xDA models: (3) Front-mounted power-supply status LEDs:
  - (1) for supply 1 (the upper transformer), lit while supply is outputting power;
  - (1) for supply 2 (the lower transformer), lit while supply is outputting power;
  - (1) for the Affinity chassis (marked "SYSTEM"), lit while either supply is outputting power unless internal diodes have failed

Connectors:
- All rear-mounted;
- On Affinity chassis: IEC 320 male power inlet(s):
  - KV13xDA models: (2);
  - All other models: (1);
- On all Affinity Port Cards (KV1300C and KV1301C):
  - (4) DB25 female for CPU connections;
  - (1) RJ-12 ("6-wire RJ-11") female for serial management;
- On 1 x 4 Port Cards (KV1301C):
  - (1) DB25 female for user connections;
- On 4-User Expansion Cards (KV1305C):
  - (2) DB15 female: (1) for input to Port Cards in slots 1 and 2, (1) for input to Port Cards in slots 3 and 4;
  - (2) DB15 male: (1) for output from Port Cards in slots 1 and 2, (1) for output from Port Cards in slots 3 and 4
- On 8-User Expansion Cards (KV1306C):
  - (4) HD15 female:
    - (1) for input to Port Cards set as KVM 1/2 or 9/10;
    - (1) for input to Port Cards set as KVM 3/4 or 11/12;
    - (1) for input to Port Cards set as KVM 5/6 or 13/14;
    - (1) for input to Port Cards set as KVM 7/8 or 15/16;
  - (4) HD15 male:
    - (1) for output from Port Cards set as KVM 1/2 or 9/10;
    - (1) for output from Port Cards set as KVM 3/4 or 11/12;
    - (1) for output from Port Cards set as KVM 5/6 or 13/14;
    - (1) for output from Port Cards set as KVM 7/8 or 15/16

Maximum Altitude: 10,000 ft. (3048 m)

Temperature Tolerance: 32 to 113°F (0 to 45°C)

Humidity Tolerance: 5 to 80% noncondensing

Enclosure: Steel

Fuses: KV13xDA models: Autoresetting switch fuses that cut in when power surges exceed the maximum ratings of the chassis

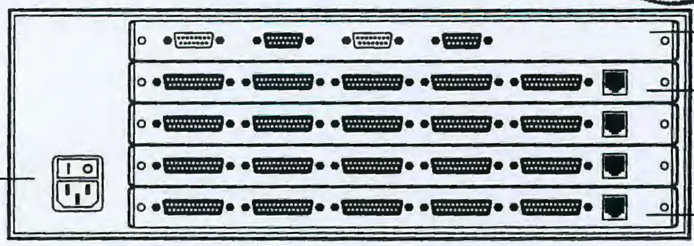
Power:
- Input: 90 to 264 VAC, 47 to 63 Hz, 700 mA from AC outlet(s) through included power cord(s) and inlet(s) into internal transformer(s):
  - KV13xDA models: Dual transformers with separate AC inlets, electrically isolated from one another;
  - All other models: Single transformer;
- Consumption: Up to 40 VA (40 watts)

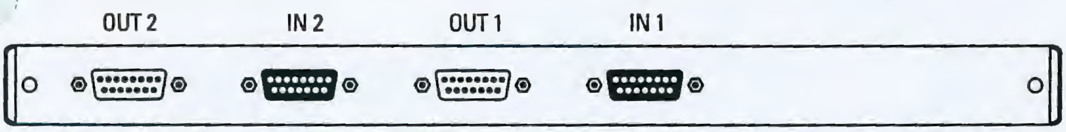
Size:
- KV139A and KV139DA chassis: 7"H (4U) x 16.7"W x 7"D (17.8 x 42.4 x 17.8 cm);
- All other Affinity chassis: 5.25"H (3U) x 16.7"W x 7"D (13.3 x 42.4 x 17.8 cm);
- Port Cards and Expansion Cards: 0.9"H x 13.9"W x 4.8"D (2.3 x 35.3 x 12.2 cm);
- Terminator Card (4-User models only): 0.4"H x 2.1"W x 0.8"D (1 x 5.3 x 2 cm)

Weight:
- KV130A, KV130DA, KV138A, and KV138DA: 10.5 lb. (4.8 kg);
- KV132A: 12 lb. (5.5 kg);
- KV134A: 14 lb. (6.4 kg);
- KV139A and KV139DA: 11 lb. (5 kg);
- KV1300C, KV1301C, and KV1306C: 0.9 lb. (0.4 kg);
- KV1304C: 0.2 lb. (0.1 kg);
- KV1305C: 0.4 lb. (0.2 kg)

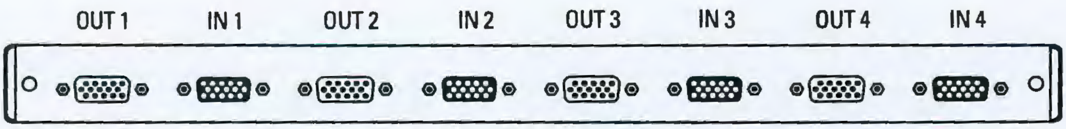
If you need to share access to a large number of CPUs, think about putting in an Affinity daisychain made up of 4-User Expansion Chassis (like the fully loaded one shown below) or 8- or 16-User Chassis. They come empty (no Cards installed), but you can install one Expansion Card (or two in the 16-User units) and add as many as four 0 x 4 or 1 x 4 Port Cards to them, giving you a maximum of four, eight, or sixteen user stations and sixteen CPUs attached to each unit. (Keep in mind that however many user stations a unit is designed for, only that many video paths can be open through that unit at a time. For example, a 4-User unit only has four video paths, so if there are already four users attached to a 4-User unit, and a user at another Affinity unit selects one of the 4-User unit's CPUs, one of the 4-User unit's users—and all other users on that slot—will be locked out until the new connection ends.)

The 8-User units look very similar to the 4-User unit shown here, but they accept only 8-User Expansion Cards like the one shown below. The 16-User Units accept two of the 8-User Expansion Cards. The 8-User Cards have jumper blocks that you can set to control which four KVM slots are used by the users attached to the Affinity chassis that the Card is installed in: KVM 1 through 4, 5 through 8, 9 through 12, or 13 through 16.





DB15 female expansion ports on 4-User Expansion Card (KV1305C)



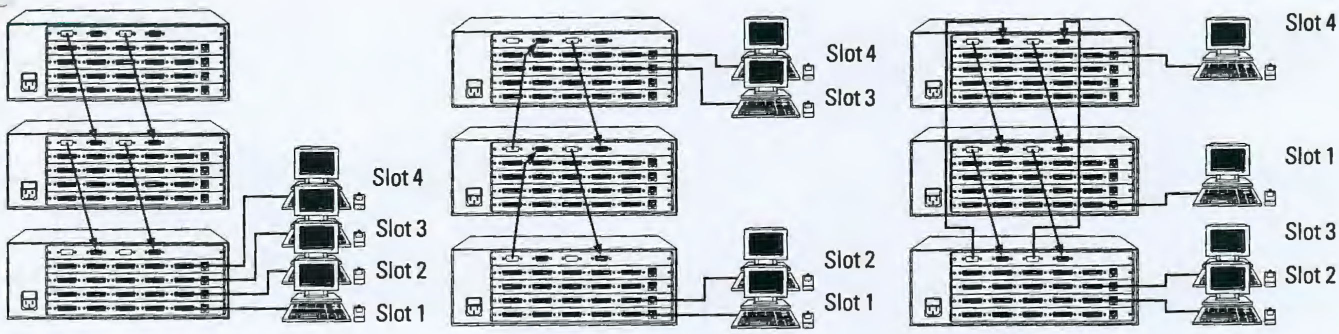
HD15 female expansion ports on 8- and 16-User Expansion Card (KV1306C)

On the 4-User Expansion Cards (above, top), IN 1 and OUT 1 carry signals for the Port Cards in slots 1 and 2, while IN 2 and OUT 2 carry signals for the Port Cards in slots 3 and 4.

On the 8-User Expansion Cards (above, bottom), IN 1 and OUT 1 carry the signals for either KVM 1 and 2 or, if installed in the bottom slot of a 16-User unit, KVM 9 and 10; IN 2 and OUT 2 cary the signals for either KVM 3 and 4 or KVM 11 and 12; and so on. A pair of jumper blocks, mentioned above, determines which four KVM slots the four users on that Affinity chassis will use.

Because the control paths are carried on different connectors this way, you have maximum flexibility for designing your daisychain layout:

- If all of your users are on one Chassis, use the regular bus topology (below, left).
- If you have two users on one Chassis and two on another, use the "split bus" topology (below, middle).
- If your users are spread across several Chassis, use the ring topology (below, right).*



Regular Bus   Split Bus   Ring

*It is always important to keep in mind that only one user at a time can use the bus that interconnects daisychained Affinity units, especially when you implement a ring topology. For example, when your Affinity units are interconnected in a ring, if any user on Slot 1 selects a CPU attached to an Affinity unit other than his own, no other Slot 1 user can select any CPUs.

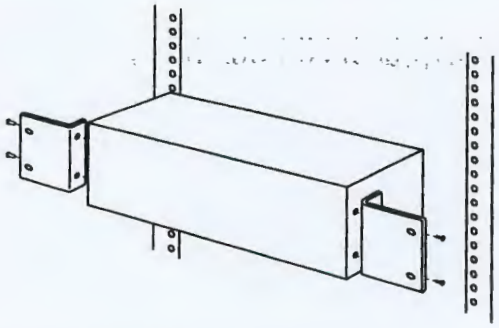
The complete package

- The ServSwitch Affinity, including any cards and blanking plates that are normally preinstalled with your model. (Blanking plates will cover all unused slots, as well as the slot on 4-User models that the tiny Terminator Card is installed in.)
- A power cord.
- *KV13xDA models only:* A second power cord.
- A 6-ft. (1.8-m) serial cable with RJ-12 ("6-wire RJ-11") plugs.
- An RJ-12 to DB9 modular adapter.
- A manual.

What else you might need

- CPU Adapter Cables, User Adapter Cables, and (if you're cascading) Expansion Cables.
- Keyboards, mice, and monitors for your users. If you're mixing platforms, we recommend true multiscan, multisync monitors capable of syncing to each CPU's video-output frequencies and compatible with all of the CPUs' video cards. Also, if one of the multiple platforms is IBM, the monitors must be able to accept both separate H/V sync and composite sync. (Such monitors are widely available.) We recommend that the monitors be able to display a maximum resolution of not less than 1280 x 1024 at a maximum refresh rate of not less than 75 Hz.
- An AC-power surge protector and uninterruptible power supply.
- Data-line surge protectors for the keyboard and mouse lines.
- *To attach an Apple Mac®:* A ServSwitch™ Micro Mac® Converter (product code KV99MCON), a G3™/G4™ or legacy Macintosh® style CPU-Extension Cable, and, if the Mac needs to see ID bits from its monitor, a Mac Video Adapter for ServSwitch (KV99MA).
- *If you purchase a 4-User Expansion Chassis or an 8- or 16-User Chassis:* Port Cards for your CPU and user-station connections.
- *To cascade a ServSwitch Affinity:* An Expansion Card.
- *To rackmount a ServSwitch Affinity:* A ServSwitch Affinity Rackmount Kit.

If you can use a screwdriver, you can install the Rackmount Kits.



Ordering Information

ITEM	CODE
ServSwitch Affinity	
4-User Expansion Chassis (Terminator Card installed, no Port Cards installed)	
Single power supply	KV130A
Dual power supply	KV130DA
4-User Standalone Chassis:	
2 Users by 8 CPUs (Terminator Card installed, 1 x 4 Port Cards installed in slots 1 and 2)	KV132A
4 Users by 16 CPUs (Terminator Card installed, 1 x 4 Port Cards installed in slots 1 through 4)	KV134A
8-User Chassis (no Cards installed)	
Single power supply	KV138A
Dual power supply	KV138DA
16-User Chassis (no Cards installed)	
Single power supply	KV139A
Dual power supply	KV139DA
Port Cards	
0 x 4 (No Users, Four CPUs)	KV1300C
1 x 4 (One User, Four CPUs)	KV1301C
4-User Terminator Card	KV1304C
4-User Expansion Card	KV1305C
8- and 16-User Expansion Card	KV1306C

Ordering Information (continued)

ITEM **CODE**

NOTE: For CPU and User Cables, specify length by adding any of these suffixes to the product code (not all cables are available in all lengths):
"-0001" for 1 ft. (0.3 m, User Cables only),
"-0005" for 5 ft. (1.5 m),
"-0010" for 10 ft. (3 m),
"-0020" for 20 ft. (6.1 m),
"-0035" for 35 ft. (10.7 m),
"-0050" for 50 ft. (15.2 m),
"-0075" for 75 ft. (22.8 m), or
"-0100" for 100 ft. (30.5 m)

*You will need a **CPU Cable** for each CPU you attach:*

Standard CPU Cables, available in standard lengths up to 20 ft. (6.1 m)—Mac styles require keyboard/mouse conversion
- IBM PS/2 style EHN051
- IBM PC/AT style EHN048
- Mac style with legacy DB15 video connectors EHN215
- Mac style with HD15 VGA video connectors for G3™, G4™, and similar models EHN550

Coaxial CPU Cables—IBM and Sun styles available in all standard lengths, SGI and RS/6000 styles available in standard lengths up to 20 ft. (6.1 m), Mac styles require keyboard/mouse conversion
- Universal IBM style EHN282
- Sun style with traditional 13W3 video connectors EHN206
- Sun style with VGA (HD15) video connectors EHN515
- SGI style EHN500
- RS/6000 style EHN520
- Mac style with traditional DB15 video connectors EHN208
- Mac style with HD15 VGA video connectors for G3, G4, and similar models EHN560

ServSwitch™ Micro Mac® Converter to convert PS/2 kbd/mouse to ADB™ kbd/mouse signals KV99MCON
For older Mac models that must see monitor ID: Mac® Video Adapter for ServSwitch™ KV99MA

*You will need a **User Cable** for each monitor/keyboard/mouse user station you attach:*

Regular (non-coaxial) User Cables, available in standard lengths up to 20 ft. (6.1 m)
- IBM PS/2* style EHN054
- Sun style with VGA (HD15) video connector for multisync monitor EHN059

Coaxial User Cables
- IBM PS/2* style, available in all standard lengths except 1 ft. (0.3 m) EHN283
- Sun style with 13W3 video connector for Sun monitor, available in all standard lengths EHN201
- Sun style with VGA (HD15) video connector for multisync monitor, available in all standard lengths EHN225
- SGI style, 1 ft. (0.3 m) only EHN501-0001
- RS/6000 style, 1 ft. (0.3 m) only EHN521-0001

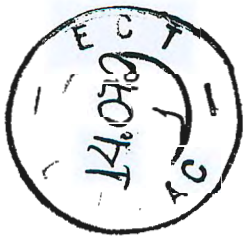
*We no longer offer IBM PC/AT type User Cables for the ServSwitch Affinity, because its current firmware does not support serial mice, although it will still translate signals from PS/2 type mice into serial protocol for PC/AT CPUs.

Ordering Information (continued)

ITEM	CODE
You might also need:	
Expansion Cables for 4-User Units	
10 ft. (3 m)	KV140010
20 ft. (6.1 m)	KV140020
35 ft. (10.7 m)	KV140035
50 ft. (15.2 m)	KV140050
100 ft. (30.5 m)	KV140100
Expansion Cables for 8- and 16-User Units	
10 ft. (3 m)	KV180010
20 ft. (6.1 m)	KV180020
35 ft. (10.7 m)	KV180035
50 ft. (15.2 m)	KV180050
100 ft. (30.5 m)	KV180100
Replacement 6-wire straight-through-pinned flat-satin cable for serial management (specify length)	EL06MS-MM
Rackmount Kits	
To mount 4- or 8-User units in 19" Racks	RMK19A
To mount 4- or 8-User units in 23" Racks	RMK23A
To mount 4- or 8-User units in 24" Racks	RMK24A
To mount 16-User units in 19" Racks	RMK19A139
To mount 16-User units in 23" Racks	RMK23A139
To mount 16-User units in 24" Racks	RMK24A139
Surge protector for IBM PS/2 style keyboard and mouse lines (6-pin mini-DIN M/F)	SP519A-R2
Surge protector for IBM PC/AT style keyboard lines (5-pin DIN M/F)	SP518A-R2

Call Black Box Tech Support for help determining your best options for AC-power backup and protection.

Black Box offers the best warranty program in the industry—Fido Protection®. For more information, request **FaxBack 22512**.



Manual 28

eHealth AIM for Apache User Guide

eHealth AIM for Apache User Guide

09-16050-003
December 2001

Important Notice

Concord Communications, Inc., *e*Health, *e*Health Suite, the Concord Logo, eROI, AdvantEDGE, SystemEDGE, Live Health, Network Health, Live Status, System Health, Application Health, Automating Technology Management, Constellation, Enterprise, Enterprise Monitor, Firstsense, FirstSense and design, FirstSense Enterprise, Pulse, Pulsecheck, Token/Net, Token/Scope, We See It Happening, Fault Manager, Empire, Empire Technologies and/or other Concord marks or products referenced herein are either registered trademarks or trademarks of Concord Communications, Inc. Other trademarks are the property of their respective owners.

Adobe, Acrobat, and the Acrobat logo are trademarks, which may be registered in certain jurisdictions, and PostScript is a registered trademark of Adobe Systems Incorporated.
Linux is a registered trademark of Linus Torvalds.
Microsoft, Windows, Windows NT, Windows 2000, and Windows XP are trademarks of Microsoft Corporation.
Intel is a registered trademark of Intel Corporation.
Red Hat is a registered trademark of Red Hat, Inc.
Sun, Solaris, and SunOS are trademarks of Sun Microsystems, Inc.
UNIX is a trademark in the United States and other countries licensed exclusively through X/Open Company Ltd.

This product includes software developed by the Apache Group for use in the Apache HTTP server project (http://www.apache.org/).

General Notice: Some of the product names used herein have been used for identification purposes only and may be trademarks of their respective companies.

Proprietary Notice

The information and descriptions contained herein are the property of Concord Communications, Inc. Such information and descriptions may not be copied, disseminated, or distributed without the express written consent of Concord Communications, Inc. Concord Communications, Inc., assumes no responsibility for any inaccuracies that may appear in this document. Concord Communications, Inc., reserves the right to improve its products and change specifications at any time without notice.

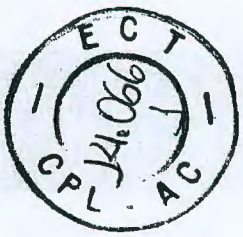
U. S. Government Restricted Rights

Use, reproduction, and disclosure by the U.S. Government are subject to the restrictions set forth in FAR §52.227-19 (c) (1) and (2) and DFARS §252.227-7013 (c) (1) (ii).

Patent Information

U. S. Patent 5,615,323
Patents Pending

Table of Contents



Preface

This guide describes how to install and use the *e*Health application insight module (AIM) for Apache for Solaris SPARC, Linux x86, HP-UX, and Windows NT 4.0, Windows 2000, and Windows XP systems. This guide supports the following:

- *e*Health AIM for Apache Release 1.0 Patchlevel 2 and later
- *e*Health SystemEDGE Release 4.0 Patchlevel 3 and later

This product supports the Apache Web server Version 1.3.2 and later.

Audience

This guide is intended for the person responsible for installing and configuring *e*Health AIM for Apache. To use *e*Health AIM for Apache, you should have a basic understanding of the Apache Web server, *e*Health SystemEDGE, and your host's operating system environment. For more information, refer to Apache documentation (http://www.apache.org) and the *eHealth SystemEDGE User Guide*.

About This Guide

This section describes the changes and enhancements that have been made since the last release of this guide. It also includes the documentation conventions used in this guide.

Revision Information

This guide now includes installation and configuration instructions for *e*Health AIM for Apache on Windows NT, Windows 2000, Windows XP, and HP-UX 10.x and 11.x systems.

Documentation Conventions

Table 1 lists the conventions used in this document.

Table 1. Documentation Conventions (Page 1 of 2)

Convention	Description
File or Directory Name	File or directory names.
`code`	System, code, or operating system command line examples.
emphasis	Emphasis and guide titles.
`enter`	Text that you must type exactly as shown.
Name	Text that defines menus, fields in dialog boxes, or keyboard keys.
New Term	A new term, that is, one that is being introduced.
`Variable`	Variable values that you substitute.
→	A sequence of menus or menu options. For example, **File** → **Exit** means "Choose **Exit** from the **File** menu."

Table 1. Documentation Conventions (Page 2 of 2)

Convention	Description
NOTE	Important information, tips, or other noteworthy details.
CAUTION	Information that helps you avoid data corruption or system failures.
WARNING	Information that helps you avoid physical danger.

Technical Support

If you need any assistance with this product or the SystemEDGE agent, contact Technical Support at the following:

Phone: (888) 832-4340
(508) 303-4300
Fax: (508) 303-4343
E-mail: support@concord.com
Web site: http://www.concord.com

Professional Services

If you need any assistance with customizing this product, contact Professional Services at the following:

Phone: (800) 851-8725 (Choose option 7)
Fax: (508) 486-4555
E-mail: proserv@concord.com
Web site: http://www.concord.com

Introduction

This chapter provides an overview of *e*Health AIM for Apache.

Introducing *e*Health AIM for Apache

*e*Health AIM for Apache is a plug-in for the SystemEDGE agent that enables information technology (IT) operators to monitor the Apache Web server. The power and flexibility of the Apache Web server make it the server of choice for many corporations.

*e*Health AIM for Apache enables you to monitor the Apache server's performance and availability on these operating systems:

- Sun Solaris Release 2.5 and later
- RedHat Linux Release 6.0 and later
- HP-UX Release 10.x and 11.x (not including 10.01)
- Microsoft Windows NT 4.0, Windows 2000, and Windows XP

To use *e*Health AIM for Apache, you must install it on every Apache server that you want to monitor. For more information, refer to Chapter 2, "Installing eHealth AIM for Apache."

NOTE

This guide is not intended to describe how to install, administer, or use the Apache Web server. For help with Apache, refer to your Apache Web server documentation.

Features

*e*Health AIM for Apache monitors the following:

- Apache server processes
- Apache server log files
- Performance metrics that are specific to Apache
- Web service response and availability

*e*Health AIM for Apache monitors httpd process attributes. For example, it monitors whether each process is running (alive). It can also restart processes, if necessary. In addition, it monitors memory usage, memory size, and page faults.

Because the Apache Web server records Web accesses and errors in log files, *e*Health AIM for Apache can use the SystemEDGE agent log-file monitoring capability to scan those logs and forward certain events as Simple Network Management Protocol (SNMP) traps when appropriate.

*e*Health AIM for Apache is designed to monitor one or more Apache servers running on a single system. To support multiple servers, the data presented in the *e*Health AIM for Apache management information base (MIB) is organized into tables that are indexed by server port number. For instance, if you have a server running on port 80 and another on port 8080, entries appear in each table for index 80 and index 8080. For more information, refer to Chapter 3, "Using the eHealth AIM for Apache MIB."

Using the mod_info and mod_status Facilities

*e*Health AIM for Apache obtains server status and behavior information from the Apache server through the Apache mod_info and mod_status facilities. To access this type of information, you must enable these facilities in your Apache configuration file (httpd.conf). If these facilities are secured through the use of an authentication mechanism, you must also provide a valid user name and password for accessing these resources in the apachemod.cf file. For more information, refer to "Editing the httpd.conf File" on page 23 and "Editing the apachemod.cf File" on page 25.

Caching Disk Space Information

As part of the application footprint calculations, *e*Health AIM for Apache can calculate the total amount of disk space used by your Apache server. On some systems with large amounts (greater than 1 GB) of Web data, this calculation can take a long time. For this reason, *e*Health AIM for Apache is designed to cache the disk space information to avoid frequent recalculations. You can control the frequency of the disk space calculations in the *e*Health AIM for Apache configuration file (apachemod.cf). For more information, refer to "Editing the apachemod.cf File" on page 25.

Using *e*Health AIM for Apache

*e*Health AIM for Apache provides you with the tools and information that are necessary for monitoring the health and availability of the Apache Web server. It makes important information about Apache available to management software through the SystemEDGE agent and SNMP.

*e*Health AIM for Apache works with the SystemEDGE agent to closely manage the Apache Web server, providing real-time fault detection and automatically correcting problems, if necessary. You can use *e*Health AIM for Apache with any SNMP-compliant management software, including Concord's *e*Health suite of products, AdvantEDGE View, HP OpenView, and others.

*e*Health AIM for Apache and the SystemEDGE agent can provide you with the following types of information:

- Number of "hits" your Web server is receiving, which can help you keep up with daily volume and set monitor points to watch for unusual traffic loss or denial of service attacks
- Amount of space your Web log and Web server files are consuming
- How effectively the Apache processes monitor idle services, warn you when the number of idle services is too low, and monitor the number of active processes
- How much of your system resources (Central Processing Unit [CPU] and memory) Apache is using on your server
- Whether bottlenecks on your Web servers are caused by problems with the CPU, memory, disk, or network

Using *e*Health AIM for Apache with AdvantEDGE View

You can use AdvantEDGE View with *e*Health AIM for Apache to monitor the performance, configuration, availability, and health of the Apache Web server.

To run an AdvantEDGE View query for Apache:

1. Select the target system or group from the **System** or **Group** list in the AdvantEDGE View interface.
2. Select **Apache** from the **Applications** list.
3. Click the **Applications** icon.

1

Figure 1 shows a sample image map that AdvantEDGE View displays when you run a query on the target Apache workstation. Click the area for which you want to display information.

Figure 1. AdvantEDGE View Image Map for Apache Queries

For example, if you click the **Footprint** area, AdvantEDGE View displays information about Apache's CPU, memory, and disk resource consumption. Figure 2 shows the Disk Usage section of the AdvantEDGE View Footprint query for an Apache Web server.

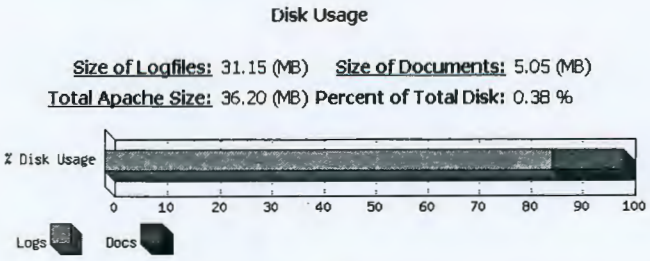


Figure 2. Sample Section of an AdvantEDGE View Footprint Query for Apache

Using *e*Health AIM for Apache with *e*Health

In previous releases, eHealth – Application Insight was called eHealth – Application Assessment.

You can use *e*Health AIM for Apache and the SystemEDGE agent with the *e*Health product suite to provide historical data for long-term trending analysis and capacity planning. With *e*Health – Application Insight, you can run At-a-Glance, Trend, Top N, and MyHealth reports for the following types of information:

- Amount of Central Processing Unit (CPU), total memory, and disk space the Apache Web server is using
- Number of users who are connected to the Apache server
- Number and type of processes that are running
- Amount of Web traffic
- Total size of the Apache service logs
- End-to-end performance summaries for your Apache application, host system, and network

For more information about the variables you can monitor and reports that you can run when you integrate *e*Health AIM for Apache with *e*Health, refer to the *e*Health Web Help.

Using *e*Health AIM for Apache with Live Health

You can also use *e*Health AIM for Apache and the SystemEDGE agent with Live Health for real-time detection of potential problems. Live Health applies intelligent algorithms to the data, resulting in precise assessments of application health and performance. For more information about how Live Health can detect "brownouts" and service delays across applications, systems, and networks, refer to the Live Health Web Help.

Installing eHealth AIM for Apache

This chapter explains how to install, configure, and license *e*Health AIM for Apache.

NOTE

For the most current information about installing this module, refer to the relnotes.txt file on the *e*Health AIM for Apache installation CD-ROM.

Installation Requirements

Before you install *e*Health AIM for Apache, you must first install, license, and configure the SystemEDGE agent Release 4.0, Patchlevel 3 or later. For more information, refer to the *eHealth SystemEDGE User Guide*. Also, your system must be running the Apache Web server Release 1.3.2 or later on one of these operating systems:

- Sun Solaris (SPARC) Release 2.5 or later
- Red Hat Linux (x86) Release 6.0 or later
- HP-UX Release 10.x and 11.x (not including 10.01)
- Microsoft Windows NT 4.0, Windows 2000, or Windows XP

Installing the Software

This section describes how to install *e*Health AIM for Apache for Solaris, Linux, HP-UX, and Windows operating systems.

Installing the Software for UNIX Systems

For Solaris, Linux, and HP-UX systems, *e*Health AIM for Apache is distributed as a tar file.

To install *e*Health AIM for Apache:

1. Locate the Apache server that you want to monitor.
2. Log in to the UNIX system where that server is located as **root**.
3. Copy the apachemod.tar file from the CD-ROM to the /tmp directory.
4. Change directory to the SystemEDGE agent directory on your system by entering the following:

   ```
   cd /opt/EMPsysedge
   ```
5. Create the plugins directory, if it is not already present, by entering the following:

   ```
   mkdir plugins
   ```
6. Change directory to the plugins directory by entering the following:

   ```
   cd plugins
   ```
7. Enter the following to start the installation.

   For Solaris, enter the following command:

   ```
   tar xvf /tmp/apachemod_1.0p2_sol.tar
   ```

   For Linux, enter the following command:

   ```
   tar xvf /tmp/apachemod_1.0p2_linux.tar
   ```

   For HP-UX, enter the following command:

   ```
   tar xvf /tmp/apachemod_1.0p2_hpux.tar
   ```

   The installation creates files in the plugins/apachemod directory. *e*Health AIM for Apache is now installed.

Installing the Software for Windows NT Systems

Throughout this guide, the term Windows NT encompasses Windows NT 4.0, Windows 2000, and Windows XP.

For Windows NT 4.0, Windows 2000, and Windows XP systems, *e*Health AIM for Apache is distributed as a self-extracting executable named apachemod_1.0p2_ntx86.exe.

To install *e*Health AIM for Apache:

1. Log in to the Windows NT system as administrator.
2. Click **Start.**
3. Select **Programs → Command Prompt.**
4. Insert the CD containing the Concord software distributions into the CD-ROM drive.
5. Windows automatically mounts the drive using the CD-ROM drive's corresponding drive letter. The particular drive letter is specific to your system and depends on the number and types of disks attached to your system.
6. Determine which directory you want to use as the installation directory for *e*Health AIM for Apache. If the SystemEDGE agent is installed in C:\sysedge, the recommended installation directory is C:\sysedge\plugins.

NOTE

You *cannot* run apachemod.exe by double-clicking the executable from the CD-ROM.

7. Run the self-extracting executable by entering the following at the command prompt, where `D:` is the CD-ROM drive for your system, and `C:sysedge\plugins` is the installation directory:

```
D:\apachemod\ntx86\apachemod1.0p2_ntx86.exe -dir C:\sysedge\plugins
```

The -dir option instructs the self-extracting executable to create the intended subdirectory hierarchy that is described throughout this guide. It then places the distribution in an apachemod subdirectory within the specified target directory (such as C:\sysedge\plugins). *e*Health AIM for Apache is now installed.

*e*Health AIM for Apache Files

Table 2 describes the files created by the *e*Health AIM for Apache installation procedure.

Table 2. Files Installed by *e*Health AIM for Apache

File Name	Description
apachemod.asn1	*e*Health AIM for Apache MIB specification
apachemod.cf	*e*Health AIM for Apache configuration file
apachemod.pdf	*eHealth AIM for Apache User Guide*
apachemod.dll (Windows only)	*e*Health AIM for Apache dynamic link library (DLL) module for Windows NT, Windows 2000, and Windows XP
apachemod.so (Solaris and Linux only)	*e*Health AIM for Apache shared library for 32-bit Solaris and Linux operating systems
apachemod-sparcv9.so (Solaris only)	*e*Health AIM for Apache shared library for 64-bit Solaris operating systems
apachemod-hpux.so (HP-UX only)	*e*Health AIM for Apache shared library for 32-bit HP-UX (10.x and 11.x) operating systems
apachemod-hpux11-64.so (HP-UX only)	*e*Health AIM for Apache shared library for 64-bit HP-UX (11.x) operating systems
relnotes.txt	Release notes for *e*Health AIM for Apache

Configuring *e*Health AIM for Apache

After you install *e*Health AIM for Apache, you must configure it by editing the following files:

- sysedge.cf
- httpd.conf
- apachemod.cf

2

Editing the sysedge.cf File

By default, the SystemEDGE agent does not load any plug-ins at initialization time, but you can edit the sysedge.cf file to configure the agent to load any *e*Health AIMs that you have installed. To enable the SystemEDGE agent to load *e*Health AIM for Apache at startup, you must edit the sysedge.cf configuration file. This file is located in your system directory by default; for example, it is located in the /etc/sysedge.cf directory on UNIX systems and in C:\winnt\system32 for Windows NT and 2000 systems. Use the **sysedge_plugin** keyword as described in the following sections to configure SystemEDGE to load *e*Health AIM for Apache at startup.

NOTE

To configure the SystemEDGE agent to start *e*Health AIM for Apache, you must provide the *complete pathname* to the shared library file for your system.

Enabling *e*Health AIM for Apache for UNIX Systems

Add one of the following lines to the sysedge.cf file.

For Solaris or Linux systems in 32-bit mode, add the following line:

```
sysedge_plugin /opt/EMPsysedge/plugins/apachemod/apachemod.so
```

For Solaris 2.7 and later systems in 64-bit mode, add the following line:

```
sysedge_plugin /opt/EMPsysedge/plugins/apachemod/apachemod-sparcv9.so
```

For HP-UX 10.x systems in 32-bit mode, add the following line:

```
sysedge_plugin /opt/EMPsysedge/plugins/apachemod/apachemod-hpux.so
```

For HP-UX 10.x and 11.x systems in 64-bit mode, add the following line:

```
sysedge_plugin /opt/EMPsysedge/plugins/apachemod/apachemod-hpux11-64.so
```

Enabling *e*Health AIM for Apache for Windows Systems

To enable *e*Health AIM for Apache for Windows NT, Windows 2000, and Windows XP systems, you must provide the complete path name to apachemod.dll. The actual path depends on the location you selected when you installed *e*Health AIM for Apache. For example, enter the following command if you installed the files in the C:\sysedge\plugins\apachemod directory:

```
sysedge_plugin C:\sysedge\plugins\apachemod\apachemod.dll
```

For more information about the sysedge.cf file, refer to the *eHealth SystemEDGE User Guide.*

Editing the httpd.conf File

Edit the httpd.conf file to enable the Apache mod_info and mod_status facilities. These facilities control access to HTML pages that provide information about the server's status and behavior. When these modules are enabled, *e*Health AIM for Apache can use them to obtain information about the Apache server's status and behavior. For more information about the mod_info and mod_status modules, refer to Apache documentation (at http://www.apache.org).

NOTE

You must ensure that your server has server-status and server-info built into Apache by enabling the mod_status and mod_info facilities, as described in the following section. If you do not, you may experience process-termination errors.

To enable the mod_info and mod_status features in your Apache server:

1. Remove the pound sign (#) in front of the following lines in httpd.conf:

   ```
   LoadModule status_module modules/mod_status.so
   LoadModule info_module modules/mod_info.so
   ```

2. Add the following lines to httpd.conf:

```
# Turn on Extended Status Information
ExtendedStatus On
# Enable server-status access from the local host
<Location /server-status>
    SetHandler server-status
    Order deny,allow
    Deny from all
   Allow from 127.0.0.1
</Location>
   # Enable server-info access from the local host
   <Location /server-info>
      SetHandler server-info
       Order deny,allow
       Deny from all
       Allow from 127.0.0.1
   </Location>
```

NOTE

You must restart the Apache server after you make these changes to ensure that they take effect.

Editing the apachemod.cf File

You can edit the apachemod.cf file to do the following:

- Indicate which Transmission Control Protocol (TCP) port your Apache server is using.
- Assign user names and passwords for the mod_info and mod_status facilities. You must include user names and passwords to the apachemod.cf file, even if they are not specifically required by the Apache Web server. The Apache Web server requires these fields *only* if you have enabled the mod_info and mod_status facilities as described in the previous section, "Editing the httpd.conf File," and you are using authentication (through user names and passwords) to restrict access to those modules. The apachemod.cf file, however, *always* requires these fields.

NOTE

Even if you do not password protect your server-info and server-status pages, you must configure artificial user name/password combinations in apachemod.cf. The Apache Web server and *e*Health AIM for Apache then ignore those user names and passwords.

- Indicate which Apache server(s) *e*Health AIM for Apache should monitor if you are running more than one Apache server on your system through port numbers. Port 80 is the default Web server port.
- Set the interval for calculating the total amount of disk space being used by the Apache server, or disable this checking.

Sample apachemod.cf File

The following is a sample apachemod.cf file:

```
# apachemod.cf
# Configuration file for eHealth AIM for Apache
#
# For each apache server running on your system, specify the following:
# apache port username password filestat-interval
#  port - port number on which the server is running
#  username - the username for accessing server-status and server-info pages
#  password - the password for accessing server-status and server-info pages
#  filestat-interval - interval in seconds between checks of the file sizes
#                      specify "0" to disable file size checking
# Primary server - example
apache 80 status statpass1 3600
# Application server - example
# apache 8080 status statpass1 3600
```

NOTE

After you make any changes to the apachemod.cf file, you must restart the SystemEDGE agent to ensure that the changes take effect.

Licensing *e*Health AIM for Apache

Like the SystemEDGE agent, *e*Health AIM for Apache utilizes a host-based license method. Copies of *e*Health AIM for Apache can run only on systems that possess a valid license key. This license is separate from the one used for the SystemEDGE agent.

The first time that you attempt to start the SystemEDGE agent after installing *e*Health AIM for Apache, the agent displays a message stating that it could not find a valid license for *e*Health AIM for Apache. It then provides you with a public key that is used to generate a permanent license key for your host machine.

A license key is composed of four space-separated, 8-character sequences, totaling 32 characters. The sysedge.lic file contains the *e*Health AIM for Apache license, as well as the SystemEDGE agent license and other *e*Health AIM licenses. For an example, refer to the sample license file in "Sample License File" on page 34.

Obtaining a License

To obtain a license, you can do any of the following:

- Complete the online license form through the Internet, as described in the next section, "Generating the License through the Web-Based License Form."
- Use AdvantEDGE View to receive an SNMP license trap or to query and license the plug-in without a trap. For more information, refer to "Generating a License through AdvantEDGE View Event Processing" on page 30 or "Generating a License through AdvantEDGE View Host Administration" on page 32.
- Send an e-mail request to licenses@concord.com, and place the returned license key in the sysedge.lic file. Always include your user name in license requests that you send through e-mail.
- Run the Concord-supplied licenseutil.pl script.
- Run the licenseme.exe license utility.

For more information about licensing, refer to the *eHealth SystemEDGE User Guide* and the *Automating the Licensing of the AdvantEDGE Point Plug-in Modules* white paper.

Generating the License through the Web-Based License Form

This section describes how to generate the *e*Health AIM for Apache license through the Web-based license form.

NOTE

If you are using an evaluation copy of *e*Health AIM for Apache, you must request a temporary license to enable it to operate during the evaluation period.

To generate a license:

1. Start the SystemEDGE agent as follows:
   a. Log in as **root**.
   b. Change directory (cd) to /opt/EMPsysedge.
   c. Enter the following:

      bin/sysedge

      The SystemEDGE agent displays a message indicating that you need a license for the *e*Health AIM for Apache module on this host system. It then displays a message similar to the following:

```
SystemEDGE Version 4.1 Patchlevel 1
Copyright 2001 by Concord Communications, Inc.
Please contact Concord Communications, Inc. to obtain a license
http://www.concord.com/support, Email: licenses@concord.com
Provide this: apachemod neptune sol2 5.9 346561363366b19c 1.0 Patchlevel 2
```

2. Using a Web browser, go to the licensing Web site at http://license.concord.com, and select the **Create License** option that matches your use of the agent:
   - **Create SystemEDGE/AdvantEDGE Eval License** (if you are evaluating the AIM or are a Concord partner or reseller)
   - **Create SystemEDGE Outsource License** (if you are outsourcing the AIM)
   - **Create SystemEDGE/AdvantEDGE License** (if you have purchased the AIM)

NOTE

You must supply a user name and password to access the license form.

3. Complete the license form, entering the information that was printed by the SystemEDGE agent. You must supply the following information:
   - Name
   - E-mail address
   - Software version number (1.0 in the example)
   - Patchlevel (2 in the example)
   - System name (neptune in the example)
   - Operating system name (sol2 in the example)
   - Operating system version (5.9 in the example)

NOTE

When you request a license, select the option for *e*Health AIM for Apache in the product field of the licensing form.

After you submit the license request form, the Concord Web server generates a license and displays it on your Web browser. It also e-mails the license to the contact person in your organization.

4. Copy the license into the sysedge.lic file. This file is located in the /etc directory for UNIX operating systems and in the \winnt\system32 directory for Windows NT, Windows 2000, and Windows XP operating systems.

   The license key is case sensitive. Copy it exactly as it appears. If possible, use your system's copy-and-paste facility instead of typing it by hand. If you are entering the license key manually, be careful not to confuse characters such as the letters l and I and the number 1, or the letter O and the number 0.

5. Save the sysedge.lic file.

6. Restart the SystemEDGE agent.

   For UNIX systems, restart the SystemEDGE agent by entering the following when you are logged in as root:

   ```
   bin/sysedge -b
   ```

   For Windows systems, stop and restart the Windows NT Master agent by entering these commands at the command prompt:

   ```
   net stop snmp
   net start snmp
   ```

Generating a License through AdvantEDGE View Event Processing

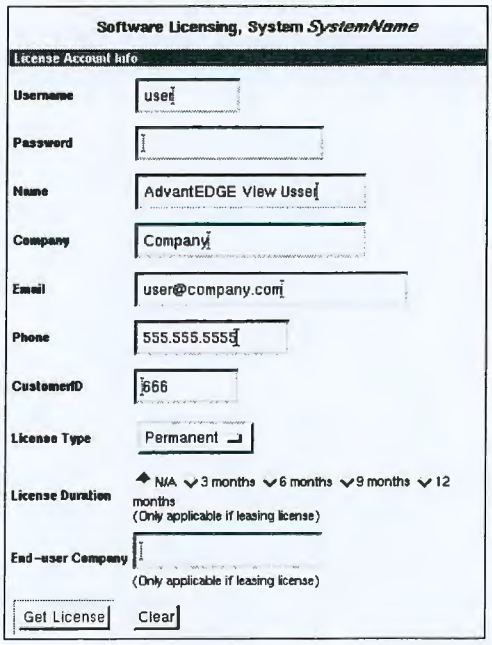
In order to use AdvantEDGE View event processing to license *e*Health AIM for Apache, your system must meet the following requirements:

- You must be using SystemEDGE Release 4.0 Patchlevel 3 or later with AdvantEDGE View.
- You must configure the SystemEDGE agent to send SNMP traps to AdvantEDGE View. For more information, refer to the section on configuring the SystemEDGE agent in the *eHealth SystemEDGE User Guide.*
- You must configure the SystemEDGE agent with a read-write community so that AdvantEDGE View can issue an SNMP Set to transmit the license key to it. For more information, refer to the section on configuring the SystemEDGE agent in the *eHealth SystemEDGE User Guide.*
- Your AdvantEDGE View system must have access to the Internet, either directly or through a Web proxy.
- The AdvantEDGE View User who is generating the license must have either write or admin permissions.

To generate a license through AdvantEDGE View:

1. Start the SystemEDGE agent with *e*Health AIM for Apache in unlicensed mode. SystemEDGE sends a license trap to AdvantEDGE View for that module.
2. Start AdvantEDGE View, and click the **Events** icon to display the Event Processing screen.

   AdvantEDGE View displays a license trap for the system that requires a license.
3. Click the index number for that system to view the Trap Details form for **License Software** to display the AdvantEDGE View Software Licensing form.
4. Complete the licensing form, and click **Get License**.



NOTE

If you have configured AdvantEDGE View preferences, AdvantEDGE View fills in all of the information (except password) on this form. You must enter the password each time you use the form for security purposes.

AdvantEDGE View contacts the Web-based license server, obtains a license for *e*Health AIM for Apache and issues an SNMP Set to the target SystemEDGE agent to inform it of the new software license key.

Generating a License through AdvantEDGE View Host Administration

You can also license systems through AdvantEDGE View Host Administration.

To access Host Administration:

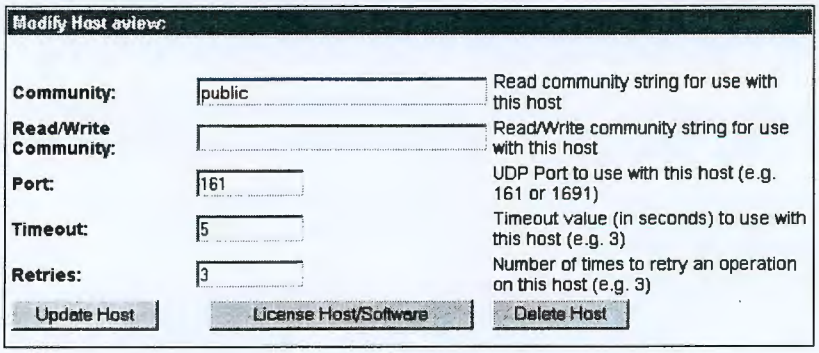
1. Start AdvantEDGE View, and click the **Administration** icon. AdvantEDGE View displays the Administration page.
2. Click the **Host Administration** icon. AdvantEDGE View displays the host list.

SystemEDGE Host Configuration

System Name	Community	Read/Write Community	Port	Timeout	Retries
aviewdemo	public		161	2	2
mailserver	public		161	6	3
nethealth	public		161	3	3
ntclient	public		161	6	3
ntserver	public		161	3	2
unixclient	public		161	6	3
unixserver	public		161	3	3
win2kclient	public		161	5	3
www	public		161	6	3

Add New Host

3. Click the name of the system that you want to license from the **System Name** column. AdvantEDGE View displays the Modify Host form.



4. Click **License Host/Software** to display the licensing form.
5. Select the product you want to license from the **Product** list, and then click **License Software.**

   AdvantEDGE View contacts the Web-based license server, obtains a license for the software, and issues an SNMP Set to the target SystemEDGE agent, informing it of the new software license key.

Sample License File

The following is a sample SystemEDGE agent license file. A pound character (#) in column 1 indicates that the entire line is a comment.


```
# license file for SystemEDGE Agent
# Concord Communications, Inc.
# http://www.concord.com
#
# file /etc/sysedge.lic or %SystemRoot%\system32\sysedge.lic
# A valid license key has four parts of 8 characters per part
# parts are separated by space(s) with one license key per line

# sysedge neptune sol2 5.8 807cb1da007cb1da 4.1 Patchlevel 1
e13311d3 0F2a7cb1 abC512dc fF8C923a
# apachemod neptune sol2 5.8 807cb1da007cb1da 1.0 Patchlevel 2
a7943fde 098a87ij a4kiuf39 afafEkj4
```

3

Using the eHealth AIM for Apache MIB

This chapter explains the organization and content of the Concord Communications MIB for the Apache Web server. The MIB specification (apachemod.asn1) defines a collection of objects for monitoring and managing Apache. You must configure the SystemEDGE agent to monitor the MIB objects that are relevant for your configuration. For more information, refer to Chapter 4, "Using eHealth AIM for Apache." Figure 3 shows the organization of the Apache MIB.

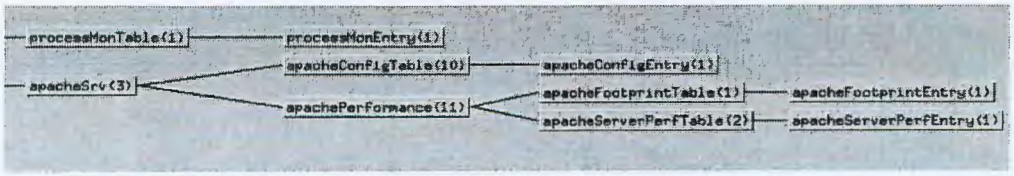


Figure 3. *e*Health AIM for Apache MIB

The figures in the following sections represent AdvantEDGE View queries on information that is available through the AdvanatEDGE for Apache MIB.

The MIB is organized into sections for server configuration and performance. Within the performance section, a footprint section defines MIB objects that convey how much of the underlying system's resources are consumed by Apache. This chapter defines all sections of the Apache MIB and highlights important MIB objects from each section. For a complete list of MIB objects, refer to the *e*Health AIM for Apache MIB specification (apachemod.asn1).

Configuration Section

The Configuration section of the *e*Health AIM for Apache MIB contains configuration parameters and settings that are important for streamlining the health and performance of the Apache Web server. It also includes information about server configuration.

Server Configuration

The Server Configuration group contains configuration parameters, process IDs, and version numbers. Table 3 defines important Server Configuration parameters.

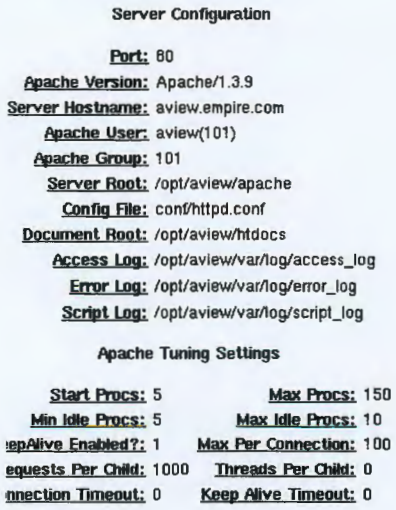
Table 3. Selected MIB Objects – Apache Server Configuration Group (Page 1 of 2)

MIB Object	Description
apacheConfigTable	Table of configuration settings for each Apache installation.
apacheConfigEntry	Entry in the Apache configuration table.
apacheConfigPort	TCP port currently used by this Apache configuration. **NOTE** This value serves as the index for this table.
apacheConfigVersion	Apache Web server version.
apacheConfigPID	Process ID (PID) of the master Apache process; zero if the server is not running.
apacheConfigRunMode	Current operating mode (for example, standalone).
apacheConfigUser	User who is currently running the server processes.
apacheConfigGroup	Group that is currently running the server processes.
apacheConfigHostname	Host name used by this Apache configuration.
apacheConfigStartProcs	Number of server processes started by the Apache server at startup.
apacheConfigMinIdleProcs	Minimum number of idle server processes maintained by the Apache server.

Table 3. Selected MIB Objects – Apache Server Configuration Group (Page 2 of 2)

MIB Object	Description
apacheConfigMaxIdleProcs	Maximum number of idle server processes allowed by the Apache server.
apacheConfigMaxProcs	Maximum number of server processes allowed by the Apache server.
apacheConfigRequestsMaxPerChild	Number of requests handled by a server process before it is recycled by the Apache server.
apacheConfigRequestsKeepAlive	Status of whether keep-alive mode is enabled for persistent connections: disabled = 0; enabled = 1.
apacheConfigRequestsMaxPerConn	Number of requests handled in a single connection if keep-alive mode is enabled.
apacheConfigThreadsPerChild	Maximum number of threads per child process.
apacheConfigConnectionTimeout	Timeout value for closing inactive connections.
apacheConfigKeepAliveTimeout	Keep-alive timeout value for open connections.
apacheConfigServerRoot	Root directory for this Apache installation.
apacheConfigConfigFile	Current configuration file for this Apache installation.
apacheConfigPIDFile	Current PID file for this Apache installation.
apacheConfigScoreboardFile	Current scoreboard file for this Apache installation.
apacheConfigDocumentRoot	Current document root directory for this Apache installation.
apacheConfigAccessLogFile	Current access or transaction log file for this Apache installation.
apacheConfigErrorLogFile	Current error log file for this Apache installation.
apacheConfigScriptLogFile	Current script log file for this Apache installation.

Figure 4 shows a sample AdvantEDGE View Apache Server Configuration query.



Server Configuration

Port:	80
Apache Version:	Apache/1.3.9
Server Hostname:	aview.empire.com
Apache User:	aview(101)
Apache Group:	101
Server Root:	/opt/aview/apache
Config File:	conf/httpd.conf
Document Root:	/opt/aview/htdocs
Access Log:	/opt/aview/var/log/access_log
Error Log:	/opt/aview/var/log/error_log
Script Log:	/opt/aview/var/log/script_log

Apache Tuning Settings

Start Procs:	5	**Max Procs:**	150
Min Idle Procs:	5	**Max Idle Procs:**	10
epAlive Enabled?:	1	**Max Per Connection:**	100
equests Per Child:	1000	**Threads Per Child:**	0
nnection Timeout:	0	**Keep Alive Timeout:**	0

Figure 4. Sample AdvantEDGE View Server Configuration Query for Apache

Performance Section

The Performance section of the *e*Health AIM for Apache MIB contains performance data that is necessary for capacity planning and trend analysis, as well as real-time performance and availability monitoring. The Performance group is divided into subgroups for footprint data and server performance.

Apache Footprint

The Footprint group provides information about the Apache CPU, memory, data flow, and disk-resource consumption, which is more commonly called the *footprint.* Long-term trending analysis of footprint information is useful for anticipating and avoiding problems due to resource exhaustion.

You can also monitor footprint information in real time to detect and correct temporary resource exhaustion due to viruses, security incidents, and hardware failures. Table 4 defines important Apache Footprint metrics.

Table 4. Selected MIB Objects – Apache Footprint Group (Page 1 of 2)

MIB Object	Description
apacheFootprintTable	Table that reports the performance footprint for each Apache service.
apacheFootprintEntry	Entry in the Apache Performance Footprint table.
apacheFootprintPort	TCP port that is currently used by this Apache configuration. **NOTE** This value serves as the index for this table.
apacheFootprintCPUTime	CPU time, in seconds, accumulated by the Apache server, including all Apache processes.
apacheFootprintPercentCPU	Percentage of CPU utilization by the Apache server over the last sample interval; the value reported is percentage multiplied by 100.
apacheFootprintTotalMEMSize	Combined size of Apache's text, data, and stack segments in KB; summation of the process sizes for all Apache server processes.
apacheFootprintTotalRSS	Real memory (resident set) size (RSS) of the Apache server in KB; summation of all process RSS for all Apache server processes.
apacheFootprintPercentMEM	Percentage (0 to 100) of real memory used by the Apache server, which includes all Apache server processes.
apacheFootprintNumThreads	Number of threads executing within all Apache processes of which the operating system is aware.
apacheFootprintInBlks	Number of blocks of data input by the processes.
apacheFootprintOutBlks	Number of blocks of data output by the processes.
apacheFootprintMsgsSent	Number of messages sent by the processes.
apacheFootprintMsgsRecv	Number of messages received by the processes.
apacheFootprintSysCalls	Number of system calls invoked by the processes.

Table 4. Selected MIB Objects – Apache Footprint Group (Page 2 of 2)

MIB Object	Description
apacheFootprintMinorPgFlts	Number of minor page faults (which do not require input/output [I/O] to retrieve the page) incurred by the processes.
apacheFootprintMajorPgFlts	Number of major page faults (which require I/O to retrieve the page) incurred by the processes.
apacheFootprintNumSwaps	Number of times the processes have been swapped.
apacheFootprintVolCtx	Number of voluntary context switches incurred by the processes.
apacheFootprintInvolCtx	Number of involuntary context switches incurred by the processes.
apacheFootprintTotalLogSize	Size in KB of the Apache service logs; sum of the access and error log file sizes.
apacheFootprintDocSize	Size in KB of the Apache document root directory and all files beneath it.
apacheFootpringTotalDiskSize	Size in KB of all the Apache disk storage areas; summation of log sizes and service directories.

The following figures show sample AdvantEDGE View Footprint queries for an Apache system that is serving a medium-sized company. Figure 5 shows a sample Disk Usage query.

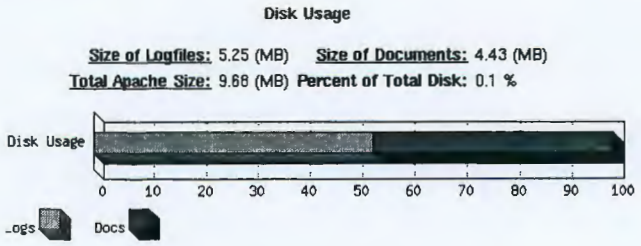


Figure 5. AdvantEDGE View Disk Usage Query for Apache

Figure 6 shows a sample CPU and Memory Footprint query.

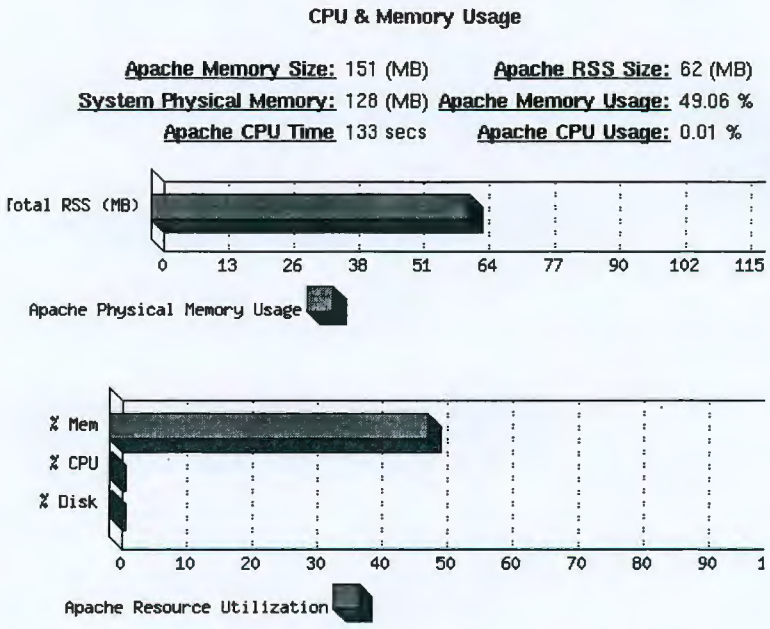


Figure 6. AdvantEDGE View CPU and Memory Footprint Query for Apache

Server Performance

The Server Performance group provides performance metrics and counters for the Apache Web server, including user statistics and transfer statistics. These metrics include those useful for real-time management and longer-term capacity planning and trend analysis. Table 5 defines important Server Performance metrics.

Table 5. Selected MIB Objects – Apache Server Performance Group (Page 1 of 2)

MIB Object	Description
apacheServerPerfTable	Table that reports the performance of each Apache service.
apacheServerPerfEntry	Entry in the Apache Server Performance table.
apacheServerPerfPort	TCP port that is currently used by this Apache configuration; index for this table.
apacheServerPerfUptime	Number of seconds that the Apache server has been running.
apacheServerPerfTotalAccesses	Number of accesses (hits) to this server since it was last started.
apacheServerPerfTotalTraffic	Number of KB transferred by this server since it was last started.
apacheServerPerfCurrentUsers	Number of current active users (connections) maintained by the Apache server.
apacheServerPerfCurrentIdleProcs	Number of current idle processes available on the Apache server.
apacheServerPerfCurrentStartupProcs	Number of processes that are currently in startup mode on the Apache server.
apacheServerPerfCurrentReadProcs	Number of processes that are currently reading requests on the Apache server.
apacheServerPerfCurrentReplyProcs	Number of processes that are currently replying to requests on the Apache server.
apacheServerPerfCurrentKeepAliveProcs	Number of processes that are currently in keep-alive mode on the Apache server.
apacheServerPerfCurrentDNSProcs	Number of processes that are currently doing a Domain Name System (DNS) lookup on the Apache server.

Table 5. Selected MIB Objects – Apache Server Performance Group (Page 2 of 2)

MIB Object	Description
apacheServerPerfCurrentLoggingProcs	Number of processes that are currently logging transactions on the Apache server.
apacheServerPerfCurrentFinishingProcs	Number of processes that are currently finishing transactions on the Apache server.
apacheServerPerfCurrentTotalProcs	Total number of Apache processes that are currently running on the Apache server.

Figure 7 shows an Apache server Performance summary.

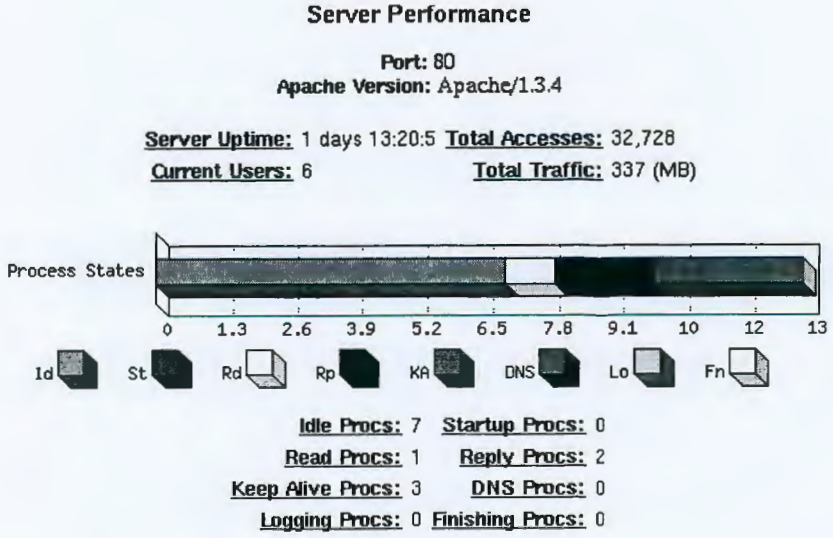


Figure 7. AdvantEDGE View Server Performance Summary for Apache

4

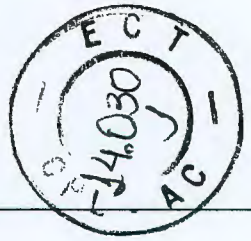
Using eHealth AIM for Apache

This chapter describes how to use *e*Health AIM for Apache. This module is implemented as a SystemEDGE agent plug-in. After you enable this plug-in in the sysedge.cf file and obtain a license for it, it will load automatically at SystemEDGE start time. For more information, refer to "Editing the sysedge.cf File" on page 21 and "Licensing eHealth AIM for Apache" on page 25.

Overview

The *e*Health AIM for Apache plug-in implements additional MIB objects that provide advanced information about the health and availability of the Apache Web server. It can operate with any SNMP-compliant management software such as Concord's *e*Health suite of products, AdvantEDGE View, HP OpenView, and others. If you are using *e*Health AIM for Apache with *e*Health, refer to the *e*Health Web Help for more information about the reports you can generate.

The default configuration settings of *e*Health AIM for Apache enable you to use the advanced self-monitoring capabilities of the SystemEDGE agent in conjunction with *e*Health AIM for Apache.



*e*Health AIM for Apache MIB Branch

You can use AdvantEDGE View or another SNMP tool to edit the SystemEDGE configuration file to utilize the MIB objects found in *e*Health AIM for Apache with the process-monitoring, threshold-monitoring, and history-collection features of the SystemEDGE agent. All MIB objects related to *e*Health AIM for Apache exist at object identifier (OID) branch *1.3.6.1.4.1.546.16.3* in the Concord Systems Management MIB. The MIB is defined in the apachemod.asn1 file, which is available in the *e*Health AIM for Apache product installation.

Assigning Entry Rows for the SystemEDGE Self-Monitoring Tables

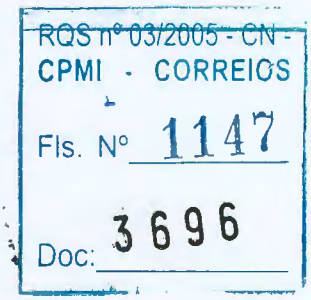
All SystemEDGE self-monitoring tables require the use of unique row numbers. Each table contains an Index column which acts as a **key field** to distinguish rows in the table. This section describes the benefits of reserving a block of rows (in the range of 11 to the maximum number of rows in your table) for use by the system or application administrator.

Setting Local Policy

You may choose, as a matter of local policy, to reserve a block of rows for system administration. This policy allows you to define row entries within a reserved block of rows without being concerned that the row might already be taken by another user's entry. In compliance with the local policy, all other users should use row indices that are outside the reserved range when defining user-configured entries.

Reserving Blocks of Rows

By reserving a block of rows, you can define a consistent set of conditions (row entries) to be monitored across all machines such that the same condition is defined in the same row number on each machine. For example, you can use row 3000 in each table to define entries monitoring the number of accesses to the server (apacheServerPerfTotalAccesses). You can



then distribute this configuration to every host so that every system that is running Apache uses row 3000 for monitoring the number of accesses to the server in any of the SystemEDGE agent monitoring tables.

To reserve a block of rows for monitoring Apache:

1. Decide which block of rows you want to reserve for use with monitoring Apache.
2. Use that block of rows to define a set of row entries for each SystemEDGE self-monitoring table. For more information, refer to the chapter on self monitoring in the *eHealth SystemEDGE User Guide*.
3. Distribute configuration file entries to all hosts that are running the Apache Web server and *e*Health AIM for Apache. For more information, refer to the *Automating the Deployment of SystemEDGE and the AdvantEDGE Point Plug-in Modules* white paper.

   NOTE

   As an alternative, you can use this row-number assignment policy with AdvantEDGE View for group-configuration operations.

4. Require end users to avoid your block of rows when defining their own self-monitoring table entries.

Using the SystemEDGE Self-Monitoring Features

This section provides examples of how to use SystemEDGE process, threshold, and history monitoring to monitor the Apache Web server. Add these commands to the sysedge.cf file to enable monitoring of the MIB objects that they specify. Modify these examples as necessary to monitor the MIB objects and thresholds that are relevant for your configuration.

The examples in the following sections present row numbers in the 5000 range; select a row number for your configuration that conforms to local policies. For more information on row assignment, refer to "Assigning Entry Rows for the SystemEDGE Self-Monitoring Tables" on page 46.

The following command, for example, instructs the SystemEDGE agent to monitor whether the Apache process is alive at 30-second intervals and to store the data in row 5000 of the Process Monitoring table:

```
watch process procAlive 'httpd' 5000 0x0100 30 'Apache Web Server' ''
```

For more information about the syntax for the commands in this section, refer to the *eHealth SystemEDGE User Guide.*

NOTE

Enter the commands throughout this chapter on one line. Do *not* use a carriage return to match the formatting shown here.

Using SystemEDGE Process Monitoring

This section provides an example of how to use the SystemEDGE agent to monitor the availability of a critical Apache process. For more information, refer to the section on process and service monitoring in the *eHealth SystemEDGE User Guide.*

To ensure that the Apache Web server is running, enter the following command in the sysedge.cf file:

```
watch process procAlive 'httpd' 5000 0x0100 30 'Apache Web Server' ''
```

You must include the 0x0100 flag to force the SystemEDGE agent to monitor the parent process of the Apache process group.

Using SystemEDGE Threshold Monitoring

This section provides examples of how to use the SystemEDGE agent to monitor thresholds for important Apache metrics. Add the commands in the following sections to the sysedge.cf file to monitor thresholds for these MIB objects. For more information, refer to the section on threshold monitoring in the *eHealth SystemEDGE User Guide.*

NOTE

The thresholds in this section may not be appropriate for your Apache Web server. Select thresholds that are appropriate for your environment.

Monitoring Idle Apache Processes

To monitor the number of idle Apache processes on the server that is running on port 80, enter the following:

```
monitor oid apacheServerPerfCurrentIdleProcs.80 5000 0x0 60
absolute < 10 'Idle Server Processes' ''
```

Monitoring Total Resident Memory Size of an Apache Service

To monitor the total resident memory size of the Apache service that is running on port 80, enter the following:

```
monitor oid apacheFootprintTotalRSS.80 5001 0x0 60 absolute > 50000
'Total Resident Memory' ''
```

Monitoring Total Size of Apache Service Log Files

To monitor the total size of the log files for the Apache service that is running on port 80, enter the following:

```
monitor oid apacheFootprintTotalLogSize.80 5002 0x0 60
absolute > 100000 'Total Log Size' ''
```

Monitoring Total Size of Apache Service Document Files

To monitor the total size of the document files for the Apache service that is running on port 80, enter the following:

```
monitor oid apacheFootprintTotalDocSize.80 5003 0x0 60
absolute > 500000 'Total Document Size' ''
```

Using SystemEDGE History Collection

This section provides examples of how to use SystemEDGE history collection to track the value of important Apache metrics over time. Add the commands in the following sections to the sysedge.cf file to collect history for these MIB objects. For more information, refer to the section on history collection in the *eHealth SystemEDGE User Guide*.

NOTE

The number of samples and the interval between samples used in this section may not be appropriate for your Apache system; select values that are suitable for your environment.

Collecting History on Number of Hits to the Server

To collect history on the number of hits to the server on port 8080, enter the following:

```
emphistory 5000 60 apacheServerPerfTotalAccesses.8080 300 'Total Hits
To Port 8080 Server'
```

Collecting History on the Number of Current Active Users

To collect history on the number of current active users that are being maintained by the Apache server on port 8080, enter the following:

```
emphistory 5001 60 apacheServerPerfCurrentUsers.8080 300 'Total Users
On Port 8080 Server'
```

Glossary

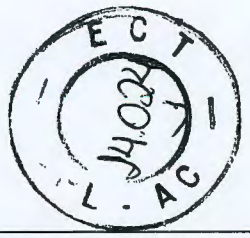
Abstract Notation One (ASN.1) A language that describes data types independent of computer structures and representations. For more information refer to ISO International Standard 8824.

Active Server Page (ASP) An HTML file that includes one or more scripts written using VBScript, JavaScript, or ActiveX Data Objects program statements. ASP files (named with the ".asp" suffix) receive a user request and create a customized Web page for the user (usually based on database information).

AdvantEDGE View A Web-based management interface for use with the SystemEDGE agent that enables an administrator to use a Web browser to manage systems and applications.

agent In network management, a program that provides information from a management information base (MIB) for SNMP agents. *e*Health or a network management system (NMS) use the information about managed devices and take corrective action when appropriate.

American Standard Code for Information Interchange (ASCII) The most common format for character representation in computers and the Internet. Characters fit into a single byte. It was developed by the American National Standards Institute (ANSI).



Apache A freely distributed Web server that runs on most UNIX, Linux, and Windows NT operating systems. For details about the Apache server, refer to the Apache Web site, http://www.apache.org.

application A program that performs a specific function for one or more users or for another application program. Types of applications include communication programs, management programs, word processors, databases, and drawing programs.

ASCII *See* American Standard Code for Information Interchange (ASCII).

ASN.1 *See* Abstract Notation One (ASN.1).

ASP *See* Active Server Page (ASP).

buffer A temporary storage area for data. Often implemented as holding areas between the backplane and an interface; data remains in the buffer until it can be transmitted on the interface or processed by the central processing unit (CPU).

central processing unit (CPU) The component within a device that performs the instruction execution for the applications and programs that run on the device. Also referred to as a processor or microprocessor.

CGI *See* Common Gateway Interface (CGI).

client A computer system, usually a desktop computer or laptop, that presents data directly to a user and accepts input. They drive the computing process, supporting local processing and accessing remote servers as needed for data access and analysis.

Also refers to the application software residing on a machine that is used by an end user.

Common Gateway Interface (CGI) A server-side interface for Web-based applications that defines how a Web server can exchange data with an application. The Active Server Pages (ASP) and Internet Server Application Program Interface (ISAPI) technologies are alternatives to CGI.

congestion A condition in which the network traffic is greater than the amount that the network can carry. Often causes performance problems and delays on a network.

CPU *See* central processing unit (CPU).

DHCP *See* Dynamic Host Configuration Protocol

DNS *See* domain name system (DNS).

domain name system (DNS) The system that locates and translates Internet domain names such as concord.com into Internet Protocol (IP) addresses. A DNS server is typically a device that translates domain names to IP addresses within your network.

Dynamic Host Configuration Protocol A protocol that enables dynamic allocation of IP addresses so that they can be reused.

***e*Health AIM** *See* eHealth application insight module.

***e*Health application insight module** A plug-in (supplementary program) that extends the functionality of the SystemEDGE agent. AIMs add the capability to manage application-specific events, processes, thresholds, and health.

event An occurrence on a system that typically results in a message, such as an SNMP trap, being sent to a configured management system. Common events include system failures, system reboots, exceeded thresholds, or any user-configurable situation that the user wants to identify.

file cache A block of memory that holds frequently or recently used data. A system can read those blocks at memory speed rather than the slower disk access speed.

File Transfer Protocol (FTP) A means for uploading and downloading files on the Internet (the oldest Internet protocol for retrieving files). You can use an FTP client application to request files from or transfer files to an FTP server.

FTP *See* File Transfer Protocol (FTP).

Host Resources MIB A MIB (management information base) that defines a set of objects that are useful for the management of host computers. For example, it defines host storage areas, devices, and file systems. This MIB is defined in RFC 1514.

hostname The name for an individual IP (Internet Protocol) address on a computer. While many computers have only one hostname, some machines, such as network servers have multiple hostnames.

HTML *See* Hypertext Markup Language (HTML).

HTTP *See* Hypertext Transfer Protocol (HTTP).

Hypertext Markup Language (HTML) A programmatic language used for controlling the way that text and images appear when a file is displayed on the World Wide Web.

Hypertext Transfer Protocol (HTTP) An application protocol that defines the set of rules for exchanging files (text, graphics, multimedia, and other files) on the World Wide Web.

I/O *See* input/output (I/O).

Information Technology (IT) A widely-used term to describe all of the technologies used for creating, exchanging, managing, and using information in various forms.

input/output (I/O) Any operation, program, or device that transfers data to or from a computer.

Internet Control Message Protocol (ICMP) A protocol between a server and a gateway to the Internet.

Internet Protocol (IP) The method (or protocol) by which packets of information are sent across the Internet. IP defines addressing, error handling, routing, and option codes for data transmission. IP requires no continuing connection between the endpoints that are communicating.

IP *See* Internet Protocol (IP).

IT *See* Information Technology (IT).

management information base (MIB) A formal description of a set of network objects that can be managed using Simple Network Management Protocol (SNMP).

MIB *See* management information base (MIB).

network A collection of computers, printers, routers, switches, and other devices that are able to communicate using a common transmission media such as TCP/IP.

network management system (NMS) An application program usually residing on a computer that manages at least part of a network, including systems and applications. The NMS communicates with agents to monitor network statistics and resources, control network device configuration, and analyze network problems. *See also* agent.

NMS *See* network management system (NMS).

object identifier (OID) a unique identifier of a managed object in a MIB hierarchy. *See also* management information base (MIB).

OID *See* object identifier (OID).

operating system (OS) The program that manages all other programs (applications or application programs) on a computer. Provides the following services: determining the order in which each application runs and the time allotted for that application, managing the sharing of internal memory among multiple applications and handling input to and output from attached hardware devices.

OS *See* operating system (OS).

packet A logical unit of data routed between an origin and a destination on the Internet or any other packet-switched network. On the Internet, the Transmission Control Protocol (TCP) layer of TCP/IP divides a file into packets of manageable size for routing.

packet-switched network A communications network in which data is transferred in small units called packets. Individual packets for a file may travel different routes. When all packets for a file reach their destination, the file is reassembled.

packet-switching A networking technology in which network nodes share bandwidth by sending packets. The same data path can be shared by many users in the network. Packet-switching is widely used throughout the Internet.

page In computers that utilize virtual memory, a unit of data storage. Systems transfer pages of data from disk storage to memory and back again.

On the World Wide Web, a file written using Hypertext Markup Language (HTML) that specifies how text, images, and other multimedia will be presented to the user. A Web site delivers information to the user one page at a time.

paging The process by which a computer moves portions of programs between random access memory and auxiliary storage (on disk).

partition A logical division of a hard disk on a PC that is created so that each partition can have a different operating system or can be used for different purposes (for example, file management or multiple users).

performance threshold The upper limit of acceptable response time.

ping An Internet echo message used to confirm the reachability of a network device. An abbreviation for Packet Internet or Inter-Network Groper.

process Typically, an instance of a program or application that is running on a server. Applications can have one or more associated processes.

protocol The set of rules by which the endpoints in a telecommunication connection communicate. The protocol defines the packet format of the transmitted information. On the Internet, common protocols are TCP, IP, HTTP and FTP.

queue In a system, a set of jobs awaiting resources. In a network device such as a router, a collection of packets waiting to be processed or forwarded. Insufficient central processing unit (CPU) speed, memory, or interface speeds can contribute to long queues, and therefore, to delay on the network.

real-time A level of computer responsiveness that an end user would deem as immediate or fast enough to show incremental changes of an external process (for example, to present visualizations of the weather as it constantly changes).

Request For Comments (RFC) The name of the document series regarding Internet design. Most RFCs define protocol specifications such as Telnet and FTP. RFCs are widely available online.

RFC *See* Request For Comments (RFC).

server A program that provides services to other programs in the same and other computers.

Also a computer that performs file storage and application hosting as well as provides computing services to other devices and users on the network. Typically has one or more central processing units (CPUs), disks, interfaces, and storage partitions.

Simple Network Management Protocol (SNMP) The network management protocol used almost exclusively in data networks. A method for monitoring and controlling network devices, as well as managing configurations, statistics collection, performance, and security.

SNMP *See* Simple Network Management Protocol (SNMP).

SNMP agent A program such as the SystemEDGE agent that conforms to a management information base (MIB) specification to collect information about managed devices and to take corrective action (using SNMP traps) when appropriate.

SystemEDGE agent Concord's SNMP agent that autonomously monitors system configuration, status, performance, users, applications, file systems, and other critical resources.

Systems Management MIB A set of MIB (management information base) objects that extends the capabilities of the Host Resources MIB. It provides greater visibility into systems and specific information about Windows NT and UNIX systems.

TCP/IP *See* Transmission Control Protocol (TCP) and "Internet Protocol (IP).

threshold *See* performance threshold.

Transmission Control Protocol (TCP) A connection-based protocol used along with the Internet Protocol (IP) to send data in the form of message units between computers over the Internet. While IP is responsible for the actual delivery of the data, TCP is responsible for dividing data into packets at the sending system and constructing the data message from individual packets at the receiving system.

trap A message sent by an SNMP agent to a console or network management system (NMS) to indicate that a threshold has been reached or another user-defined condition has occurred. The SystemEDGE agent defines a number of traps for system and application management.

UDP *See* User Datagram Protocol (UDP).

User Datagram Protocol (UDP) A communications protocol that uses Internet Protocol (IP) to send and receive data and is similar to Transmission Control Protocol (TCP), but provides fewer packet management services.

variable A performance metric for an element. A characteristic or behavior upon which *e*Health gathers data and evaluates the performance of the element. SystemEDGE agents can also monitor local variables to reduce network polls and increase scalability.

Web *See* World Wide Web (WWW, Web).

workstation A powerful computer that is equipped with a fast processor, a large amount of random access memory, and other features such as high-speed graphical rendering that make it suitable for business users such as engineers, graphic designers, and architects.

World Wide Web (WWW, Web) All of the resources on the Internet that use Hypertext Transfer Protocol (HTTP). Users of the Web access information through browser software.

Index

T

U

CONTACT CONCORD COMMUNICATIONS AT:

CONCORD COMMUNICATIONS, INC.
NORTH AMERICA
600 NICKERSON ROAD
MARLBORO, MASSACHUSETTS 01752
800-851-8725
P 508-460-4646
F 508-481-9772

CONCORD COMMUNICATIONS EUROPE
DELFTECHPARK 26
2628 XH DELFT
THE NETHERLANDS
P +31 (0) 15 2600 930
F +31 (0) 15 2600 929

CONCORD COMMUNICATIONS ASIA PACIFIC
LEVEL 7, 53 WALKER STREET
NORTH SYDNEY NSW 2060
AUSTRALIA
P 61-2-9965-0600
F 61-2-9929-0411

FRANCE: +33 (0) 1 4692 2420
GERMANY +49 (0) 89 944 90 105
UK: 00800 3283 2888

JAPAN 813-5778-7629
SINGAPORE: 65-4309533

CONCORD.COM

Manual 29

eHealth Service Response User Guide

Job Title:

Time Queued: Thu Jun 24 [illegible] 2003

Time Printed: Thu Jun 24 [illegible] 2003

Submitted By: Administrator [illegible]

Need help? Call your local NCO HelpDesk.

eHealth Service Response User Guide

09-16020-005
December 2001

Important Notice

Proprietary Notice

U. S. Government Restricted Rights

Patent Information

U. S. Patent 5,615,323
Patents Pending

Table of Contents

Preface

This guide explains how to install, license, and configure *e*Health Service Response Release 1.2 Patchlevel 2. This release of *e*Health Service Response supports the monitoring of common Internet applications on the following operating systems:

- Solaris 2.x and later
- HP-UX 10.x and 11.x
- IRIX 6.x
- AIX 4.2 and later
- Microsoft Windows 4.0, Windows 2000, and Windows XP
- Red Hat Linux 6.0 and later

This release of *e*Health Service Response supports *e*Health SystemEDGE Release 4.0 Patchlevel 3 and later.

Audience

This guide is intended for the person who is installing and configuring *e*Health Service Response to monitor the response time and availability of critical Internet applications. To use this guide, you must have a basic familiarity with the SystemEDGE agent, the Internet applications you are monitoring, and your host's operating system environment.

About This Guide

This section describes the changes and enhancements that have been made since the last release of this guide. It also includes the documentation conventions used in this guide.

Revision Information

Since Release 1.2 Patchlevel 1, this guide has been updated to use a new documentation template and to include a glossary.

Documentation Conventions

Table 1 lists the conventions used in this document.

Table 1. Documentation Conventions (Page 1 of 2)

Convention	Description
File or Directory Name	File or directory names.
`code`	System, code, or operating system command line examples.
emphasis	Emphasis and guide titles.
`enter`	Text that you must type exactly as shown.
Name	Text that defines menus, fields in dialog boxes, or keyboard keys.
New Term	A new term, that is, one that is being introduced.
`Variable`	Variable values that you substitute.
→	A sequence of menus or menu options. For example, **File** → **Exit** means "Choose **Exit** from the **File** menu."

Table 1. Documentation Conventions (Page 2 of 2)

Convention	Description
NOTE	Important information, tips, or other noteworthy details.
CAUTION	Information that helps you avoid data corruption or system failures.
WARNING	Information that helps you avoid physical danger.

Customer Support

If you need any assistance with *e*Health Service Response, contact Customer Support at the following:

Phone: (888) 832-4340
(508) 303-4300
Fax: (508) 303-4343
E-mail: support@concord.com
Web site: http://www.concord.com

Professional Services

If you need any assistance with customizing *e*Health Service Response, contact Professional Services at the following:

Phone: (800) 851-8725 (Choose option 7)
Fax: (508) 486-4555
E-mail: proserv@concord.com
Web site: http://www.concord.com

Introduction

Introducing *e*Health Service Response

*e*Health Service Response is a plug-in to the SystemEDGE agent that monitors the response and availability of critical network services. Through the Service Response plug-in, the SystemEDGE agent performs real, active test transactions to measure response time and track availability for the following Internet applications from a user's perspective:

- Domain Name System (DNS)
- File Transfer Protocol (FTP)
- Hypertext Transfer Protocol (HTTP)
- Secure HTTP (HTTPS)
- Packet Inter-Network Groper (PING)
- Network News Transfer Protocol (NNTP)
- Post Office Protocol version 3 (POP3)
- Simple Mail Transfer Protocol (SMTP)
- Transmission Control Protocol connections (TCPConnect)

*e*Health Service Response also enables you to define your own service tests through custom scripts and programs. You can perform these measurements from any system within the enterprise network.

Using *e*Health Service Response

*e*Health Service Response provides the flexibility you need to monitor service delivery. You can use *e*Health Service Response to monitor all critical applications on a single system or to monitor a particular service or application across a group of systems. You can also modify Service Response tests in real time so that you always get the information you need.

The SystemEDGE agent provides configuration and reporting for the Service Response module through Simple Network Management Protocol (SNMP). Its self-monitoring and autonomous management capabilities work with the data that *e*Health Service Response gathers.

You can configure *e*Health Service Response and the SystemEDGE agent to do the following:

- Monitor the response times of various Web servers and send a warning when the servers become unavailable.
- Warn you of response slowdowns or unavailable applications.
- Test site access and issue an alarm if it detects a service disruption.

Performance Criteria Measured by *e*Health Service Response

Table 2 shows the performance criteria that *e*Health Service Response measures and reports for services.

Table 2. Performance Criteria for Each Service

Criterion	Description
Availability	Percentage of successful service requests.
Name Lookup Time	Time required to resolve the server name for the service to a network address. *e*Health Service response provides values for Last Sample, Mean, Minimum, Maximum, and Sample Variance.
Connection Time	Time required to connect to the server providing this service. *e*Health Service response provides values for Last Sample, Mean, Minimum, Maximum, and Sample Variance.
Transaction Time	Time required to perform the requested transaction, after the connection is established. For example, this value could be the amount of time required to download the Web page or check the mail status. *e*Health Service response provides values for Last Sample, Mean, Minimum, Maximum, and Sample Variance.
Total Response Time	Total time required for the given service to correctly respond to the request. This value is simply the sum of the other three measurements: Name Lookup Time, Connection Time and Transaction Time. *e*Health Service response provides values for Last Sample, Mean, Minimum, Maximum, and Sample Variance.

Configuration Options

*e*Health Service Response allows you to configure service measurement mechanisms to best meet the needs of your network environment. Table 3 shows the options that you can specify for each measurement entry.

Table 3. Configuration Options for Each Measurement Entry

Option	Description
Target Host	Host that provides the service to be tested.
Timeout	Time (in seconds) to wait before canceling the service request.
Sample Interval	Interval at which to perform the sample operation. For example, set this value to 60 to instruct Service Response to query the DNS server every 60 seconds.
Samples Per Interval	Number of samples to take at each interval. For example, set this option to 3 to instruct Service Response to PING the server three times in succession at each interval.
Sample Window	Time (in seconds) over which to make the statistics calculations. Service Response calculates the statistics over a sliding window of the most samples. For example, set this value to 600 to instruct Service Response to use all samples it took during the past 10 minutes to calculate the results.

For several of the services, *e*Health Service Response requires additional configuration information to complete the sample transactions. Table 4 shows the additional information that is required for each service.

Table 4. Information Required for Each Service (Page 1 of 2)

Service	Additional Information Required
HTTP	Target URL [proxy host][username:user password:pass]
HTTPS	Target URL [proxy host][username:user password:pass]
SMTP	None
POP3	User name and password for valid POP user

Table 4. Information Required for Each Service (Page 2 of 2)

Service	Additional Information Required
DNS	Internet name to lookup
NNTP	None
FTP	User name and password for valid FTP user
PING	Packet size
TCPCONNECT	Port number
CUSTOM	Name of script to run for each sample

Using *e*Health Service Response with AdvantEDGE View

You can use *e*Health Service Response with AdvantEDGE View to run queries for monitoring the response and availability of Internet applications.

To run an AdvantEDGE View Application query for Service Response:

1. Select the target system or group from the **System** or **Group** list.
2. Select **Service Response** from the **Applications** list.
3. Click the **Applications** icon.

AdvantEDGE View runs the query for the specified application on the system or group you selected.

NOTE

If you run a query for a group of systems, AdvantEDGE View may request additional information before running the query. For more information, refer to the AdvantEDGE View Web Help.

AdvantEDGE View displays the response time, service availability, and configuration details for all of the services that are running on the system or group that you selected. Figure 1 shows the Mean Service Response Times portion of the AdvantEDGE View Service Response query.

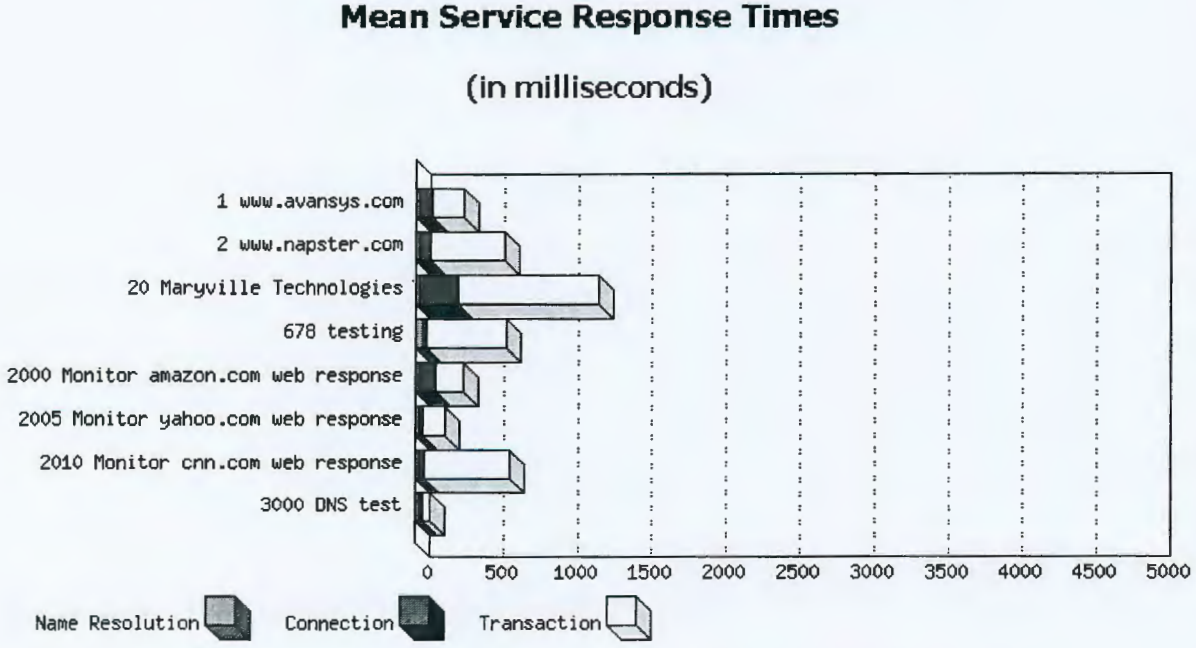


Figure 1. Sample Portion of AdvantEDGE View Service Response Query

2 Installing eHealth Service Response

Throughout this guide, the term Windows NT encompasses Windows NT 4.0, Windows 2000, and Windows XP.

This chapter describes how to install and license *e*Health Service Response for UNIX and Windows NT systems. If you are installing the software on a UNIX system, refer to "Installing eHealth Service Response on UNIX Systems." If you are installing the software on a Windows NT system, refer to "Installing eHealth Service Response on Windows NT Systems" on page 2-18.

Before installing *e*Health Service Response, you must install, license, and configure the SystemEDGE agent Release 4.0 Patchlevel 3 or later. For more information, refer to the *eHealth SystemEDGE User Guide*.

Installing *e*Health Service Response on UNIX Systems

This section describes how to install *e*Health Service Response on UNIX systems.

Installing the Software

*e*Health Service Response for UNIX systems is distributed as a tar file named svcrsp.tar.

To install the software:

1. Log in as root by entering **su** and the root password at the command prompt.

2. Verify that the plugins directory exists in the SystemEDGE agent distribution area. For most systems, the recommended directory is /opt/EMPsysedge/plugins. If that directory does not exist, verify that you have SystemEDGE agent Release 4.0 Patchlevel 3 or later installed, and then create the directory manually.
3. Insert the CD containing the software distributions into the CD-ROM drive and mount it on the partition /cdrom. For mounting instructions, refer to your system documentation. For example, enter the following command for Solaris systems:

   ```
   mount -r -t hsfs /dev/sr0 /cdrom
   ```

4. Change directory to the *e*Health Service Response home directory, and load the files from the CD-ROM. For example, enter the following commands for Solaris systems:

   ```
   cd /opt/EMPsysedge/plugins
   tar xvof /cdrom/svcrsp/sol2/svcrsp.tar
   ```

   *e*Health Service Response is now installed.
5. Review the installed files. For more information, refer to "eHealth Service Response Files" on page 2-20.
6. License *e*Health Service Response. For more information, refer to "Licensing eHealth Service Response" on page 23.

Installing *e*Health Service Response on Windows NT Systems

This section describes how to install *e*Health Service Response on Windows NT systems.

Installing the Software

*e*Health Service Response for Windows NT is distributed as a self-extracting executable named svcrsp.exe.

To install *e*Health Service Response:

1. Log on to the Windows NT system as **administrator**.
2. Select **Start** → **Programs** → **Command Prompt**.
3. Insert the CD-ROM that contains the Concord software distributions into the CD-ROM drive.

   Windows NT automatically mounts the drive using the CD-ROM drive's corresponding drive letter. The drive letter is specific to your system and depends on the number and types of disks attached to your system. Step 5 in this procedure uses `D:` as the CD-ROM drive. Modify that step if necessary to use the drive letter for your system's CD-ROM drive.
4. Determine which directory you want to use as the installation directory for *e*Health Service Response. If the SystemEDGE agent is installed in C:\sysedge, the recommended installation directory is C:\sysedge\plugins.
5. Run the self-extracting executable by typing the following at the command prompt:

```
D:\svcrsp\ntx86\svcrsp.exe -dir C:\sysedge\plugins
```

   where `D:` is the CD-ROM drive for your system, and `C:\sysedge\plugins` is the installation directory.

   NOTE

   The -dir option instructs the self-extracting executable to recreate the intended sub-directory hierarchy described throughout this guide. This command places the distribution in a svcrsp subdirectory within the specified target directory (for example, C:\sysedge\plugins\svcrsp).

   *e*Health Service Response is now installed.
6. Review the installed files. For more information, refer to "eHealth Service Response Files" on page 2-20.
7. License *e*Health Service Response. For more information, refer to "Licensing eHealth Service Response" on page 23.

*e*Health Service Response Files

This section describes the files installed with *e*Health Service Response.

Files Installed for UNIX Systems

Table 5 shows the files that the *e*Health Service Response installation program installs on UNIX systems.

Table 5. Files Installed on UNIX Systems

File	Description
collector.exe	*e*Health Service Response collector program.
svcrsp.asn1	*e*Health Service Response MIB specification.
svcrsp.cf.example	Sample configuration file for *e*Health Service Response.
svcrsp.pdf	*eHealth Service Response User Guide.*
svcrsp.so	Shared library module for *e*Health Service Response.
svcwatch	Configuration utility program for *e*Health Service Response.
svcwatch.1	Manual page that explains how to use the svcwatch utility.

Files Installed for Windows NT Systems

Table 6 shows the files that the *e*Health Service Response installation program installs on Windows NT systems.

Table 6. Files Installed on Windows NT Systems (Page 1 of 2)

File	Description
collector.exe	*e*Health Service Response collector program.
svcrsp.asn1	*e*Health Service Response MIB specification.
svcrsp.dll	Dynamic link library (DLL) module for *e*Health Service Response.
svcrsp.cf.example	Sample configuration file for *e*Health Service Response.

Table 6. Files Installed on Windows NT Systems (Page 2 of 2)

File	Description
svcrsp.pdf	*eHealth Service Response User Guide.*
svcwatch.exe	Configuration utility program for *e*Health Service Response.
svcwatch.txt	Text file that explains how to use the svcwatch utility.

2

Files Created for UNIX and Windows NT Systems

*e*Health Service Response also creates two files while it is running. It creates these files in the directory that contains the executables and configuration files. Table 7 shows the files that *e*Health Service Response creates.

Table 7. Files Created for UNIX and Windows NT Systems

File Name	Description
svcrsp.dat	Shared data file used by the collector.
svcrsp.lck	Lock file for access control.

Configuring *e*Health Service Response Startup

You must edit the sysedge.cf file to use the correct shared library file for your system and to enable the SystemEDGE agent to load *e*Health Service Response. You can use the sysedge_**plugin** keyword in the sysedge.cf configuration file to specify which plug-in modules the SystemEDGE agent will load at system initialization. By default, the SystemEDGE agent does not load any plug-ins at initialization, but you can edit the sysedge.cf file to configure the agent to load any plug-ins that you have installed.

The sysedge.cf file is located in your system directory by default; for example, it is located in the /etc/sysedge.cf directory on UNIX systems and in the C:\winnt\system32 directory on Windows NT systems. For more information about the sysedge.cf file, refer to the *eHealth SystemEDGE User Guide*.

NOTE

To configure the SystemEDGE agent to start *e*Health Service Response, you must provide the complete pathname to the shared library file for your version of *e*Health Service Response. The path depends on the location you selected when you installed *e*Health Service Response.

Table 8 shows the recommended path names for the shared library file for each operating system. Add the command shown in the right column to your sysedge.cf file to instruct the SystemEDGE agent to load *e*Health Service Response at system initialization.

Table 8. sysedge.cf Entries

Platform	Recommended sysedge.cf Entry
Solaris SPARC (32-bit)	sysedge_plugin /opt/EMPsysedge/plugins/svcrsp/svcrsp.so
Solaris SPARC (64-bit)	sysedge_plugin /opt/EMPsysedge/plugins/svcrsp/svcrsp-sparcv9.so
Windows NT, Windows 2000, or Windows XP (x86)	sysedge_plugin \sysedge\plugins\svcrsp\svcrsp.dll
HPUX 10.x and 11.x	sysedge_plugin /opt/EMPsysedge/plugins/svcrsp/svcrsp.so
Linux	sysedge_plugin /opt/EMPsysedge/plugins/svcrsp/svcrsp.so
AIX	sysedge_plugin /usr/lpp/EMPsysedge/plugins/svcrsp/svcrsp.so
IRIX	sysedge_plugin /opt/EMPsysedge/plugins/svcrsp/svcrsp.so

Licensing *e*Health Service Response

Like the SystemEDGE agent, *e*Health Service Response utilizes a host-based license method. Copies of *e*Health Service Response can run only on systems that possess a valid license key. This license key is separate from the one used for the SystemEDGE agent.

The first time that you attempt to start the SystemEDGE agent after installing *e*Health Service Response, the agent displays a message stating that it could not find a valid license for *e*Health Service Response. It then provides you with a **public key** that is used to generate a permanent license key for your host machine.

A license key is composed of four space-separated, 8-character sequences, totaling 32 characters. The sysedge.lic file contains the license for *e*Health Service Response, as well as the SystemEDGE agent license and licenses for any *e*Health application insight modules (AIMs) that you have installed. For an example, refer to the sample license file in "Sample License File" on page 30.

Obtaining a License

To obtain a license, you can do any of the following:

- Run the Concord-supplied licenseutil.pl script.
- Run the licenseme.exe license utility.
- Use AdvantEDGE View to receive an SNMP license trap or to query and license the plug-in without a trap. For more information, refer to "Generating a License through AdvantEDGE View Event Processing" on page 27 or "Generating a License through AdvantEDGE View Host Administration" on page 29.
- Send an e-mail request to licenses@concord.com and place the returned license key in the appropriate license file.

NOTE

Always include the user name in license requests that you send through e-mail.

- Complete the online license form through the Internet, as described in the next section, "Generating the License through the Web-based License Form."

For more information about licensing, refer to the *eHealth SystemEDGE User Guide*.

Generating the License through the Web-based License Form

This section describes how to generate the license using the Web-based license form.

NOTE

If you are using an evaluation copy of *e*Health Service Response, you must request a temporary license that will enable it to operate during the evaluation period.

To generate a license for *e*Health Service Response:

1. Start the SystemEDGE agent.

   Do the following for UNIX systems:

   a. Log in as **root**.

   b. Change directory (cd) to /opt/EMPsysedge.

   c. Enter the following:

   ```
   ./bin/sysedge -b
   ```

   Do the following for Windows NT systems:

   a. Log in as **administrator**.

   b. Open a command prompt window, and enter the following:

   ```
   C:\sysedge\setup -l
   ```

The SystemEDGE agent displays a message indicating that you need a license for the *e*Health Service Response module on this system. It displays a message similar to the following:

```
SystemEDGE Version 4.0 Patchlevel 3
Copyright 2001 by Concord Communications, Inc.
Please contact Concord Communications, Inc. to obtain a license
http://www.concord.com/support, Email: license@concord.com
Provide this: svcrsp pluto SunOS 5.8 8035b1f8f643ab43 1.2 Patchlevel 2
```

2. Using a Web browser, go to the licensing Web site at http://license.concord.com, and select the **Create License** option that matches your use of the module:
   - **Create SystemEDGE/AdvantEDGE Eval License** (if you are evaluating the module or are a Concord partner or reseller)
   - **Create SystemEDGE Outsource License** (if you are outsourcing the module)
   - **Create SystemEDGE/AdvantEDGE License** (if you have purchased the module)

   NOTE

   You must specify a user name and password to access the license form.

   If you do not have Web access, fill out the license request form, /config/license.txt (available as part of the *e*Health Service Response installation), with the complete string generated by the SystemEDGE agent, and e-mail the completed form to licenses@concord.com.
3. Fill out the license form, entering the information that was printed by the SystemEDGE agent. You must supply the following information:
   - Name
   - E-mail address

- Software version number (1.2 in the example on page 25)
- Patchlevel (2 in the example on page 25)
- System name (pluto in the example on page 25)
- Operating system name (SunOS in the example on page 25)
- Operating system version (5.8 in the example on page 25)
- System identifier (`8035b1f8f643ab43` in the example on page 25)

NOTE

Select the option for *e*Health Service Response from the product list on the licensing form.

After you submit the license request form, the Concord Web server generates a license and displays it on your Web browser. It also e-mails the license to the contact person in your organization.

4. Copy the license into the sysedge.lic file (located in /etc or C:\winnt\system32), and save that file.
5. Restart the SystemEDGE agent.

   For UNIX systems, enter the following:

   ```
   ./bin/sysedge -b
   ```

   For Windows NT systems, stop and start the Windows NT Master agent by entering the following:

   ```
   C:\net stop snmp
   C:\net start snmp
   ```

*e*Health Service Response is now licensed and ready to use.

Generating a License through AdvantEDGE View Event Processing

In order to use AdvantEDGE View event processing to license *e*Health Service Response, your system must meet the following requirements:

- You must be using SystemEDGE Release 4.0 Patchlevel 3 or later with AdvantEDGE View.
- You must configure the SystemEDGE agent to send SNMP traps to AdvantEDGE View. For more information, refer to the section on configuring the SystemEDGE agent in the *eHealth SystemEDGE User Guide*.
- You must configure the SystemEDGE agent with a read-write community so that AdvantEDGE View can issue an SNMP Set to transmit the license key to it. For more information, refer to the section on configuring the SystemEDGE agent in the *eHealth SystemEDGE User Guide*.
- Your AdvantEDGE View system must have access to the Internet, either directly or through a Web proxy.
- The AdvantEDGE View user who is generating the license must have either write or admin permissions.

To generate a license through AdvantEDGE View:

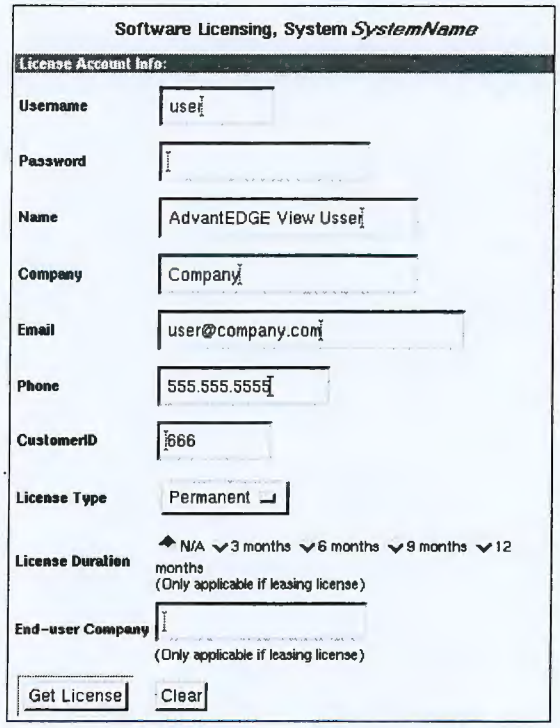
1. Start the SystemEDGE agent with *e*Health Service Response in unlicensed mode. SystemEDGE sends a license trap to AdvantEDGE View for that module.

2. Start AdvantEDGE View, and click the **Events** icon to display the Event Processing screen.

   AdvantEDGE View displays a license trap for the system that requires a license.

3. Click the index number for that system to view the Trap Details form for **License Software** to display the AdvantEDGE View Software Licensing form.

4. Complete the licensing form, and click **Get License**.



NOTE

If you have configured AdvantEDGE View preferences, AdvantEDGE View fills in all of the information (except password) on this form.

AdvantEDGE View contacts the Web-based license server, obtains a license for *e*Health Service Response, and issues an SNMP Set to the target SystemEDGE agent to inform it of the new software license key.

Generating a License through AdvantEDGE View Host Administration

You can also license systems through AdvantEDGE View Host Administration.

To access Host Administration:

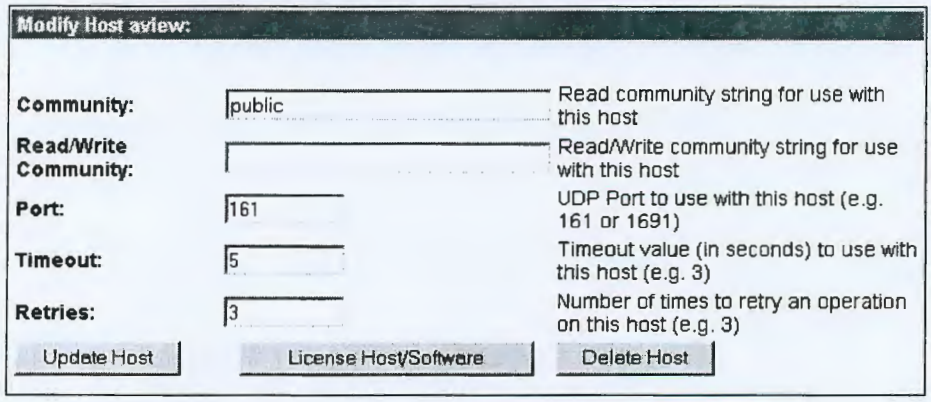
1. Start AdvantEDGE View, and click the **Administration** icon. AdvantEDGE View displays the Administration page.
2. Click the **Host Administration** icon. AdvantEDGE View displays the host list.

SystemEDGE Host Configuration

System Name	Community	Read/Write Community	Port	Timeout	Retries
avlewdemo	public		161	2	2
mailserver	public		161	6	3
nethealth	public		161	3	3
ntclient	public		161	6	3
ntserver	public		161	3	2
unixclient	public		161	6	3
unixserver	public		161	3	3
win2kclient	public		161	5	3
www	public		161	6	3

Add New Host

3. Click the name of the system that you want to license from the **System Name** column. AdvantEDGE View displays the Modify Host form.



4. Click **License Host/Software** to display the licensing form.
5. Select the product you want to license from the **Product** list, and then click **License Software**.

   AdvantEDGE View contacts the Web-based license server, obtains a license for the software, and issues an SNMP Set to the target SystemEDGE agent, informing it of the new software license key.

Sample License File

The following is a sample SystemEDGE agent license file. A pound character (#) in column 1 indicates that the entire line is a comment.

```
# license file for SystemEDGE Agent
# Concord Communications, Inc.
# http://www.concord.com
#
# file /etc/sysedge.lic or %SystemRoot%\system32\sysedge.lic
# A valid license key has four parts of 8 characters per part
# parts are separated by space(s) with one license key per line
# sysedge jupiter sol2 5.8 807cb1da007cb1da 4.1 PL 1
e13311d3 0F2a7cb1 abC512dc fF8C923a
# svcrsp pluto SunOS 5.8 807cb1da007cb1da 1.2 PL 2
a7943fde 098a87ij a4kiuf39 afafEkj4
```

Configuring eHealth Service Response

This chapter explains how to configure and use *e*Health Service Response.

The Service Response Table

*e*Health Service Response is implemented as an SNMP table in the Systems Management MIB. The Service Response table provides information about each of the services that the SystemEDGE agent is currently monitoring. Each row of the table represents a single monitored service. You can specify as many service monitor entries (rows) as necessary for your Service Response implementation. For each entry, the table provides information such as the service being monitored, specific arguments (for example, the URL to query), how often the agent checks the service, and the measurement results.

In addition to the Service Response table, *e*Health Service Response provides two additional MIB objects:

- svcRspVersion, which reports the *e*Health Service Response version information.
- svcRspPID, which reports the process identifier of the *e*Health Service Response collector process.

All MIB objects that are related to *e*Health Service Response exist at object identifier (OID) branch *1.3.6.1.4.1.546.16.6* in the Systems Management MIB. The MIB is defined in the svcrsp.asn1 file, which is installed as part of the *e*Health Service Response installation. Table 9 shows the columns of the Service Response table.

Table 9. Service Response Table (Page 1 of 5)

MIB Object	Permissions	Description
svcRspTableIndex	Read-Only	An integer (1 through MAXINT) that indicates the row index for this entry.
svcRspTableDescr	Read-Only	A textual description of the row entry. This field is entirely for the user and is not interpreted by the software.
svcRspTableSvc	Read-Write	An integer that indicates the type of service to be sampled. The following are possible values: • NNTP(1) • DNS(2) • POP3(3) • HTTP(4) • FTP(5) • SMTP(6) • PING(7) • TCPCONNECT(8) • CUSTOM(9) • HTTPS(10) Additional values will be defined in the future as new services are implemented.

Table 9. Service Response Table (Page 2 of 5)

MIB Object	Permissions	Description
svcRspTableArgs	Read-Write	A quoted string (0 through 128 characters) that specifies the service-specific arguments that the module uses for measuring purposes. The following are examples of service arguments: • DNS - dns-server hostname • HTTP - Target URL [proxy host][username:user password:pass] • HTTPS - Target URL [proxy host][username:user password:pass] • FTP - ftp-server username passwd • POP3 - pop3-server username passwd • NNTP - nntp-server • SMTP - smtp-server • PING - target-host [size] • TCPCONNECT - target-host port-number • CUSTOM - script-name
svcRspTableInterval	Read-Write	An integer value (30 through MAXINT) that indicates how often (in seconds) the agent should measure the service response. For example, the value 30 instructs the agent to sample theservice every 30 seconds. This value *must* be a multiple of 30 seconds
svcRspTableSamplesPerInterval	Read-Write	An integer value (1 through MAXINT) that indicates the number of times that the agent should perform the sample query at each interval. For example, you can specify 3 to perform a PING measurement three times each interval.
svcRspTableTimeout	Read-Write	An integer value (1 through MAXINT) that indicates the time (in seconds) that this measurement should wait for a response. A sample that does not return within the timeout value is recorded as "unavailable" for the purposes of the availability measurement.

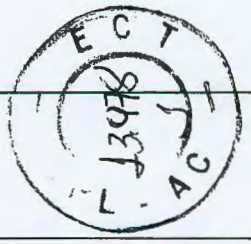


Table 9. Service Response Table (Page 3 of 5)

MIB Object	Permissions	Description
svcRspTableStatsWindow	Read-Write	An integer value (1 through MAXINT) that indicates the time in seconds to be used in the statistical calculations. For instance, a value of 1800 specifies that the agent will calculate all statistical results (for example, mean and availability) over the last 30 minutes.
svcRspTableStatus	Read-Write	Row status; one of the following values: • active • notInService • notReady • createAndGo • createAndWait These values are identical in meaning to the SNMPv2 SMI RowStatus textual convention. Normally, a row is either active or notInService.
svcRspTableLastUpdate	Read-Only	Time (based on sysUpTime) at which the agent last sampled this service. A value of 0 indicates that this service has not yet been sampled.
svcRspTableNumSamples	Read-Only	Total number of samples that the agent has taken for this response time entry since the row was initialized.
svcRspTableTotalLastSample	Read-Only	Last recorded total response time (in milliseconds) for this service. A value of 0 indicates that the last sample failed to respond within the given timeout.
svcRspTableTotalMin	Read-Only	Smallest successful total response time (in milliseconds) for this service during the current measurement window.
svcRspTableTotalMax	Read-Only	Largest successful total response time (in milliseconds) for this service during the current measurement window.

Table 9. Service Response Table (Page 4 of 5)

MIB Object	Permissions	Description
svcRspTableTotalMean	Read-Only	Sample mean of the successful total response times (in milliseconds) for this service during the current measurement window.
svcRspTableTotalVariance	Read-Only	Sample variance of the successful total response times (in milliseconds) for this service during the current measurement window.
svcRspTableTotalAvailability	Read-Only	Percentage of the total response measurement attempts that were successful during the current measurement window.
svcRspTableNameLastSample	Read-Only	Last recorded name lookup time (in milliseconds) for this service. A value of 0 indicates that the last sample failed to respond within the given timeout.
svcRspTableNameMin	Read-Only	Smallest successful name lookup time (in milliseconds) for this service during the current measurement window.
svcRspTableNameMax	Read-Only	Largest successful name lookup time (in milliseconds) for this service during the current measurement window.
svcRspTableNameMean	Read-Only	Sample mean of the successful name lookup times (in milliseconds) for this service during the current measurement window.
svcRspTableNameVariance	Read-Only	Sample variance of the successful name lookup times (in milliseconds) for this service during the current measurement window.
svcRspTableConnLastSample	Read-Only	Last recorded connection time (in milliseconds) for this service. A value of 0 indicates that the last sample failed to respond within the given timeout.
svcRspTableConnMin	Read-Only	Smallest successful connection time (in milliseconds) for this service during the current measurement window.

Table 9. Service Response Table (Page 5 of 5)

MIB Object	Permissions	Description
svcRspTableConnMax	Read-Only	Largest successful connection time (in milliseconds) for this service during the current measurement window.
svcRspTableConnMean	Read-Only	Sample mean of the successful connection times (in milliseconds) for this service during the current measurement window.
svcRspTableConnVariance	Read-Only	Sample variance of the successful connection times (in milliseconds) for this service during the current measurement window.
svcRspTableTranLastSample	Read-Only	Last recorded transaction time (in milliseconds) for this service. A value of 0 indicates that the last sample failed to respond within the given timeout.
svcRspTableTranMin	Read-Only	Smallest successful transaction time (in milliseconds) for this service during the current measurement window.
svcRspTableTranMax	Read-Only	Largest successful transaction time (in milliseconds) for this service during the current measurement window.
svcRspTableTranMean	Read-Only	Sample mean of the successful transaction times (in milliseconds) for this service during the current measurement window.
svcRspTableTranVariance	Read-Only	Sample variance of the successful transaction times (in milliseconds) for this service during the current measurement window.

Sample Entry in the Service Response Table

The following shows a sample entry in the Service Response table for monitoring the HTTP service.

Index	Service	Arguments	Interval	SamplesPerInterval	Timeout	StatsWindow	Status
10	HTTP(4)	"http://www.empire.com"	60	1	10	3600	ACTIVE(1)

The entry is the 10th row in the table, and its purpose is to monitor the HTTP service by retrieving the Web page that is located at http://www.empire.com. The agent performs this query once every 60 seconds with a timeout of 10 seconds. The value of 3600 in the statistics window column indicates that the agent uses only the last 3600 seconds (or 1 hour) of samples to calculate statistical results. The current status of this row is active.

Assigning Entry Rows for the Service Response Table

The svcRspTableIndex column is the row index of the Service Response table, and it acts as a key field to distinguish rows in the table. You may choose, as a matter of local policy, to reserve a block of rows to be used solely for system administration. By reserving a block of rows, you can define a consistent set of conditions (row entries) to be monitored across all systems such that the same condition is defined in the same row number on each of the systems. For example, you might use row 11 (svcRspTableIndex = 11) to define an entry for monitoring the DNS service throughout the enterprise. You can then distribute this configuration to every system so that they all use row 11 to measure the DNS service.

To reserve a block of rows:

1. Decide on a block of rows that you want to reserve for your use in the Service Response table.

2. Define a set of row entries (services to be measured) in the svcrsp.cf configuration file (in the block of rows you decided to reserve). For more information, refer to the next section, "Configuring the Service Response Table."
3. Distribute the svcrsp.cf configuration file to all systems on which *e*Health Service Response is installed.
4. Require end users to avoid your block of rows when defining their own Service Response table entries.

Configuring the Service Response Table

You can control the services that *e*Health Service Response monitors by adding, deleting, or modifying entries in the Service Response table.

You can configure the Service Response table in one of the following ways:

- **Dynamically.** Use SNMP commands from a management station to modify the table. For more information, refer to the next section, "Dynamic Configuration During Operation." For information about how to use the SystemEDGE agent svcwatch utility to dynamically configure the agent to monitor MIB variables, refer to "Using the svcwatch Utility" on page 52.
- **At start-up initialization.** Specify the process attributes to monitor through the svcrsp.cf configuration file. For more information, refer to "Initial Configuration During Start-Up" on page 39.
- **Through AdvantEDGE View configuration.** For more information, refer to the AdvantEDGE View Web Help.

Dynamic Configuration During Operation

You can use your network management system (NMS) to issue SNMP SetRequest messages to the agent to modify the entries in the Service Response table. The agent uses the SNMPv2 SMI Row-Status textual convention for creating, deleting, and modifying rows in the table.

Each time the Service Response table is successfully modified, the agent updates the svcrsp.cf file to record the changes so that when the agent is restarted, it starts up with the same Service Response table configuration as it had when it was stopped.

NOTE

Service Response table entries are saved to the svcrsp.cf configuration file so that any changes made during the operation of the agent are preserved across agent and system restarts. You can edit the svcrsp.cf file *only* when the SystemEDGE agent is not running.

Initial Configuration During Start-Up

On start-up, *e*Health Service Response reads the svcrsp.cf file. You can use this file to specify the services that you want the agent to measure. If you are configuring several systems to measure services throughout an enterprise, you can create a single svcrsp.cf file and distribute that file to all of your systems.

The Service Response configuration file consists of a series of entries that are delimited by brackets ({ }). Within each entry, fields exist on separate lines. The format for an entry is as follows:

```
{
    Index
    Description
    Service
    Arguments
    Interval
    SamplesPerInterval
    Timeout
    Window Size
    SNMP Row Status
}
```

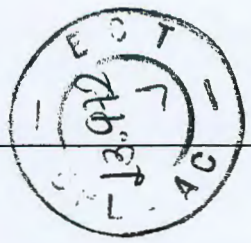


Table 10 describes each field of an entry in the svcrsp.cf file.

Table 10. Configuration File Entries

Entry	Description
Index	Row (index) of the Service Response table for this entry. Each row in the Service Response table is uniquely identified by an index number.
Description	Quoted string of up to 128 characters that describes the entry.
Service	Name of the service to be tested. Currently one of the following: • NNTP • DNS • POP3 • HTTP • HTTPS • FTP • SMTP • PING • TCPCONNECT • CUSTOM
Arguments	Quoted string of up to 128 characters that contains the service-specific parameters.
Interval	Measurement interval in seconds. This value must be a multiple of 30.
SamplesPerInterval	Number of samples to be taken at each interval.
Timeout	Sample timeout in seconds.
Window Size	Time window in seconds to use for calculating statistical results.
Row Status	SNMP row status for this row. Values of active or notInService are recommended.

Sample Entries for the svcrsp.cf Configuration File

This section contains several examples for using *e*Health Service Response to monitor services through entries in the svcrsp.cf file.

Measuring Web Server Response (HTTP)

The following entry instructs *e*Health Service Response to monitor the amount of time required to access the main Web page at www.cnn.com.

```
{
    6
    "Test CNN Web Server"
    HTTP
    "http://www.cnn.com/"
    60
    1
    20
    300
    active
    }
```

The entry is created as row 6 in the Service Response table. The agent tests the service once every 60 seconds and waits up to 20 seconds for a successful response. The agent calculates statistics over the last 300 seconds (5 minutes). This entry is active.

Measuring Web Server Response by Proxy (HTTP)

The following entry instructs *e*Health Service Response to monitor the amount of time required to access the main Web page at www.weather.com. In this case, the testing system does not access the site directly; instead, it uses the Web proxy host myproxy that is running on port 8080.

```
{
    6
    "Test Weather Channel Server Via Proxy"
    HTTP
    "http://www.weather.com/ myproxy:8080"
    60
    1
    20
    300
    active
}
```

The entry is created as row 6 in the Service Response table. The agents tests the service once every 60 seconds and waits up to 20 seconds for a successful response. The agent calculates statistics over the last 300 seconds (5 minutes). This entry is active.

Measuring Secure Web Server Response (HTTPS)

The following entry instructs *e*Health Service Response to monitor the amount of time required to access the main Web page at charge.mycredit.

```
{
      12
      "Test Secure Web Server"
"https://charge.mycredit/commit.exe username:empire password:tech"
60
1
20
300
active
}
```

The entry is created as row 12 in the Service Response table. The agent tests the service once every 60 seconds and waits up to 20 seconds for a successful response. The agent calculates statistics over the last 300 seconds (5 minutes). This entry is active.

Measuring Domain Name Service Response (DNS)

The following entry instructs *e*Health Service Response to monitor the amount of time required to resolve the IP address for www.cnn.com using the name server at 194.13.12.92. In this case, the agent is testing the response time for lookups at host 194.13.12.92. In your environment, use the IP address of your local DNS server. The actual name that is being resolved is not the most critical parameter.

```
{
    11
    "Test DNS Lookup"
    DNS
    "194.13.12.92 www.cnn.com"
    300
    1
    10
    86400
    active
}
```

The entry is created as row 11 in the Service Response table. The agent tests the service once every 300 seconds (5 minutes) and waits up to 10 seconds for a successful response. The agent calculates statistics over the last 86,400 seconds (1 day). This entry is active.

Measuring Sendmail Response (SMTP)

The following entry instructs *e*Health Service Response to monitor the amount of time required to connect to the SMTP service on host mailserver.yourdomain and to perform a null transaction. This test is a good measure of the baseline time that is required to send a mail message.

```
{
    7
    "Test Sendmail Response"
    SMTP
    "mailserver.yourdomain"
    60
    1
    10
    300
    active
}
```

The entry is created as row 7 in the Service Response table. The agent tests the service once every 60 seconds and waits up to 10 seconds for a successful response. The agent calculates statistics over the last 300 seconds (5 minutes). This configuration works well if you are using a polling station to sample the mean and availability values for this entry. This entry is active.

Measuring Post Office Protocol Service Response (POP)

The following entry instructs *e*Health Service Response to monitor the amount of time required to log in to and test the status of the POP mail service at host popserver.yourdomain. The username poptest and password pop123 must be a valid username-password combination for a POP user on this server. Any valid account works, and the sample query does not affect the contents of the mailbox.

```
{
    5
    "Test POPmail Response"
    POP3
    "popserver.yourdomain poptest pop123"
    300
    1
    10
    21600
    active
}
```

The entry is created as row 5 in the Service Response table. The agent tests the service once every 300 seconds (5 minutes) and waits up to 10 seconds for a successful response. The agent calculates statistics over the last 21,600 seconds (6 hours). This entry is active.

Measuring Network News Service Response (NNTP)

The following entry instructs *e*Health Service Response to monitor the amount of time required to connect to the NNTP service at host news.yourdomain and to perform a simple transaction.


```
{
    1
    "Test Net News Response"
    NNTP
    "news.yourdomain"
    3600
    1
    10
    86400
    active
}
```

The entry is created as row 1 in the Service Response table. The agent tests the service once every 3600 seconds (1 hour) and waits up to 10 seconds for a successful response. The agent calculates statistics over the last 86,400 seconds (1 day). This entry is active.

Measuring File Transfer Service Response (FTP)

The following entry instructs *e*Health Service Response to monitor the amount of time required to log in to and test the status of the FTP service at host ftpserver.yourdomain. The username ftptest and password ftp123 must be a valid username-password combination for an FTP user on this server. Any valid account works.

```
{
    2
    "Test FTP Service Response"
    FTP
    "ftpserver.yourdomain ftptest ftp123"
    3600
    1
    10
    604800
    active
}
```

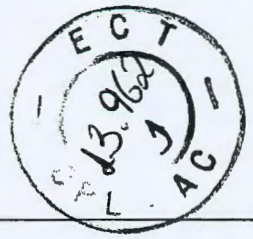
The entry is created as row 2 in the Service Response table. The agent tests the service once every 3600 seconds (1 hour) and waits up to 10 seconds for a successful response. The agent calculates statistics over the last 604,800 seconds (1 week). This entry is active.

Measuring Network Reachability (PING)

The following entry instructs *e*Health Service Response to monitor the amount of time required to perform a network-level ping of host server.yourdomain. This test is an excellent way to determine whether the system is up and network connectivity exists.

```
{
    3
    "Test PING Response"
    PING
    "server.yourdomain"
    60
    3
    5
    86400
    active
}
```

The entry is created as row 3 in the Service Response table. The agent tests the service 3 times every 60 seconds (1 minute) and waits up to 5 seconds for a successful response. The agent calculates statistics over the last 86,400 seconds (1 day). This entry is active.



Measuring TCP Service Connections

The following entry instructs *e*Health Service Response to monitor the amount of time required to connect to port 2049 on host server.yourdomain. This tes is an excellent way to determine whether the service is up and network connectivity exists.

```
{
    9
    "Test TCP Connection"
    TCPCONNECT
    "nfsserver.yourdomain 2049"
    60
    1
    5
    600
    active
}
```

The entry is created as row 9 in the Service Response table. The agent tests the service once every 60 seconds (1 minute) and waits up to 5 seconds for a successful response. The agent calculates statistics over the last 600 seconds (10 minutes). This entry is active.

Measuring Custom Services

The following entry causes *e*Health Service Response to execute the /local/bin/custom-response script and to use the output as the response time values for this custom service.

```
{
    99
       "Test Custom Service"
CUSTOM
    "/local/bin/custom-response"
    120
    1
    20
    3600
    active
}
```

The entry is created as row 99 in the Service Response table. The agent test the service once every 120 seconds (2 minutes) and waits up to 20 seconds for a successful response. The agent calculates statistics over the last 3600 seconds (1 hour). This entry is active.

You can create a custom script to perform any desired test or operation. You can write the script as a binary executable or in a scripting language such as UNIX shell or Perl. Custom response modules work very much like SystemEDGE agent extension objects. For more information, refer to the section on extension objects in the *eHealth SystemEDGE User Guide*.

*e*Health Service Response expects the custom script to provide a single line of output with three values followed by a line feed. It interprets the values as the name lookup time, connection time, and transaction time. The script must report all times in milliseconds.

Using the svcwatch Utility

svcwatch is a command-line utility that automatically configures *e*Health Service Response to monitor the service that you specify. You identify the service, arguments, measurement interval, timeout, and statistics window, and the svcwatch utility issues an SNMP SetRequest to create the appropriate entry in the target Service Response table.

Use svcwatch as follows:

```
svcwatch hostname[:port][,timeout] community command
```

Table 11 describes the svcwatch arguments.

Table 11. svcwatch Arguments

Argument	Description
hostname[:port][,timeout]	Specifies the hostname or IP address (in dotted quad notation) of the system that contains the agent and MIB object to be monitored. If the agent is running on an alternative UDP port (for example, 1691), specify that port number along with the hostname/address with a colon-separator. In addition, you can specify an optional SNMP timeout value (in seconds) using a command-separator.
community	Specifies the community string that svcwatch uses in its SNMP requests to the agent. Because svcwatch uses SNMP SetRequests, the community string must provide read-write access to the target agent.
command	Specifies the command and associated arguments. Supported commands include the following: oid – for monitoring an object filesystem – for monitoring a file system list – for listing the current entries setstatus – for setting the status of an entry delete – for deleting an entry For more information about these commands, refer to the next section, "svcwatch Command Arguments."

svcwatch Command Arguments

These are the svcwatch commands and associated arguments:

- add *index "descr" service "arguments" interval samples timeout window*
- setstatus *index status*
- delete *index*
- list
- version

Table 12 describes the svcwatch arguments that are associated with the svcwatch commands.

Table 12. svcwatch Arguments Associated with Commands (Page 1 of 2)

Argument	Description
index	Specifies the row (index) of the Service Response table for this entry.
"descr"	Describes the rows in a quoted string of up to 128 characters.
service	Specifies the service to monitor. One of the following: • HTTP • HTTPS • FTP • NNTP • DNS • SMTP • POP3 • PING • TCPCONNECT • CUSTOM
"arguments"	Specifies the service-specific arguments in a quoted string of up to 128 characters.
interval	Specifies an integer value (30 to MAXINT) that indicates how often (in seconds) the service should be performed tested. This value *must* be a multiple of 30 seconds.

Table 12. svcwatch Arguments Associated with Commands (Page 2 of 2)

Argument	Description
samples	Specifies an integer value (1 to MAXINT) that indicates how many times the agent should monitor the service at each interval.
status	Row status; one of the following: • active – Activates a table row. • notInService – Deactivates but preserves a row. • destroy – Deletes a row.
timeout	Specifies the time in seconds to wait for the service (in an integer value).
window	Specifies the time window of samples to include in statistical calculations.

svcwatch Example

Enter the following to create an entry, at index 11 in the Service Response table, that tests the network reachability to the pingtarget system:

```
svcwatch 143.45.0.12 private add 11 "Test PING" PING
"pingtarget" 120 1 10 3600
```

Removing Service Response Entries

To stop the sampling of a particular service, you must remove the appropriate entry from the Service Response table. There are two options for removing these table entries:

- Manually removing the entry from the svcrsp.cf file
- Dynamically removing the entry with the svcwatch utility

Manually Removing an Entry

You can remove an entry from the Service Response table by removing the entry from the svcrsp.cf configuration file.

NOTE

Before you edit the svcrsp.cf file, you must stop the SystemEDGE agent.

To remove an entry from the svcrsp.cf file:

1. Stop the SystemEDGE agent. For more information, refer to the *eHealth SystemEDGE User Guide*.
2. Edit the file svcrsp.cf. Locate and remove the entry you want to delete. Remove the entire entry, including the bracket characters ({ and }).
3. Save the svcrsp.cf file.
4. Restart the SystemEDGE agent.

Dynamically Removing an Entry

To dynamically remove an entry from the Service Response table, use the svcwatch utility. The following example deletes row 14 from the Service Response table on the 143.45.0.12 system. Enter the following to remove that row from memory and from the svcrsp.cf file.

```
svcwatch 143.45.0.12 private delete 14
```

In some cases, it may not be possible to use the svcwatch utility to delete entries. For example, if you have configured the SystemEDGE agent to prevent SNMP SET operations, the svcwatch utility does not work. In this situation, you need to remove the Service Response entry from the table manually. For more information, refer to "Manually Removing an Entry" on page 54.

Using SystemEDGE Self-Monitoring to Monitor Service Response Metrics

This section describes how to use SystemEDGE threshold monitoring and history collection to monitor service-response metrics. In addition to using the svcrsp.cf file to add monitoring entries to the Service Response table, you can add entries directly to the SystemEDGE agent configuration file, sysedge.cf.

Each of the following examples presents a row number in the 5000 range; select a row number for your configuration that conforms to local policies. The metrics used in these examples were chosen for illustrative purposes only; you may choose to measure other metrics. You may also choose to use other thresholds, numbers of samples, and intervals between samples. Use values that make sense for your environment.

NOTE

Enter the commands throughout this section as one line. Do *not* use a carriage return to match the formatting shown here.

Using SystemEDGE Threshold Monitoring

This section provides examples for using SystemEDGE threshold monitoring to monitor Service Response metrics. Enter the following examples into the sysedge.cf file to instruct the agent to perform the monitoring they describe. For more information about SystemEDGE threshold monitoring, refer to the *eHealth SystemEDGE User Guide*.

There are nearly 30 useful values recorded for each Service Response entry. The most common values are the Mean Response Time (svcRspTableTotalMean) and Mean Availability (svcRspTableTotalAvailability). Other values also provide interesting real-time monitoring solutions. For example, you can monitor the variance (svcRspTableTotalVariance) to watch for periods of large variation in response.

Sending a Trap when a Service Fails to Respond

To configure the agent to send a trap when a service fails to respond, you must monitor the svcRspTableTotalLastSample MIB variable. This value records the last sampled response time (in milliseconds) for this service entry. If the last test failed, the value is zero.

If, for example, you have created a Web server response-monitoring entry at row index 100 of the Service Response table, and this entry tests the server every 60 seconds, set up a SystemEDGE self-monitoring entry to watch the samples for that row and send a trap if the value is zero. To do so, enter the following in sysedge.cf:

```
monitor oid svcRspTableTotalAvailability.100 5001 0x0 60
absolute = 0 'Web Server Down' ''
```

Sending a Trap when a Response Sample is Greater than 7000

To send a trap if any response sample is greater than 7000, enter the following in sysedge.cf:

```
monitor oid svcRspTableTotalLastSample.100 5002 0x0 60 absolute
> 7000 'Web Server Too Slow' ''
```

Sending a Trap when the Mean Response Time is Greater than 5000

To send a trap when the *mean* response time is greater than 5000, enter the following in sysedge.cf:

```
monitor oid svcRspTableTotalMean.100 10 0x0 60 absolute > 5000
'Web Server Too Slow On Average' ''
```

Sending a Trap when a New Maximum Value Appears

To send a trap whenever a new maximum value appears, regardless of the value, enter the following in sysedge.cf:

```
monitor oid svcRspTableTotalMax.100 10 0x0 60 delta > 0 'New
Maximum Web Server Response' ''
```

Using SystemEDGE History Collection

This section outlines the use of SystemEDGE history collection to track the value of important Service Response metrics over time. For more information about SystemEDGE history collection, refer to the *eHealth SystemEDGE User Guide*.

Collecting History on Mean Response Time

To collect historical data on the mean service response time, you must gather history on the svcRspTableTotalMean MIB variable. This value records the mean over the sample window for this service entry.

For example, if you have created a Web server response-monitoring entry at row index 100 of the Service Response table, and this entry tests the server every 60 seconds, you can set up a SystemEDGE History table entry to record the samples for that row. To do so, enter the following command in sysedge.cf:

```
emphistory 5002 60 svcRspTableTotalMean.100 400 'Web Response
History'
```

Collecting History on Connect Time

Enter this command to collect history on the connect time:

```
emphistory 5002 60 svcRspTableConnMean.100 400 'Web Connection
History'
```


Glossary

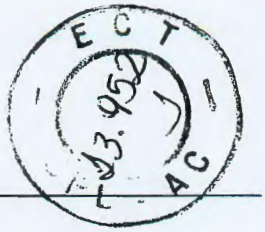
Abstract Notation One (ASN.1) A language that describes data types independent of computer structures and representations. For more information refer to ISO International Standard 8824.

access list A list of devices or IP addresses that can use a router, device, or application for particular services.

AdvantEDGE View A Web-based management interface for use with the SystemEDGE agent that enables an administrator to use a Web browser to manage systems and applications.

agent In network management, a program that provides information from a management information base (MIB) for SNMP agents. *e*Health or a network management system (NMS) use the information about managed devices and take corrective action when appropriate.

American Standard Code for Information Interchange (ASCII) The most common format for character representation in computers and the Internet. Characters fit into a single byte. It was developed by the American National Standards Institute (ANSI).



application A program that performs a specific function for one or more users or for another application program. Types of applications include communication programs, management programs, word processors, databases, and drawing programs.

ASCII *See* American Standard Code for Information Interchange (ASCII).

ASN.1 *See* Abstract Notation One (ASN.1).

availability The percentage of time that an element is operational during the report period.

bandwidth The throughput of a communications line usually measured in megabits per second (Mbps). Also refers to the difference between the highest and lowest frequencies in a communications channel, expressed in units of hertz (Hz), or cycles per second.

baseline A level of performance that is considered normal, average, or typical over a period of time such as a day, week, or month. Compare current performance metrics against baseline data to identify trends in performance levels and service delivery.

buffer A temporary storage area for data. Often implemented as holding areas between the backplane and an interface; data remains in the buffer until it can be transmitted on the interface or processed by the central processing unit (CPU).

capacity A measurement of the volume that an element can support. For interfaces, this is the bandwidth that can be carried. For hard disks, this is the disk size or the amount of information that can be stored on the disks.

central processing unit (CPU) The component within a device that performs the instruction execution for the applications and programs that run on the device. Also referred to as a processor or microprocessor.

client A computer system, usually a desktop computer or laptop, that presents data directly to a user and accepts input. They drive the computing process, supporting local processing and accessing remote servers as needed for data access and analysis.

Also refers to the application software residing on a machine that is used by an end user.

client process The client-side part of a distributed application.

connect time The total time that a user is connected to a network.

CPU *See* central processing unit (CPU).

delay The time required for a packet or frame to travel from the sending station (source) to the receiving station (destination).

DHCP *See* Dynamic Host Configuration Protocol

disk thrashing A condition that results when a server performs high disk input /output (I/O) operations—reads and writes to the disk—without producing actual work. Often occurs when a server performs excessive paging and swapping due to physical memory limitations.

DNS *See* domain name system (DNS).

domain name system (DNS) The system that locates and translates Internet domain names such as concord.com into Internet Protocol (IP) addresses. A DNS server is typically a device that translates domain names to IP addresses within your network.

Dynamic Host Configuration Protocol A protocol that enables dynamic allocation of IP addresses so that they can be reused.

***e*Health AIM** *See* eHealth application insight module.

eHealth application insight module A plug-in (supplementary program) that extends the functionality of the SystemEDGE agent. AIMs add the capability to manage application-specific events, processes, thresholds, and health.

event An occurrence on a system that typically results in a message, such as an SNMP trap, being sent to a configured management system. Common events include system failures, system reboots, exceeded thresholds, or any user-configurable situation that the user wants to identify.

fault tolerance A mechanism that protects networks and devices against downtime due to system failure. Fault tolerant solutions typically rely on redundancy in hardware and mirroring of applications and data.

file cache A block of memory that holds frequently or recently used data. A system can read those blocks at memory speed rather than the slower disk access speed.

File Transfer Protocol (FTP) A means for uploading and downloading files on the Internet (the oldest Internet protocol for retrieving files). You can use an FTP client application to request files from or transfer files to an FTP server.

filter A set of selection criteria used to focus a report on the desired data.

FTP *See* File Transfer Protocol (FTP).

Gbps An acronym representing gigabits per second, a common measurement of data transfer rates. One Gbps is equivalent to 10^9 bits per second.

group A collection of monitored elements. Typically, groups are used to organize elements by geographic location, department, market segment, vendor, or customer. Users can enter localized text for group names.

group list A set of one or more groups. Users can enter localized text for group list names.

Host Resources MIB A MIB (management information base) that defines a set of objects that are useful for the management of host computers. For example, it defines host storage areas, devices, and file systems. This MIB is defined in RFC 1514.

hostname The name for an individual IP (Internet Protocol) address on a computer. While many computers have only one hostname, some machines, such as network servers have multiple hostnames.

HTML *See* Hypertext Markup Language (HTML).

HTTP *See* Hypertext Transfer Protocol (HTTP).

Hypertext Markup Language (HTML) A programmatic language used for controlling the way that text and images appear when a file is displayed on the World Wide Web.

Hypertext Transfer Protocol (HTTP) An application protocol that defines the set of rules for exchanging files (text, graphics, multimedia, and other files) on the World Wide Web.

Hertz (Hz) A unit of frequency of one cycle per second that measures the change in the state of an alternating current, sound wave, or other cyclical wave form.

I/O *See* input/output (I/O).

ICMP *See* Internet Control Message Protocol (ICMP).

Information Technology (IT) A widely-used term to describe all of the technologies used for creating, exchanging, managing, and using information in various forms.

input/output (I/O) Any operation, program, or device that transfers data to or from a computer.

Integrated Services Digital Network (ISDN) A high-speed carrier service offered by telecommunications companies.

Internet Control Message Protocol (ICMP) A protocol between a server and a gateway to the Internet.

internet infrastructure The applications, systems, and networks that a company uses to run its business, for both internal use and for interfaces to the outside world.

Internet Protocol (IP) The method (or protocol) by which packets of information are sent across the Internet. IP defines addressing, error handling, routing, and option codes for data transmission. IP requires no continuing connection between the endpoints that are communicating.

Internet Service Provider (ISP) A company that provides individuals and companies with access to the Internet. ISPs also provide related services such as Web site building and virtual hosting.

IP *See* Internet Protocol (IP).

ISDN *See* Integrated Services Digital Network (ISDN).

ISP *See* Internet Service Provider.

IT *See* Information Technology (IT).

LAN *See* local area network (LAN).

latency A measure of delay, often network delay. Depending on the type of element, *e*Health reports can show two types of latency: round-trip latency, which is the length of time in milliseconds for a ping packet to travel from the *e*Health system to a polled element and back. Alternate latency, which is the length of time in milliseconds for a ping packet to travel from a network resource (the alternate latency source) such as a router to other critical network resources such as routers and servers (the alternate latency partner).

local area network (LAN) A shared communication medium that connects computers and devices over a limited area. The area limitations of a LAN usually result from the electrical signal limits of the medium.

management information base (MIB) A formal description of a set of network objects that can be managed using Simple Network Management Protocol (SNMP).

MB Megabytes.

Mbits Megabits.

MBps An acronym representing megabytes per second.

Mbps An acronym representing megabits per second, a common measurement of data transfer rates.

MIB *See* management information base (MIB).

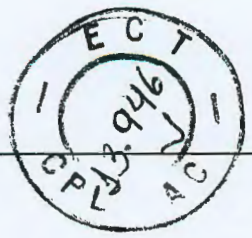
MIB Translation File (MTF) A file that normalizes the data collected from standard and proprietary SNMP (Simple Network Management Protocol) agents. *e*Health uses an MTF to translate MIB variables into its own variables. Each MTF consists of the associated MIB and its filename, an agent for the element type, and a set of statements that map MIB variables to the appropriate *e*Health database column.

mirroring A process by which data is duplicated on separate disk systems to provide faster access and fault tolerance in the event of a disk failure.

MTF *See* MIB Translation File (MTF).

network A collection of computers, printers, routers, switches, and other devices that are able to communicate using a common transmission media such as TCP/IP.

network management system (NMS) An application program usually residing on a computer that manages at least part of a network, including systems and applications. The NMS communicates with agents to monitor network statistics and resources, control network device configuration, and analyze network problems. *See also* agent.



Network News Transfer Protocol (NNTP) The predominant protocol used by computers for managing messages posted on Usenet newsgroups.

network operations center (NOC) The place where network administrators manage a telecommunications network or networks. It usually contains visualizations of the networks and workstations that are used to distribute software, troubleshoot problems, and monitor performance.

network time The time spent establishing network connections to complete a transaction.

NMS *See* network management system (NMS).

NNTP *See* Network News Transfer Protocol (NNTP).

object identifier (OID) a unique identifier of a managed object in a MIB hierarchy. *See also* management information base (MIB).

OID *See* object identifier (OID).

operating system (OS) The program that manages all other programs (applications or application programs) on a computer. Provides the following services: determining the order in which each application runs and the time allotted for that application, managing the sharing of internal memory among multiple applications and handling input to and output from attached hardware devices.

operational support system (OSS) A network management system (NMS) with a specific focus such as provisioning services or alarm surveillance.

OS *See* operating system (OS).

OSS *See* operational support system (OSS).

packet A logical unit of data routed between an origin and a destination on the Internet or any other packet-switched network. On the Internet, the Transmission Control Protocol (TCP) layer of TCP/IP divides a file into packets of manageable size for routing.

page In computers that utilize virtual memory, a unit of data storage. Systems transfer pages of data from disk storage to memory and back again.

On the World Wide Web, a file written using Hypertext Markup Language (HTML) that specifies how text, images, and other multimedia will be presented to the user. A Web site delivers information to the user one page at a time.

partition A logical division of a hard disk on a PC that is created so that each partition can have a different operating system or can be used for different purposes (for example, file management or multiple users).

path In networking, a path is a route from one location to another in a network.

PC *See* personal computer (PC).

personal computer (PC) A computer designed for individual use. Prior to the PC, computers were designed to be used by many individuals and system resources were shared by all. A PC often refers to a computer with an Intel microprocessor architecture and an operating system such as Microsoft DOS or Windows.

ping An Internet echo message used to confirm the reachability of a network device. An abbreviation for Packet Internet or Inter-Network Groper.

port The physical (hardware) connection on a device that connects the device to a network.

process Typically, an instance of a program or application that is running on a server. Applications can have one or more associated processes.

process set A collection of one or more processes that relate to a specific application. Using *e*Health – System At-a-Glance reports, you can obtain information about the impact and performance of process sets running on systems that have Concord SystemEDGE agents.

protocol The set of rules by which the endpoints in a telecommunication connection communicate. The protocol defines the packet format of the transmitted information. On the Internet, common protocols are TCP, IP, HTTP and FTP.

queue In a system, a set of jobs awaiting resources. In a network device such as a router, a collection of packets waiting to be processed or forwarded. Insufficient central processing unit (CPU) speed, memory, or interface speeds can contribute to long queues, and therefore, to delay on the network.

RAID *See* Redundant Array of Inexpensive Disks (RAID).

RAS *See* remote access server (RAS).

real time A level of computer responsiveness that an end user would deem as immediate or fast enough to show incremental changes of an external process (for example, to present visualizations of the weather as it constantly changes).

Redundant Array of Inexpensive Disks (RAID) A technology that merges several inexpensive disks into a single large disk to increase speed, capacity, and reliability. The RAID controller manipulates disks to share the work on file reads and writes for large files or to perform multiple simultaneous reads or writes for small files.

remote access server (RAS) A device that provides remote users with dial-up access to a network. RAS devices usually contain modem or Integrated Services Digital Network (ISDN) cards that provide the connection services.

remote network monitoring (RMON) A type of device that collects nine kinds of network management information, including packets sent, bytes sent, packets dropped, statistics by host, by conversations between two sets of addresses, and certain kinds of events that have occurred. A probe is an example of an RMON device.

Request For Comments (RFC) The name of the document series regarding Internet design. Most RFCs define protocol specifications such as Telnet and FTP. RFCs are widely available online.

RFC *See* Request For Comments (RFC).

RMON *See* remote network monitoring (RMON).

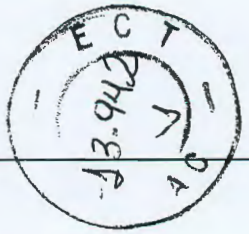
RMON2 A type of device that collects network management information as specified in the latest version of the MIB (management information base) specification, RMON, version 2. For more information, refer to RFC 2021, a document widely available on the Internet.

router A device that connects networks. Routers learn the addresses of the network points that send data by reading the address information in the data frames. Hardware vendors often use the terms router and switch interchangeably.

routing The process of finding paths through a network to a destination.

server A program that provides services to other programs in the same and other computers. Also, a computer that performs file storage and application hosting as well as provides computing services to other devices and users on the network. Typically has one or more central processing units (CPUs), disks, interfaces, and storage partitions.

server process A server-side part of a distributed application.



server time The amount of time that a server requires to process a transaction. It is calculated by determining network time and subtracting it from remote time.

server type The kind of server process associated with a particular server request protocol.

Simple Network Management Protocol (SNMP) The network management protocol used almost exclusively in data networks. A method for monitoring and controlling network devices, as well as managing configurations, statistics collection, performance, and security.

SNMP *See* Simple Network Management Protocol (SNMP).

SNMP agent A program such as the SystemEDGE agent that conforms to a management information base (MIB) specification to collect information about managed devices and to take corrective action (using SNMP traps) when appropriate.

speed The capacity (bandwidth) of an interface in bits per second (bps).

swapping The process in which a computer moves entire programs in and out of random access memory to and from auxiliary storage (swap partition or pagefile).

SystemEDGE agent Concord's SNMP agent that autonomously monitors system configuration, status, performance, users, applications, file systems, and other critical resources.

Systems Management MIB A set of MIB (management information base) objects that extends the capabilities of the Host Resources MIB. It provides greater visibility into systems and specific information about Windows NT and UNIX systems.

TCP/IP *See* Transmission Control Protocol (TCP) and "Internet Protocol (IP).

throughput The rate of data transfer on an interface over time.

Transmission Control Protocol (TCP) A connection-based protocol used along with the Internet Protocol (IP) to send data in the form of message units between computers over the Internet. While IP is responsible for the actual delivery of the data, TCP is responsible for dividing data into packets at the sending system and constructing the data message from individual packets at the receiving system.

trap A message sent by an SNMP agent to a console or network management system (NMS) to indicate that a threshold has been reached or another user-defined condition has occurred. The SystemEDGE agent defines a number of traps for system and application management.

Trivial File Transfer Protocol (TFTP) An Internet utility that uses User Datagram Protocol (UDP) instead of Transmission Control Protocol (TCP) to transfer files. TFTP is simpler than FTP, but does not support user authentication and directory visibility.

UDP *See* User Datagram Protocol (UDP).

User Datagram Protocol (UDP) A communications protocol that uses Internet Protocol (IP) to send and receive data and is similar to Transmission Control Protocol (TCP), but provides fewer packet management services.

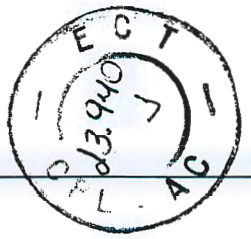
variable A performance metric for an element. A characteristic or behavior upon which *e*Health gathers data and evaluates the performance of the element. The SystemEDGE agents can also monitor local variables to reduce network polls and increase scalability.

variance A statistical term that indicates how closely most of the data points differ from the average of the data points.

WAN *See* wide area network (WAN).

Web *See* World Wide Web (WWW, Web).

wide area network (WAN) A network that interconnects multiple systems or networks over unlimited distances.



workstation A powerful computer that is equipped with a fast processor, a large amount of random access memory, and other features such as high-speed graphical rendering that make it suitable for business users such as engineers, graphic designers, and architects.

World Wide Web (WWW, Web) All of the resources on the Internet that use Hypertext Transfer Protocol (HTTP). Users of the Web access information through browser software.

Index

M

N

O

P

Q

R

S

T

U

V

W

CONTACT CONCORD COMMUNICATIONS AT:

CONCORD COMMUNICATIONS, INC.
NORTH AMERICA
600 NICKERSON ROAD
MARLBORO, MASSACHUSETTS 01752
800-851-8725
P 508-460-4646
F 508-481-9772

CONCORD COMMUNICATIONS EUROPE
DELFTECHPARK 26
2628 XH DELFT
THE NETHERLANDS
P +31 (0) 15 2600 930
F +31 (0) 15 2600 929

CONCORD COMMUNICATIONS ASIA PACIFIC
LEVEL 7, 53 WALKER STREET
NORTH SYDNEY NSW 2060
AUSTRALIA
P 61-2-9965-0600
F 61-2-9929-0411

FRANCE: +33 (0) 1 4692 2420
GERMANY +49 (0) 89 944 90 105
UK: 00800 3283 2888

JAPAN 813-5778-7629
SINGAPORE: 65-4309533

CONCORD.COM

Manual 30

ADVANTEDGE FOR MICROSOFT SQL Server

ADVANTEDGE

FOR MICROSOFT SQL SERVER

User Guide

Release 1 and Later

09-16070-002
May 2001

Important Notice

Application Health, Server Health, Live Health, SystemEDGE, AdvantEDGE, *e*Health, FirstSense Enterprise, FSagent, FServer, FStransaction, FSterminal, FSconsole, FScontroller, FSpro, Infrasense, MIB Manager, and the FirstSense logo are trademarks of Concord Communications, Inc.

The Total View, Concord, the Concord logo, Network Health, TRAKKER, FirstSense, and We See It Happening are registered trademarks of Concord Communications, Inc.

Adobe, Acrobat, and the Acrobat logo are trademarks, which may be registered in certain jurisdictions, and PostScript is a registered trademark of Adobe Systems Incorporated.
Intel is a registered trademark of Intel Corporation.
Microsoft, Microsoft SQL Server, Windows, and Windows 2000 are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

SMIC. Copyright 1992 SynOptics Communications, Inc. All Rights Reserved. SynOptics makes no representations about the suitability of this software for any particular purpose. The software is supplied "as is", and SynOptics makes no warranty, either express or implied, as to the use, operation, condition, or performance of the software. SynOptics retains all title and ownership in the software.

Network Health incorporates compression code by the Info-ZIP group. There are no extra charges or costs due to the use of this code, and the original compression sources are freely available from ftp://ftp.cdrom.com/pub/infozip/ on the Internet and from the Concord Communications Web site: http://www.concord.com.

Copyright Bigelow and Holmes 1986, 1985. Lucida is a registered trademark of Bigelow & Holmes. Sun Microsystems Inc., AT&T, and Bigelow & Holmes make no representations about the suitability of the source code for any purpose. It is provided "as is" without express or implied warranty of any kind.

General Notice: Some of the product names used herein have been used for identification purposes only and may be trademarks of their respective companies.

Proprietary Notice

The information and descriptions contained herein are the property of Concord Communications, Inc. Such information and descriptions may not be copied, disseminated, or distributed without the express written consent of Concord Communications, Inc. Concord Communications, Inc., assumes no responsibility for any inaccuracies that may appear in this document. Concord Communications, Inc., reserves the right to improve its products and change specifications at any time without notice.

U. S. Government Restricted Rights

Use, reproduction, and disclosure by the U.S. Government are subject to the restrictions set forth in FAR §52.227-19 (c) (1) and (2) and DFARS §252.227-7013 (c) (1) (ii).

Patent Information

U. S. Patent 5,615,323
Patents Pending

Table of Contents

About This Guide

Chapter 1
Introduction

Chapter 2
Installing AdvantEDGE for Microsoft SQL Server

Chapter 3
Using the AdvantEDGE for Microsoft SQL Server MIB

Chapter 4
Using AdvantEDGE for Microsoft SQL Server

About This Guide

The *AdvantEDGE for Microsoft SQL Server User Guide* provides instructions for installing and using AdvantEDGE for Microsoft SQL Server. This guide is intended for the person responsible for installing and configuring AdvantEDGE for Microsoft SQL Server. This guide supports AdvantEDGE for Microsoft SQL Server Release 1.0 and later and the SystemEDGE agent Release 4.0, Patchlevel 3 and later.

To use AdvantEDGE for Microsoft SQL Server, you should have a basic understanding of the Microsoft SQL Server application, the Concord SystemEDGE agent, Simple Network Management Protocol (SNMP), the Host Resources management information base (MIB), and your host's operating systems environment. For more information, refer to Microsoft documentation and the *SystemEDGE Agent User Guide*.

How This Guide Is Organized

This guide is organized as follows:

- Chapter 1, "Introduction," provides an overview of AdvantEDGE for Microsoft SQL Server and its capabilities for monitoring Microsoft SQL Server.
- Chapter 2, "Installing AdvantEDGE for Microsoft SQL Server," explains how to install and configure the Concord AdvantEDGE for Microsoft SQL Server software on a host system.
- Chapter 3, "Using the AdvantEDGE for Microsoft SQL Server MIB," describes the information that is available through the Concord AdvantEDGE for Microsoft SQL Server MIB.
- Chapter 4, "Using AdvantEDGE for Microsoft SQL Server," explains how to configure and use Concord's AdvantEDGE for Microsoft SQL Server in your host environment.

Conventions in This Guide

The following paragraph shows a sample command. Throughout this guide, commands are formatted this way to distinguish them from other information. Due to space limitations in this guide, some commands wrap from one line to the next. Disregard these line breaks and **enter each command on one line.** Otherwise, your command syntax will be incorrect.

```
watch process procAlive 'sqlservr' 5000 0x0
30 'Microsoft SQL Server' ''
```

You must enter the command on one line, as shown here:

```
watch process procAlive 'sqlservr' 5000 0x0 30 'Microsoft SQL Server' ''
```

Contact Information

If you need any assistance with the SystemEDGE agent or the AdvantEDGE for Microsoft SQL Server Point module, contact Customer Support, using one of the following methods:

Phone:	(888) 832-4340 (for calls from the USA and Canada) (508) 303-4300 (for calls from other countries)
Fax:	(508) 303-4343
Email:	support@concord.com
Web site:	http://www.concord.com

1

Introduction

This chapter provides an overview of the purpose and features of AdvantEDGE for Microsoft SQL Server.

Introducing AdvantEDGE for Microsoft SQL Server

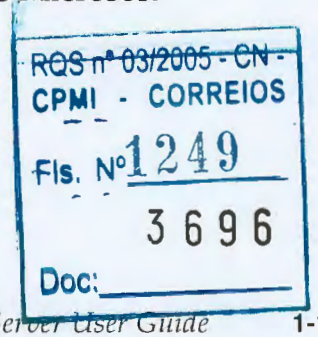
AdvantEDGE for Microsoft SQL Server is a plug-in for the SystemEDGE agent that brings the intelligent self-management capabilities of the SystemEDGE agent to the application level. You can configure this plug-in to monitor the Microsoft SQL Server processes and features that are relevant to your organization. You can also configure it to alert you to any potential issues with the application or the system on which it is running before those issues become problems.

AdvantEDGE for Microsoft SQL Server makes important information about Microsoft SQL Server available to network management software through the SystemEDGE agent and Simple Network Management Protocol (SNMP). It can provide information at the system, application, and database levels.

AdvantEDGE for Microsoft SQL Server enables you to monitor the health and availability of Microsoft SQL Server running on the Windows NT or Windows 2000 operating system. It must be installed on every SQL Server system that needs to be monitored. For more information, refer to Chapter 2, "Installing AdvantEDGE for Microsoft SQL Server."

NOTE

This document is not intended as a manual on how to install, administer, or use Microsoft SQL Server. For assistance, refer to Microsoft documentation.



Purpose of AdvantEDGE for Microsoft SQL Server

At its best, an instance of Microsoft SQL Server can process queries from thousands of concurrent users who connect over a network. It can support data warehouses or data marts that process complex queries required to discover trends and analyze critical factors in enterprise activity.

Despite advances in the design of database management systems in the last ten years, issues remain that frequently impact the health and availability of Microsoft SQL Server.

These issues include the following:

- Performance tuning, which involves trade-offs between resources for queries and resources for indexing columns
- Table locking, which can prevent users from being able to update records
- Tuning the maximum size of transaction logs to ensure that records can be updated

The purpose of AdvantEDGE for Microsoft SQL Server is to provide you with the tools and information necessary for monitoring the health and availability of Microsoft SQL Server.

Functionality of AdvantEDGE for Microsoft SQL Server

AdvantEDGE for Microsoft SQL Server accomplishes its purpose depending on the way it is deployed. It can operate with any SNMP-compliant management software such as Concord's *e*Health suite of products, AdvantEDGE View, HP OpenView, and others.

Using AdvantEDGE for Microsoft SQL Server

As a plug-in for the SystemEDGE agent, AdvantEDGE for Microsoft SQL Server works to closely manage the Microsoft SQL Server application. Right out-of-the-box, it provides real-time fault detection and is capable of correcting problems without human intervention.

Using AdvantEDGE for Microsoft SQL Server with *e*Health

When teamed with the *e*Health product suite, AdvantEDGE for Microsoft SQL Server and the SystemEDGE agent provide the historical data for long-term trending analysis and capacity planning.

With *e*Health – Application Assessment, you can run At-a-Glance, Trend, Top N, and MyHealth reports for the following types of variables:

- Amount of central processing unit (CPU), memory, and disk space the Microsoft SQL Server application is using
- Size of the Microsoft SQL Server configuration and database logs
- Transaction log size and percentage of transaction log space used
- Frequency of hits within Microsoft SQL Server caches

For more information about the variables that you can monitor and the reports that you can run when you integrate AdvantEDGE for Microsoft SQL Server with *e*Health, refer to the *e*Health Web Help.

Using AdvantEDGE for Microsoft SQL Server with Live Health

In a deployment with Live Health, AdvantEDGE for Microsoft SQL Server and the SystemEDGE agent provide the data for real-time detection of faults, potential outages, and delays associated with Microsoft SQL Server database activity. Unlike other real-time monitoring solutions and network management systems, Live Health applies intelligent algorithms to the data, resulting in precise assessments of application health and database performance. For more information about how Live Health can detect brownouts and service delays across applications, systems, and networks, refer to the Live Health Web Help.

2

Installing AdvantEDGE for Microsoft SQL Server

This chapter explains how to install, configure, and license the AdvantEDGE for Microsoft SQL Server Point module.

NOTE

For the most current information about installing AdvantEDGE for Microsoft SQL Server, refer to the release notes (relnotes.txt) on the installation CD-ROM.

Installation Requirements

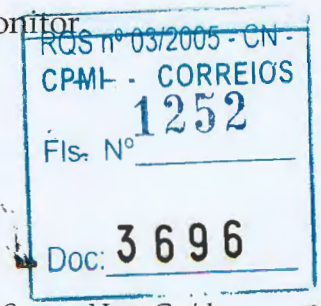
Before you install AdvantEDGE for Microsoft SQL Server, you must first install, license, and configure the SystemEDGE agent Release 4.0, Patchlevel 3 or later. For more information, refer to the *SystemEDGE Agent User Guide*. Also, your system must be running Microsoft SQL Server 7.0 or Microsoft SQL Server 2000 on Windows NT 4.0 or later. For more information, refer to the Microsoft documentation.

Installing the Software

AdvantEDGE for Microsoft SQL Server is distributed as a self-extracting executable named sqlmod.exe.

To install it:

1. Locate the SQL Server system that you need to monitor.
2. Log on to the system as the administrator.
3. Click **Start**.
4. Select **Programs** → **Command Prompt**.



5. Insert the CD-ROM containing the Concord software distributions into the CD-ROM drive.

   Windows NT automatically mounts the drive using the CD-ROM drive's corresponding drive letter.

   NOTE

   The particular drive letter is specific to your system and depends on the number and types of disks attached to your system.

6. Determine the directory that you want to use as the installation directory for AdvantEDGE for Microsoft SQL Server. If the SystemEDGE agent is installed at C:\sysedge, you should use C:\sysedge\plugins.

7. Run the self-extracting executable by entering the following at the command prompt:

   ```
   D:\sqlmod\ntx86\sqlmod.exe -dir C:\sysedge\plugins
   ```

   where `D` is the CD-ROM drive for your system, and `C:\sysedge\plugins` is the installation directory.

   NOTE

   The -dir option is important because it instructs the self-extracting executable to recreate the intended subdirectory hierarchy used throughout this manual.

   The executable then places the distribution in an sqlmod subdirectory within the specified target directory (for example, C:\sysedge\plugins\sqlmod).

NOTE

You cannot execute sqlmod.exe directly from the CD-ROM.

AdvantEDGE for Microsoft SQL Server is now installed.

AdvantEDGE for Microsoft SQL Server Files

Table 2-1 describes the files created by the installation process.

Table 2-1: Files Installed by AdvantEDGE for Microsoft SQL Server

Filename	Description
sqlmod.asn1	AdvantEDGE for Microsoft SQL Server MIB specification
sqlmod.cf	AdvantEDGE for Microsoft SQL Server configuration file
sqlmod.dll	AdvantEDGE for Microsoft SQL Server dynamic link library (DLL) for Windows NT and Windows 2000
sqlmod.pdf	AdvantEDGE for Microsoft SQL Server User Guide
examples	AdvantEDGE for Microsoft SQL Server monitoring examples
relnotes.txt	Release notes for AdvantEDGE for Microsoft SQL Server

Configuring AdvantEDGE for Microsoft SQL Server

After you install AdvantEDGE for Microsoft SQL Server, you must configure the Point module by editing the following files:

- sysedge.cf
- sqlmod.cf

Editing the sysedge.cf File

The SystemEDGE agent uses the configuration file sysedge.cf and the *sysedge_plugin* keyword to specify which AdvantEDGE modules to load at system start time. By default, the SystemEDGE agent does not load any plug-ins at initialization time, but you can edit the sysedge.cf file to configure the agent to load any AdvantEDGE Point modules that you have installed. The sysedge.cf file is located in your system directory (for example, C:\winnt\system32). For more information about the sysedge.cf file, refer to the *SystemEDGE Agent User Guide.*

To configure the SystemEDGE agent to start AdvantEDGE for Microsoft SQL Server at system start time, open the sysedge.cf file for editing; then add the following lines:

```
# SQL Server
sysedge_plugin C:\sysedge\plugins\sqlmod\sqlmod.dll
```

where C:\sysedge\plugins\sqlmod is the directory in which you installed the AdvantEDGE for Microsoft SQL Server files. This command line provides the complete pathname to sqlmod.dll, the AdvantEDGE for Microsoft SQL Server dynamic link library.

Editing the sqlmod.cf File

The sqlmod.cf file describes the AdvantEDGE for Microsoft SQL Server Point module configuration. Make sure that this file is located in the same directory as sqlmod.dll (for example, C:\sysedge\plugins\sqlmod). If you are running more than one instance of Microsoft SQL Server on your system, edit the configuration file to associate the Open Database Connectivity (ODBC) connections with the instances that you want to monitor.

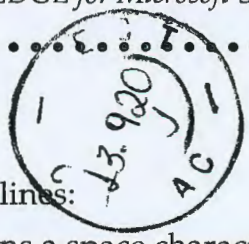
The following is a sample sqlmod.cf file.

```
sqlmod 1 "{SQL Server}" SLOWPOKE MSSQLODBC sa password
sqlmod 2 "{SQL Server}" SLOWPOKE\INSTANCE1 ODBCInstance1 sa password
sqlmod 3 "{SQL Server}" SLOWPOKE\INSTANCE2 ODBCInstance2 sa password
```

- Position 1: sqlmod.
- Position 2: The index number uniquely assigned to the instance.
- Position 3: The name of the driver to connect with Microsoft SQL Server; it will usually be "{SQL Server}". The driver name must be enclosed in brackets.
- Position 4: The name of the Microsoft SQL Server to which to connect.
- Position 5: The name of the ODBC connection.
- Position 6: A user name; for example, "sa" would be an appropriate choice for a user with a system administrator role.
- Position 7: An appropriate password.

NOTE

The user that you specify in this file does **not** need to be a system administrator and does **not** need db_owner level access.



Editing Guidelines

When editing the sqlmod.cf file, follow these guidelines:

- Enclose an entry in quotation marks if it contains a space character.
- After you modify the sqlmod.cf file, save it and restart the SystemEDGE agent.
- After restarting the SystemEDGE agent, license the module as described in "Licensing AdvantEDGE for Microsoft SQL Server" on page 2-6.
- The user that you specify in sqlmod.cf does not need to have a server role, but **must** have at least db_datareader access to the master database. You can set up and verify this access from the Enterprise Manager under Security -> Logins.

Creating an ODBC Connection to Microsoft SQL Server

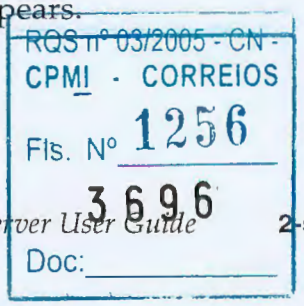
The system administrator should set up an ODBC connection to use Microsoft SQL Server authentication with a login ID and password. This connection stays open after it is established.

NOTE

It is important that the username assigned for the ODBC connection have the proper Microsoft SQL Server access permissions. Failure to do so may cause SQL Server operation to lock up when attempting the connection.

To create a new ODBC connection using Microsoft SQL Server authentication:

1. Log on to the system as the administrator.
2. Click **Start**.
3. Select **Settings** → **Control Panel**. The Control Panel window appears.
4. Double-click the **ODBC Data Sources** icon. (In Windows 2000, this is in the Administrative Tools folder of the Control Panel window.) The ODBC Data Sources Administrator window appears.
5. Select the **User DSN** tab (if it is not already selected.)
6. Select **Add**.
7. Select **SQL Server** from the list of ODBC drivers and click **Finish**. The Create a New Data Source to SQL Server wizard appears.
8. Specify a connection name in the **Name** field.



9. Optionally, specify a description of the data source in the **Description** field.
10. Specify the server for the ODBC connection in the **Server** field.
11. Select **Next**.
12. Select **With SQL Server authentication using a login ID and password entered by the user**.
13. Select **Next**.
14. Select **Next** to accept the default values. The ODBC Microsoft SQL Server Setup window appears.
15. Select **Test Data Source**.

Licensing AdvantEDGE for Microsoft SQL Server

Like the SystemEDGE agent, AdvantEDGE for Microsoft SQL Server utilizes a host-based license method. Copies of AdvantEDGE for Microsoft SQL Server can run only on systems that possess a valid license key. This license is separate from the one used for the SystemEDGE agent.

The first time that you attempt to start the SystemEDGE agent after installing AdvantEDGE for Microsoft SQL Server, the agent displays a message stating that it did not find a valid license for AdvantEDGE for Microsoft SQL Server. It then provides you with a *public key* that you can use to generate a permanent license key for your host machine.

A license key is made up of four space-separated, 8-character sequences, totaling 32 characters. The sysedge.lic file contains the AdvantEDGE for Microsoft SQL Server license, as well as the SystemEDGE agent license and other AdvantEDGE Point module licenses. For an example of a license file, refer to "Sample License File" on page 2-9.

NOTE

If you are using an evaluation copy of AdvantEDGE for Microsoft SQL Server, you must request a temporary license that will enable AdvantEDGE for Microsoft SQL Server to operate during the evaluation period.

Obtaining a License

To obtain a license, choose one of the following methods:

- Run the Concord licenseutil.pl script.
- Run the licenseme.exe license utility.
- Use the AdvantEDGE View licensing procedure; refer to the AdvantEDGE View Web Help.
- Send an e-mail request to license@empire.com.
- Complete the online license form through the Internet, as described in "Generating the License" on page 2-7.

You can obtain a license at any time from the Concord licensing Web server (http://license.concord.com). If you use AdvantEDGE View licensing, AdvantEDGE View can automatically retrieve and set up licenses for the SystemEDGE agent and the plug-ins. For more information, refer to the *Automating the Licensing of SystemEDGE and AdvantEDGE Point Plugin Modules* white paper and the *SystemEDGE Agent User Guide*.

Generating the License

The SystemEDGE setup program generates the licensing information for your system.

To generate a license:

1. Run the SystemEDGE agent setup command by entering the following at the command prompt:

   ```
   sysedge\setup -l
   ```

   The setup program displays a message similar to the following:

```
SystemEDGE Version 4.0 Patchlevel 3
Copyright 2001 by Concord Communications, Inc.
Please contact Concord Communications, Inc. to obtain a license
http://www.concord.com/support, Email: license@concord.com
Provide: sysedge neptune NTx86 5.0 346561363366b19c 4.0 Patchlevel 3
```

2. Complete the Web-based license form for AdvantEDGE for Microsoft SQL Server available from Concord's licensing Web server at the following URL:

   http://license.concord.com

NOTE

You must supply a user name and password to access the license form.

Supply the following information on the form:

- Customer ID
- Name
- E-mail address
- Software version number (4.0 in the example above)
- Patchlevel
- System name (neptune in the example above)
- Operating system name (NTx86 in the example above)
- Version (5.0 in the example above)
- System identifier (346561363366b19c in the example above)

NOTE

When you are licensing AdvantEDGE for Microsoft SQL Server, select **sqlmod** as the product on the licensing form.

After you submit the license request, the Concord Web server generates a license and displays it to your Web browser. It also e-mails the license to the contact person in your organization.

3. Copy the generated license key into the sysedge.lic file in the system32 subdirectory (C:\winnt\system32) and save this file.

NOTE

The license key is case-sensitive. Copy it exactly as it appears. If possible, use your system's cut-and-paste feature instead of entering it manually. If you do enter the license key manually, ensure that you do not confuse characters such as the letters **l** and **I** and the number **1**, or the letter **O** and the number **0**.

4. Stop and restart the Windows NT Master agent by entering these commands at the command prompt:

```
net stop snmp
net start snmp
```

AdvantEDGE for Microsoft SQL Server is now licensed and ready to use.

Sample License File

The following is a sample SystemEDGE agent license file. A pound character (#) in column 1 indicates that the entire line is a comment.

```
# license file for SystemEDGE Agent
# Empire Technologies, Inc.
# A Concord Communications Company
# http://www.empire.com
#
# file /etc/sysedge.lic or %SystemRoot%\system32\sysedge.lic
# A valid license key has four parts of 8 characters per part
# parts are separated by space(s) with one license key per
  line
# sysedge neptune NTx86 5.0 807cb1da007cb1da 4.0
e13311d3 0F2a7cb1 abC512dc fF8C923a
# sqlmod neptune NTx86 5.0 807cb1da007cb1da 1.0
a7943fde 098a87ij a4kiuf39 afafEkj4
```

3

Using the AdvantEDGE for Microsoft SQL Server MIB

This chapter outlines the information available from the Concord Communications Management Information Base (MIB) for the Microsoft SQL Server. The MIB specification (sqlmod.asn1) defines a collection of objects for monitoring and managing Microsoft SQL Server. All MIB objects related to AdvantEDGE for Microsoft SQL Server exist at object identifier (OID) branch 1.3.6.1.4.1.546.16.8 in the Concord Systems Management MIB.

This chapter explains the organization and content of the AdvantEDGE for Microsoft SQL Server MIB. You must configure the SystemEDGE agent to monitor the MIB objects that are relevant to your configuration. For that information, refer to Chapter 4, "Using AdvantEDGE for Microsoft SQL Server."

MIB Overview

The MIB is organized into broad sections for server configuration, footprint, and performance. The server configuration section describes MIB objects that capture data such as database names, database creation dates, database status, and database device names, as well as overall server-level activity indicators. The footprint section defines MIB objects that convey how much of the underlying system's resources are consumed by Microsoft SQL Server. The performance section contains MIB objects that capture data regarding lock requests, access methods, transaction log activity, memory management, SQL statistics, buffer management, and cache management.

SQL Server 2000 supports multiple instances of the sqlserver process. The Concord Communications MIB for Microsoft SQL Server was specifically designed to handle data from multiple instances. The information set contained in this MIB is unique.

The following sections briefly describe the MIB objects. Refer to the AdvantEDGE for Microsoft SQL Server MIB Specification (sqlmod.asn1) for a list of MIB objects and their syntax sequences and statuses.

Configuration Section

The Configuration section of the AdvantEDGE for Microsoft SQL Server MIB contains configuration parameters and settings that are important for monitoring the Microsoft SQL Server process and configuring databases.

Database Description Group

The Database Description group contains high-level information about the Microsoft SQL Server application including the status of the database. Table 3-1 describes the Database Description MIB objects.

Table 3-1: SQL Server Database Description MIB Objects

MIB Object	Description
sqlmodDBDescInstanceIdx	SQL Server instance InstanceIdx
sqlmodDBDescVendor	Database server vendor
sqlmodDBDescProdName	Product name for the database server
sqlmodDBDescVers	SQL Server version
sqlmodDBDescContact	Contact individual or organization
sqlmodDBDescStatus	Number indicating SQL Server status where 1=initialized, 2=ready, 3=running, 4=standby, 5=terminated, 6=waiting, 7=transitioning, 8=unknown
sqlmodDBDescUptime	SQL Server uptime in msec
sqlmodDBDescIsClustered	Number indicating SQL Server clustering status where 1=not clustered, 2=clustered, 3=not determined

SQL Server General Information Group

The SQL Server General Information group contains MIB objects that capture basic information about an instance of Microsoft SQL Server and the status of this process. Table 3-2 describes the SQL Server General Information MIB objects.

Table 3-2: SQL Server General Information MIB Objects

MIB Object	Description
sqlmodDBGenProcInstanceIdx	SQL Server instance InstanceIdx
sqlmodDBGenProcServName	Name of SQL Server instance
sqlmodDBGenProcStartTime	Date and time that the SQL Server instance started
sqlmodDBGenProcCompPageRead	Number of physical page reads completed for this instance since it started
sqlmodDBGenProcCompPageWrite	Number of physical page writes completed for this instance since it started
sqlmodDBGenProcTDSPackRead	Number of TDS packets read from network for this instance since it started
sqlmodDBGenProcTDSPackWrite	Number of TDS packets written to network for this instance since it started
sqlmodDBGenProcBlkngLocks	Total number of blocking locks for this instance
sqlmodDBGenProcUsersBlkd	Number of users blocked by other users for this instance

Advanced Configuration Group

The Advanced Configuration group contains MIB objects that capture data about advanced configuration parameters such as locks, query wait, and maximum number of worker threads. Table 3-3 describes the Advanced Configuration MIB objects.

Table 3-3: Advanced Configuration MIB Objects

MIB Object	Description
sqlmodDBAdvCfgInstanceIdx	SQL Server instance InstanceIdx
sqlmodDBAdvCfgParams	SQL Server configuration values (For a list of values, refer to the sqlmod.asn1 file.)
sqlmodDBAdvCfgParamName	Description of parameter
sqlmodDBAdvCfgMin	Minimum value of parameter
sqlmodDBAdvCfgMax	Maximum value of parameter
sqlmodDBAdvCfgCfg	Configured value for parameter
sqlmodDBAdvCfgRun	Runtime value for parameter

Databases Information Group

The Databases Information group includes MIB objects that report on total database size, transaction log size, and other measures of database management activity. Table 3-4 describes the Database Information MIB objects.

Table 3-4: Database Information MIB Objects (Page 1 of 2)

MIB Object	Description
sqlmodDBDbasesInfoInstanceIdx	SQL Server instance InstanceIdx
sqlmodDBDbasesInfoDBID	SQL Server DBID
sqlmodDBDbasesInfoName	SQL Server database name
sqlmodDBDbasesInfoState	SQL Server database state. (For a list of values, refer to the sqlmod.asn1 file.)
sqlmodDBDbasesInfoCreat	Database creation date and time
sqlmodDBDbasesInfoOwn	Database owner
sqlmodDBDbasesInfoSz	Database size in KB

Table 3-4: Database Information MIB Objects (Page 2 of 2)

MIB Object	Description
sqlmodDBDbasesInfoUnalloc	Unallocated space in KB
sqlmodDBDbasesInfoReserv	Reserved space in KB
sqlmodDBDbasesInfoUseddata	Used data space in KB
sqlmodDBDbasesInfoUsedIdx	Used index space in KB
sqlmodDBDbasesInfoUnused	Unused space in KB
sqlmodDBDbasesInfoLasttranslog	Date and time of last transaction log dump
sqlmodDBDbasesInfoTranslogsz	Transaction log size in KB
sqlmodDBDbasesInfoTranslogsp	Percent of transaction log space used
sqlmodDBDbasesInfoLastfull	Date and time of last transaction log full backup
sqlmodDBDbasesInfoLastdifferential	Date and time of last transaction log differential backup
sqlmodDBDbasesInfoLastfilegroup	Date and time of last transaction log file/filegroup backup

Database Options Group

The Database Options group relates the database ID and database name to a database option which has been set. Table 3-5 describes the Database Options MIB objects.

Table 3-5: Database Options MIB Objects

MIB Object	Description
sqlmodDBDbasesOptInstanceIdx	SQL Server instance InstanceIdx
sqlmodDBDbasesOptDBID	SQL Server database ID
sqlmodDBDbasesOptOptID	Option index
sqlmodDBDbasesOptName	Name of SQL Server database to which option applies
sqlmodDBDbasesOptOption	Name of the database option which is set

Database Devices Group

The Database Devices group includes MIB objects for device-specific information such as device description, device status, and device size. Table 3-6 describes the Database Devices MIB objects.

Table 3-6: Database Devices MIB Objects

MIB Object	Description
sqlmodDBDbasesDevInstanceIdx	SQL Server instance InstanceIdx
sqlmodDBDbasesDevDevice	SQL Server device index
sqlmodDBDbasesDevName	SQL Server device name
sqlmodDBDbasesDevPhysName	SQL Server device physical name
sqlmodDBDbasesDevDescrip	SQL Server device description
sqlmodDBDbasesDevStatus	SQL Server device status
sqlmodDBDbasesDevCtrlType	SQL Server device controller type
sqlmodDBDbasesDevSize	SQL Server device size

Footprint Section

The Footprint section of the AdvantEDGE for Microsoft SQL Server MIB contains footprint statistics that are important for monitoring the SQL Server process and its impact on the system. Long-term trend analysis of footprint information is useful for anticipating and avoiding problems due to resource exhaustion. You can also monitor footprint information in real time to detect and correct temporary resource exhaustion due to viruses, security incidents, and hardware failures.

General Footprint Group

The General Footprint group contains MIB objects that pertain to the system, not just to an instance of SQL Server. Table 3-7 describes the General Footprint MIB objects.

Table 3-7: General Footprint MIB Objects

MIB Object	Description
sqlmodFootprintTotCPUTime	Total CPU time for all SQL Server instances
sqlmodFootprintTotPercentCPU	Total percent of CPU usage for all SQL Server instances
sqlmodFootprintTotMEMSize	Total memory usage for all SQL Server instances
sqlmodFootprintTotRSS	Total resident set size for all SQL Server instances
sqlmodFootprintTotPercentMEM	Total percent of memory usage for all SQL Server instances
sqlmodFootprintTotThreads	Total number of threads for all SQL Server instances
sqlmodFootprintTotFaults	Total number of page faults for all SQL Server instances

Physical Disk Group

The Physical Disk group contains MIB objects that describe the physical disks in which database files are stored. Table 3-8 describes the Physical Disk MIB objects.

Table 3-8: Physical Disk MIB Objects (Page 1 of 2)

MIB Object	Description
sqlmodFootprintPhysicalDiskIdx	Number indicating the disk drive being monitored where 1 = total, 2 = drive C, 3 = drive D, 4 = drive E, 5 = drive F, etc.
sqlmodFootprintPhysicalDiskWhichdr	Name of the disk drive (for example, "C", "D") or "Total"

Table 3-8: Physical Disk MIB Objects (Page 2 of 2)

MIB Object	Description
sqlmodFootprintPhysicalDiskDisktrans	Total disk transfers
sqlmodFootprintPhysicalDiskCurrdskquelen	Current disk queue length
sqlmodFootprintPhysicalDiskDskbytes	Total number of bytes moved

SQL Server Process Footprint Group

The SQL Server Process Footprint group contains MIB objects that report the impact of the SQL Server process on the CPU and virtual memory. Table 3-9 describes the SQL Server Process Footprint MIB objects.

Table 3-9: SQL Server Process Footprint MIB Objects

MIB Object	Description
sqlmodFootprintProcessInstanceIdx	SQL Server InstanceIdx
sqlmodFootprintProcessMEM	Percent of real memory used by the process
sqlmodFootprintProcessSize	Combined size of the text, data, and stack segments in bytes
sqlmodFootprintProcessRSS	Size of resident set used by the process in kilobytes
sqlmodFootprintProcessTime	Accumulated CPU time used by the process in seconds
sqlmodFootprintProcessThreads	Number of threads used by the process
sqlmodFootprintProcessFaults	Number of page faults related to the process
sqlmodFootprintProcessPercentCPU	Percent of CPU usage by the process

Performance Section

The Performance section of the AdvantEDGE for Microsoft SQL Server MIB contains MIB objects that are indicators of the availability and performance of the application. This information is necessary for capacity planning and trend analysis.

Locks Group

The Locks group contains the MIB objects that indicate the frequency of users being prevented from updating records in the database. Table 3-10 describes the Locks MIB objects.

Table 3-10: Locks MIB Objects

MIB Object	Description
sqlmodLocksInstanceIdx	SQL Server InstanceIdx
sqlmodLocksWhichlock	Number indicating lock type where 1 = extent, 2 = key, 3 = page, 4 = table, 5 = rid, 6 = database, and 7 = total
sqlmodLocksAvgwaittime	Average wait time (in msec) for lock request
sqlmodLocksLockreq	Number of lock requests
sqlmodLocksLocktimeouts	Number of lock timeouts
sqlmodLocksLockwaittime	Total lock wait time (in msec)
sqlmodLocksLockwaits	Number of lock requests that require a wait
sqlmodLocksDeadlocks	Number of deadlocked lock requests

Access Methods Group

The Access Methods group contains MIB objects that reflect the types of searching that the SQL Server process performs during execution. Table 3-11 describes the Access Methods MIB objects.

Table 3-11: Access Methods MIB Objects (Page 1 of 2)

MIB Object	Description
sqlmodAccessMethodsInstanceIdx	SQL Server InstanceIdx
sqlmodAccessMethodsExtalloc	Number of extents allocated to database objects
sqlmodAccessMethodsFrwdrec	Number of records fetched through forwarded pointers
sqlmodAccessMethodsFullscans	Number of unrestricted full scans
sqlmodAccessMethodsIdxsearch	Number of index searches

Table 3-11: Access Methods MIB Objects (Page 2 of 2)

MIB Object	Description
sqlmodAccessMethodsPagesplits	Number of page splits (overflowing index pages)
sqlmodAccessMethodsPagesalloc	Number of pages allocated to database objects
sqlmodAccessMethodsProbescans	Number of probe scans
sqlmodAccessMethodsRangescans	Number of range scans
sqlmodAccessMethodsSkipghostrec	Number of ghosted records skipped
sqlmodAccessMethodsTablelockescl	Number of times locks on a table were escalated
sqlmodAccessMethodsWorktblcreat	Number of worktables created

Log Management Group

The Log Management group includes MIB objects that relate instances of the database to key indicators of transaction log activity. Table 3-12 describes the Log Management MIB objects.

Table 3-12: Log Management MIB Objects (Page 1 of 2)

MIB Object	Description
sqlmodDatabasePerfInstanceIdx	SQL Server InstanceIdx
sqlmodDatabasePerfDBidx	SQL Server DBidx
sqlmodDatabasePerfName	Name of SQL Server database or "Total"
sqlmodDatabasePerfActtrans	Number of active transactions
sqlmodDatabasePerfBulkcopyrows	Number of rows bulk copied
sqlmodDatabasePerfBulkcopythroughput	Size of bulk data copied (in KB)
sqlmodDatabasePerfDatafilesizes	Cumulative size of data files (in KB)
sqlmodDatabasePerfLogcachehitratio	Percent of reads satisfied from the log cache
sqlmodDatabasePerfLogfilesize	Cumulative size of the transaction log files

Table 3-12: Log Management MIB Objects (Page 2 of 2)

MIB Object	Description
sqlmodDatabasePerfLogflushes	Number of flushes of the transaction log
sqlmodDatabasePerfLoggrowths	Number of times that the transaction log has expanded
sqlmodDatabasePerfLogshrinks	Number of times that the transaction log has shrunk
sqlmodDatabasePerfLogtruncs	Number of times that the transaction log has been truncated
sqlmodDatabasePerfLogutilized	Percent of log space used
sqlmodDatabasePerfShrinkdata	Amount of data being moved by autoshrink operations (in bytes)
sqlmodDatabasePerfTrans	Number of transactions

Memory Management Group

The Memory Management group contains MIB objects that characterize management of dynamic memory. Table 3-13 describes the Memory Management MIB objects.

Table 3-13: Memory Management MIB Objects (Page 1 of 2)

MIB Object	Description
sqlmodMemoryManagerInstanceIdx	SQL Server InstanceIdx
sqlmodMemoryManagerConnmem	Total dynamic memory used for connections
sqlmodMemoryManagerLockmem	Total dynamic memory used for locks
sqlmodMemoryManagerMaxworkspacemem	Maximum memory for executing processes
sqlmodMemoryManagerMemgrantsout	Number of processes with a workspace memory grant
sqlmodMemoryManagerMemgrantspend	Number of processes awaiting a workspace memory grant
sqlmodMemoryManagerOptmem	Total dynamic memory for query optimization

Table 3-13: Memory Management MIB Objects (Page 2 of 2)

MIB Object	Description
sqlmodMemoryManagerSQLcachemem	Total dynamic memory for the SQL cache
sqlmodMemoryManagerTargservmem	Total dynamic memory that the server may consume
sqlmodMemoryManagerTotservmem	Total dynamic memory that the server is using

SQL Statistics Group

The SQL Statistics group contains the MIB objects that characterize the autoparameterizations (comparisons of SQL text to a template as part of query optimization) that take place in response to batch Transact-SQL (TSQL) requests. Table 3-14 describes the SQL Statistics MIB objects.

Table 3-14: SQL Statistics MIB Objects

MIB Object	Description
sqlmodSQLStatisticsInstanceIdx	SQL Server InstanceIdx
sqlmodSQLStatisticsAutoparamattmpt	Total failed, safe, and unsafe autoparameterizations
sqlmodSQLStatisticsBatchreq	Number of TSQL batch requests
sqlmodSQLStatisticsFailedautoparam	Number of failed autoparameterizations
sqlmodSQLStatisticsSafeautoparam	Number of safe autoparameterizations
sqlmodSQLStatisticsSQLComp	Number of SQL compilations
sqlmodSQLStatisticsUnsafeautoparam	Number of unsafe autoparameterizations

Buffer Management Group

The Buffer Management group contains the MIB objects that track statistics that are relevant to the efficiency of buffer management. Table 3-15 describes the Buffer Management MIB objects.

Table 3-15: Buffer Management MIB Objects

MIB Object	Description
sqlmodBufferManagerInstanceIdx	SQL Server InstanceIdx
sqlmodBufferManagerPagereads	Number of SQL Server (**not** total system) page reads
sqlmodBufferManagerChkptpages	Number of checkpoint pages
sqlmodBufferManagerPagewrites	Number of SQL Server page writes (inclusive)
sqlmodBufferManagerBuffercachehitratio	Percent of data being retrieved from cache
sqlmodBufferManagerLazWriteFlush	Number of pages flushed by LazyWriter for this instance since it started
sqlmodBufferManagerPhysRead	Number of physical reads by Read Ahead Manager for this instance since it started

General Statistics Group

The General Statistics group contains MIB objects that track the level of user login activity. Table 3-16 describes the General Statistics MIB objects.

Table 3-16: General Statistics MIB Objects

MIB Object	Description
sqlmodGeneralStatisticsInstanceIdx	SQL Server InstanceIdx
sqlmodGeneralStatisticsLogins	Number of logins
sqlmodGeneralStatisticsLogouts	Number of logouts
sqlmodGeneralStatisticsUserConns	Number of user connections

Cache Management Group

The Cache Management group contains MIB objects that are factors in the efficiency and effectiveness of cache management. Table 3-17 describes the Cache Management MIB objects.

Table 3-17: Cache Management MIB Objects

MIB Object	Description
sqlmodCacheManagerInstanceIdx	SQL Server InstanceIdx
sqlmodCacheManagerAdhocSQLCachehitratio	Percent of data found in cache for adhoc SQL queries
sqlmodCacheManagerAdhocSQLNumobj	Number of objects for adhoc SQL queries
sqlmodCacheManagerAdhocSQLNumpages	Number of pages for adhoc SQL queries
sqlmodCacheManagerProcplansCachehitratio	Percent of data found in cache for procedure plans
sqlmodCacheManagerProcplansNumobj	Number of objects for procedure plans
sqlmodCacheManagerProcplansNumpages	Number of pages for procedure plans
sqlmodCacheManagerTrigplansCachehitratio	Percent of data found in cache for trigger plans
sqlmodCacheManagerTrigplansNumobj	Number of objects for trigger plans
sqlmodCacheManagerTrigplansNumpages	Number of pages for trigger plans
SqlmodCacheManagerPrepSQLplansCachehitratio	Percent of data found in cache for prepared SQL plans
sqlmodCacheManagerPrepSQLplansNumobj	Number of objects for prepared SQL plans
sqlmodCacheManagerPrepSQLplansNumpages	Number of pages for prepared SQL plans

Flat Information Group

The Flat Information group contains MIB objects that are totals across the set of databases for each instance of Microsoft SQL Server. Table 3-18 describes the Flat Information MIB objects.

Table 3-18: Flat Information MIB Objects

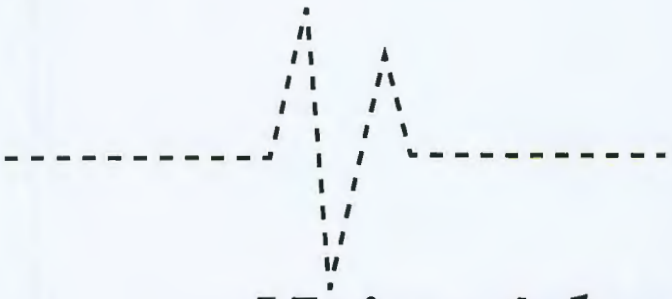
MIB Object	Description
sqlmodDBDbasesFlatInfoInstanceIdx	SQL Server instance
sqlmodDBDbasesFlatInfoANDedState	SQL Server database state where 64=pre-recovery, 128=recovering, 256=not recovered, 32768=emergency mode
sqlmodDBDbasesFlatInfoSzTotal	Database size in kilobytes
sqlmodDBDbasesFlatInfoUnallocTotal	Unallocated space in kilobytes
sqlmodDBDbasesFlatInfoTranslogszTotal	Transaction log size in kilobytes
sqlmodDBDbasesFlatInfoTranslogspTotal	Percent of transaction log space used
sqlmodDBDbasesFlatInfoLasttranslog	Date and time of last transaction log backup
sqlmodDBDbasesFlatInfoLastfull	Date and time of last transaction log full backup
sqlmodDBDbasesFlatInfoLastdifferential	Date and time of last transaction log differential backup
sqlmodDBDbasesFlatInfoLastfilegroup	Date and time of last transaction log file/filegroup backup

Flat Transaction Performance Group

The Flat Transaction Performance group contains MIB objects that are totals across the set of databases for each instance of Microsoft SQL Server. Table 3-19 describes the Flat Transaction Performance MIB objects.

Table 3-19: Flat Information MIB Objects

MIB Object	Description
sqlmodDatabaseFlatPerfInstanceIdx	SQL Server instance
sqlmodDatabaseFlatPerfTransTotal	Number of total transactions
sqlmodDatabaseFlatPerfLogcachehitsTotal	Total number of log cache hits
sqlmodDatabaseFlatPerfLogcachemissesTotal	Total number of log cache misses



4

Using AdvantEDGE for Microsoft SQL Server

This chapter describes how to configure and use AdvantEDGE for Microsoft SQL Server. After you license this plug-in and enable it in the sysedge.cf file (refer to "Configuring AdvantEDGE for Microsoft SQL Server" on page 2-3), it will load automatically at SystemEDGE start time.

This plug-in implements additional MIB objects that provide advanced information about the health and availability of Microsoft SQL Server. AdvantEDGE for Microsoft SQL Server can operate with any SNMP-compliant management software such as Concord's *e*Health suite of products, AdvantEDGE View, HP OpenView, and others. If you are using AdvantEDGE for Microsoft SQL Server with *e*Health, refer to the *e*Health Web Help for more information about the reports that you can generate.

The purpose of this chapter is to illustrate how you can edit the SystemEDGE configuration file to utilize the new MIB objects with the process-monitoring, threshold-monitoring, and history-collection features of the SystemEDGE agent. For more examples of configuration file commands, refer to the examples file, which is available in the AdvantEDGE for Microsoft SQL Server product installation.

Assigning Entry Rows for the SystemEDGE Self-Monitoring Tables

All of the SystemEDGE self-monitoring tables (for example, Log Monitor table, Windows NT Event Monitor table, Process/Service Monitor table, Threshold Monitor table, and History table) require the use of unique row numbers. Each table contains an *Index* column which acts as a *key field* to distinguish rows in the table. The following sections describe the benefits of reserving a block of rows (somewhere in the range of 11 to the maximum number of rows in your table) for use by the system or application administrator.

Setting Local Policy

System administrators may choose, as a matter of local policy, to reserve a block of rows for system administration. In compliance with this policy, all other users should use row indices that are outside of the reserved range when defining user-configured entries. This policy prevents users from using rows reserved for system administration.

Reserving Blocks of Rows

This policy also allows system administrators to define a consistent set of conditions (row entries) to be monitored across all machines such that the same condition is defined in the same row number on each machine. For example, you can use row 3000 in each table to define entries monitoring the total number of page faults (sqlmodFootprintGeneralPageFaults) MIB object. You can then distribute this configuration to every host so that every machine running Microsoft SQL Server uses row 3000 for monitoring the total number of page faults, whether it is the Threshold Monitoring table or the History table.

To reserve a block of rows for monitoring Microsoft SQL Server:

1. Identify a block of rows that you want to reserve for use with monitoring Microsoft SQL Server.
2. Use that block of rows to define a set of row entries for each SystemEDGE self-monitoring tables. For more information, refer to the chapter on self-monitoring in the *SystemEDGE Agent User Guide*.

3. Distribute the configuration file entries to all hosts that are running Microsoft SQL Server and AdvantEDGE for Microsoft SQL Server. For more information, refer to the *Automating the Deployment of SystemEDGE and AdvantEDGE Point Plugin Modules* white paper.

NOTE

Alternatively, you can use this row-number assignment policy with AdvantEDGE View for group configuration operations.

4. Require end users to avoid your block of rows when defining their own self-monitoring table entries.

Using the SystemEDGE Self-Monitoring Features

This section provides examples of how to use SystemEDGE process-monitoring, threshold-monitoring, and history-collection features to monitor the Microsoft SQL Server application. Add these examples to the sysedge.cf file to enable monitoring of the MIB objects they specify. Modify these examples as necessary to monitor the MIB objects that are relevant for your configuration.

The examples in this section use row numbers in the 5000 range; use a row number for your configuration that conforms to local policies. For more information on row assignment, refer to "Assigning Entry Rows for the SystemEDGE Self-Monitoring Tables" on page 4-2. For more information on SystemEDGE process monitoring and service monitoring, refer to the *SystemEDGE Agent User Guide*.

NOTE

Enter the commands in this section and throughout this chapter as one line. Do **not** use a carriage return to match the formatting shown here.

Using SystemEDGE Process Monitoring

This section provides an example of how to use the SystemEDGE agent to monitor the availability of a critical Microsoft SQL Server process. For more information, refer to the chapter on process monitoring in the *SystemEDGE Agent User Guide*.

Monitoring the Microsoft SQL Server Process

To ensure that Microsoft SQL Server is running, enter the following command:

```
watch process procAlive 'sqlservr' 5000 0x0
  30 'SQL Server' ''
```

This entry instructs the SystemEDGE agent to monitor the run-status (or liveness) of the Microsoft SQL Server process every 30 seconds and to store the data in row 5000 of the Process Monitor table.

Using SystemEDGE Threshold Monitoring

This section provides examples of how to use SystemEDGE threshold-monitoring capabilities to monitor important Microsoft SQL Server metrics. Add the following commands to the sysedge.cf file to monitor thresholds for these MIB objects. For more information on SystemEDGE threshold-monitoring, refer to the chapter on threshold monitoring in the *SystemEDGE Agent User Guide*.

NOTE

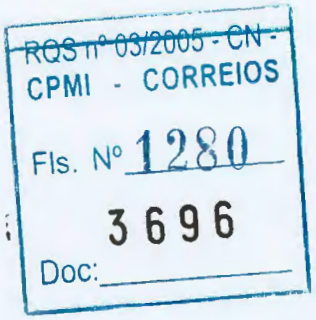
The thresholds used in these examples may not be appropriate for your system; select thresholds that are appropriate for your environment.

Monitoring the Status of the SQL Server Process

To monitor if the SQL Server process has paused, enter the following command:

```
monitor oid sqlmodDBDescStatus 5002 0x0 60 absolute = 2 'SQL
  Server has paused'
```

This entry instructs the SystemEDGE agent to track the object, sqlmodDBDescStatus, and save the data to row 5002 of the agent's monitor table. The agent will sample the status of the SQL Server process every 60 seconds. The sample-type is `'absolute'` since the object is an integer. The operator type `'='` instructs the agent to send a trap whenever the status of the SQL Server process is equal to `'2'` which is specified in Concord's MIB for Microsoft SQL Server as indicating a paused process.



Monitoring the Number of Blocked Users

To monitor the number of blocked users, enter the following command:

```
monitor oid sqlmodDBGenProcUsersBlkd 5004 0x0 60 absolute >
  20 'Number of Blocked Users exceeds threshold'
```

Monitoring the Percentage of Log Space Used

To monitor the percentage of the transaction log that is used, enter the following command:

```
monitor oid sqlmodDatabasePerfLogutilitzed 5005 0x0 60
  absolute > 85 'Percentage of Transaction Log Utilized
  exceeds threshold'
```

Monitoring the Number of Processes Awaiting a Workspace Memory Grant

To monitor the number of processes awaiting a workspace memory grant, enter the following command:

```
monitor oid sqlmodMemoryManagerMemgrantspend 5006 0x0 60
  absolute > 20 'Number of Processes Awaiting a Workspace
  Memory Grant exceeds threshold'
```

Using SystemEDGE History Collection

This section provides examples of how to use SystemEDGE history collection to track the value of important Microsoft SQL Server metrics over time. Add the following commands to the sysedge.cf file to collect history for these MIB objects. For more information on SystemEDGE history capabilities, refer to the chapter on history collection in the *SystemEDGE Agent User Guide*.

NOTE

The number of samples and the interval between samples used in these examples may not be appropriate for your system; select values that are appropriate for your environment.

Collecting Number of Blocked Users History

To collect history for the number of blocked users, enter the following command:

```
emphistory 5010 60 sqlmodDBGenProcUsersBlkd 400 'Num Blocked
 Users History'
```

This entry instructs the SystemEDGE agent to track the value of the object, sqlmodDBGenProcUsersBlkd, and save the data in row 5010 of the empireHistoryCtrlTable. The agent will sample the value every 60 seconds and store the last 400 samples.

Collecting Lock Requests Requiring a Wait History

To collect history for the number of lock requests requiring a wait, enter the following command:

```
emphistory 5011 60 sqlmodLocksLockwaits 480 'Number of Lock
 Requests Requiring a Wait History'
```

Collecting Average Length of Disk Queue History

To collect history for the average length of the disk queue, enter the following command:

```
emphistory 5012 60 sqlmodPhysicalDiskAvgdskquelen 480
 'Average Length of Disk Queue History'
```

Collecting Number of Database Transactions History

To collect history for the number of database transactions, enter the following command:

```
emphistory 5013 60 sqlDatabasePerfTrans 480 'Number of
 Database Transactions History'
```

Collecting Total Amount of Dynamic Memory Used History

To collect history for the total amount of dynamic memory used, enter the following command:

```
emphistory 5014 60 sqlMemoryManagerTotservmem 480 'Total
 Amount of Dynamic Memory Used History'
```

Index

T

U

Manual 31

eHealth AIM for Oracle - User Guide

eHealth AIM for Oracle User Guide

09-16060-003
December 2001

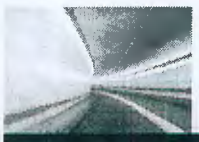
Important Notice

Proprietary Notice

U. S. Government Restricted Rights

Patent Information

Table of Contents



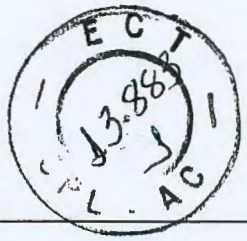
About This Guide

This guide describes how to install and use the *e*Health application insight module (AIM) for Oracle. It is intended for the person responsible for installing and configuring *e*Health AIM for Oracle. This guide supports *e*Health AIM for Oracle Release 1.3 Patchlevel 1 or later, and *e*Health SystemEDGE Release 4.0, Patchlevel 3 or later. *e*Health AIM for Oracle supports the following operating systems:

- Sun Solaris (SPARC) Release 2.6 or later in *32-bit mode* and one of the following versions of Oracle in *32-bit mode*:
  - Oracle 8.0.4, 8.0.5, 8.0.6
  - Oracle 8i (8.1.5, 8.1.6, or 8.1.7)
- AIX Releases 4.2 and 4.3 on Oracle 8i
- HP-UX Releases 11.0 and 11.1 on Oracle 8i

Audience

This guide is intended for the person who is installing and using *e*Health AIM for Oracle. To use *e*Health AIM for Oracle, you should have a basic understanding of the Oracle database, *e*Health SystemEDGE, and your host's operating system environment. For more information, refer to Oracle documentation (http://www.oracle.com) and the *eHealth SystemEDGE User Guide*.



About This Guide

This section describes the changes and enhancements that have been made since the last release of this guide. It also includes the documentation conventions used in this guide.

Revision Information

This guide describes information that is specific to *e*Health AIM for Oracle 1.0 Patchlevel 2. The following is new in this version of the guide:

- Installation instructions for the AIX and HP-UX versions of *e*Health AIM for Oracle
- Licensing through AdvantEDGE View Event Processing and Host Administration
- Glossary

Documentation Conventions

Table 1 lists the conventions used in this document.

Table 1. Documentation Conventions (Page 1 of 2)

Convention	Description
File or Directory Name	File or directory names.
`code`	System, code, or operating system command line examples.
emphasis	Emphasis and guide titles.
`enter`	Text that you must type exactly as shown.
Name	Text that defines menus, fields in dialog boxes, or keyboard keys.
New Term	A new term, that is, one that is being introduced.
`Variable`	Variable values that you substitute.

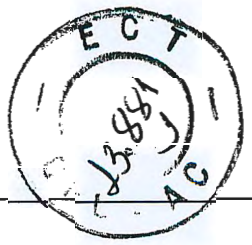
Table 1. Documentation Conventions (Page 2 of 2)

Convention	Description
→	A sequence of menus or menu options. For example, **File** → **Exit** means "Choose **Exit** from the **File** menu."
NOTE	Important information, tips, or other noteworthy details.
CAUTION	Information that helps you avoid data corruption or system failures.
WARNING	Information that helps you avoid physical danger.

Technical Support

If you need any assistance with this product, contact Technical Support at the following:

Phone: (888) 832-4340
(508) 303-4300
Fax: (508) 303-4343
E-mail: support@concord.com
Web site: http://www.concord.com



Professional Services

If you need any assistance with customizing this product, contact Professional Services at the following:

Phone:	(800) 851-8725 (Choose option 7)
Fax:	(508) 486-4555
E-mail:	proserv@concord.com
Web site:	http://www.concord.com

Introduction

This chapter provides an overview of *e*Health AIM for Oracle.

Introducing *e*Health AIM for Oracle

*e*Health AIM for Oracle is a plug-in for the SystemEDGE agent that enables information technology (IT) operators to monitor the health and availability of Oracle databases and servers. You can configure this plug-in to monitor the Oracle processes and features that are relevant to your organization. You can also configure *e*Health AIM for Oracle to alert you to any potential issues with the application or the system on which it is running before those issues become problems.

To use *e*Health AIM for Oracle, you must install it on every Oracle system that you want to monitor. For more information, refer to Chapter 2, "Installing eHealth AIM for Oracle."

NOTE

This guide is not intended to describe how to install, administer, or use Oracle databases. For help with Oracle, refer to your Oracle documentation.

Features

*e*Health AIM for Oracle monitors the following:

- Oracle database configuration
- Oracle log files (including alert, redo, database, and configuration logs)
- Performance metrics
- Database response and availability

*e*Health AIM for Oracle monitors database process attributes. For example, it monitors whether each process is alive; and it can restart processes, if necessary. In addition, it monitors memory use, log sizes, number of transactions, and efficiency of the library and the data dictionary.

Because the Oracle application records error information in alert log files, *e*Health AIM for Oracle can use the log-file monitoring capability of the SystemEDGE agent to scan the logs and forward certain events as SNMP traps when appropriate.

For more information about the management information base (MIB) objects that you can monitor with *e*Health AIM for Oracle, refer to Chapter 3, "Using the eHealth AIM for Oracle MIB." For more information about configuring the SystemEDGE agent to monitor these MIB objects, refer to Chapter 4, "Using eHealth AIM for Oracle."

*e*Health AIM for Oracle is designed to monitor one or more Oracle databases of the same Oracle release that are running on a single system. To support multiple databases, the data in the *e*Health AIM for Oracle MIB is organized into tables that are indexed by database session identification (SID) number. Each table includes an entry for the SID. For more information, refer to Chapter 3, "Using the eHealth AIM for Oracle MIB."

Using *e*Health AIM for Oracle

1

*e*Health AIM for Oracle provides important information about Oracle to management software through the SystemEDGE agent and Simple Network Management Protocol (SNMP). This AIM works with the SystemEDGE agent to closely manage the Oracle application, providing real-time fault detection and automatically correcting problems, if necessary.

You can use *e*Health AIM for Oracle with any SNMP-compliant management software, including Concord's *e*Health suite of products, AdvantEDGE View, HP OpenView, and others. *e*Health AIM for Oracle and the SystemEDGE agent can provide you with the following types of information:

- Number and type of users connected to the database
- Amount of work that each transaction performs
- Database workload per transaction
- Number of client and database requests per transaction
- Rate at which application systems reference the database
- Effectiveness of the database buffer cache and library cache
- Number of changes to the database
- Amount of memory allocated to sessions
- Sort statistics and efficiency percentages
- Server statistics

Using *e*Health AIM for Oracle with AdvantEDGE View

You can use *e*Health AIM for Oracle with AdvantEDGE View to run queries for monitoring the performance, configuration, availability, and health of the Oracle application.

To run an AdvantEDGE View Application query for Oracle:

1. Select the target system or group from the **System** or **Group** list.
2. Select **Oracle** from the **Applications** list.

3. Click the **Applications** icon.

AdvantEDGE View runs the query for the specified application on the system or group you selected.

NOTE

If you run a query for a group of systems, AdvantEDGE View may request additional information before running the query. For more information, refer to the AdvantEDGE View Web Help.

Figure 1 shows the image map that AdvantEDGE View displays when you run an Application query for Oracle. Click the area for which you want to display information.

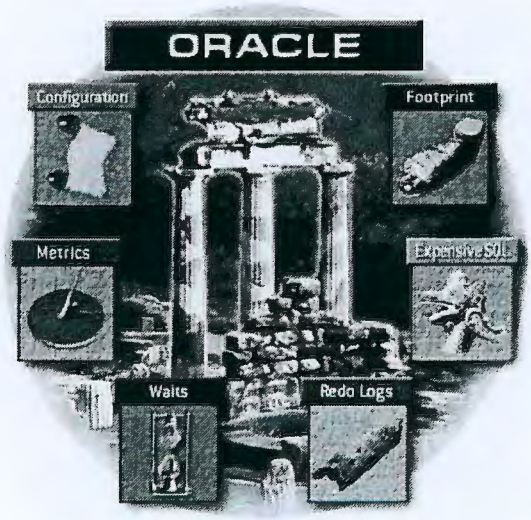


Figure 1. AdvantEDGE View Image Map for Oracle Queries

For example, if you click the **Metrics** area, AdvantEDGE View displays the Oracle metrics. Figure 2 shows a sample Metrics query for the Oracle application.

Oracle Metrics

Instance :	15	Block Changes Per Transaction :	25,664
Block Get Rate :	4	Block Visits Per Transaction :	90,653
Cache Hit Ratio :	233	Call Rate :	90,653
Calls Per Transaction :	158,886	Changed Blocks :	44,981
Consistent Change Ratio :	0	Continued Row Ratio :	0
Library Cache Miss Ratio :	99	Recursive To User Call Ratio :	18,666
Redo Log Space Wait Ratio :	0	Row Source Ratio :	1,608,212,080
Row Source Ratio :	3	Transaction Rate Ratio :	15
User Call Rate Ratio :	23,833	Users Calls Per Parse :	59
User Rollback Ratio :	72	Libray Cache Efficiency :	98
Data Dict. Cache Efficiency :	0	Reads and Writes :	336978
Block Changes:	6,116,597	Block Gets :	556
Consistent Gets :	336,722	Physical Reads :	279
Disk Sorts :	6,982	Memory Sorts:	0
Free Block Wait :	0	Multi-threaded Queue Wait :	341,612
Highwater Session Memory :	344,548	Maximum Session Memory :	3
Highwater Number of Sessions :	1	Sessions Current :	15
User Commits :	39	User Rollbacks :	23,833
Transactions :	0	Physical Writes :	16,082,075
Rows Table Scan :	0	Rowid Rows fetched:	135
Continued Row Fetch :	4,448,746	Recursive Calls :	0
Consistent Changes :	39,833	Parses:	4
CPU Time :	230,087	Redo Log File Switches:	0

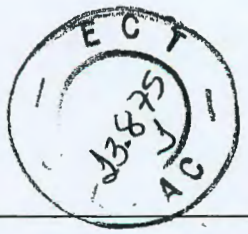
Figure 2. Sample AdvantEDGE View Oracle Metrics Query

Using *e*Health AIM for Oracle with *e*Health

In previous releases, eHealth – Application Insight was called eHealth – Application Assessment.

You can use *e*Health AIM for Oracle and the SystemEDGE agent with the *e*Health product suite to provide the historical data for long-term trending analysis and capacity planning. With *e*Health – Application Insight, you can run At-a-Glance, Trend, Top N, and MyHealth reports for the following types of variables:

- Amount of Central Processing Unit (CPU), memory, and disk space that the Oracle application is using
- Size of the Oracle configuration and database logs



- Number of transactions that the Oracle application is performing each second
- Amount of CPU used, disk input/output, work performed, and user calls for each transaction
- Ratio of transaction rollbacks and failures in writing to the redo logs
- Frequency with which the Oracle application uses the database cache to redisplay information

For more information about the variables that you can monitor and reports that you can run when you integrate *e*Health AIM for Oracle with *e*Health, refer to the *e*Health Web Help.

Using *e*Health AIM for Oracle with Live Health

You can also use *e*Health AIM for Oracle and the SystemEDGE agent with Live Health for real-time detection of potential problems. Live Health applies intelligent algorithms to the data, resulting in precise assessments of application health and performance. For more information about how Live Health can detect "brownouts" and service delays across applications, systems, and networks, refer to the Live Health Web Help.

Installing eHealth AIM for Oracle

This chapter explains how to install, configure, and license *e*Health AIM for Oracle.

NOTE

> For the most current information about installing this AIM, refer to the **relnotes.txt** file on the *e*Health AIM for Oracle installation CD-ROM.

Installation Requirements

Before you install *e*Health AIM for Oracle, you must first install, configure, and license the SystemEDGE agent Release 4.0, Patchlevel 3 or later. For more information, refer to the *eHealth SystemEDGE User Guide*.

To use *e*Health AIM for Oracle, your system must be running one of the following:

- Sun Solaris (SPARC) Release 2.6 or later in *32-bit mode* and one of the following versions of Oracle in *32-bit mode*:
  - Oracle 8.0.4, 8.0.5, 8.0.6
  - Oracle 8i (8.1.5, 8.1.6, or 8.1.7)
- AIX Releases 4.2 and 4.3 and Oracle 8i
- HP-UX Releases 11.0 and 11.1 and Oracle 8i

NOTE

If you are using the Solaris operating system, you *must* run both Solaris and Oracle in *32-bit mode only*.

Installing the Software

*e*Health AIM for Oracle is distributed as a tape archive (tar) file. The name of the tar file varies for each operating system, as follows:

- oramod_1.3p1_sol.tar for Solaris systems
- oramod_1.3p1_aix.tar for AIX systems
- oramod_1.3p1_hpux.tar for HP-UX systems

To install *e*Health AIM for Oracle:

1. Locate the Oracle database that you need to monitor.
2. Log on to that system as the root user.
3. Copy the tar file for your system from the CD-ROM to the /tmp directory.
4. Change directory to the SystemEDGE agent directory on your system by entering one of the following commands.

   For Solaris and HP-UX systems, enter the following:

   ```
   cd /opt/EMPsysedge
   ```

   For AIX systems, enter the following:

   ```
   cd /usr/lpp/EMPsysedge
   ```

5. Create the plugins directory, if it is not already present, by entering the following:

   ```
   mkdir plugins
   ```

6. Change directory to the plugins directory by entering the following:

   ```
   cd plugins
   ```

7. Enter one of the following commands to launch the installation, depending on your operating system.

   For Solaris systems, enter the following:

   ```
   tar xvf /tmp/oramod_1.3p1_sol.tar
   ```

   For AIX systems, enter the following:

   ```
   tar xvf /tmp/oramod_1.3p1_aix.tar
   ```

   For HP-UX systems, enter the following:

   ```
   tar xvf /tmp/oramod_1.3p1_hpux.tar
   ```

   The installation creates files in the plugins/oramod directory.

8. Edit the sysedge.cf file as described in "Editing the sysedge.cf File" on page 21. After you install the files, you must edit the sysedge.cf file to specify the correct shared library for your version of Oracle.

9. Edit the oramod.cf file to indicate which databases, SIDs, and Oracle home directories to use, as described in "Editing the oramod.cf File" on page 22.

10. Edit the SystemEDGE startup file to include Oracle environment variables so that the agent and AIM can find the Oracle home and lib directories, as described in "Editing the SystemEDGE Startup File" on page 24.

11. Start the SystemEDGE agent, using one of the following commands.

    For Solaris systems, enter the following:

    ```
    /etc/rc2.d/S99sysedge start
    ```

    For AIX systems, enter the following:

    ```
    bin/sysedge -b
    ```

For HP-UX systems, enter the following:

```
/sbin/rc2.d/S990sysedge start
```

12. License the AIM, as described in "Licensing eHealth AIM for Oracle" on page 27.
13. Restart the SystemEDGE agent.

*e*Health AIM for Oracle Files

Table 2 describes the files created by the *e*Health AIM for Oracle installation procedure.

Table 2. Files Installed by *e*Health AIM for Oracle

File Name	Description
oramod.asn1	*e*Health AIM for Oracle MIB specification
oramod.cf	*e*Health AIM for Oracle configuration file
oramod.pdf	*eHealth AIM for Oracle User Guide*
oramod8.so	eHealth AIM for Oracle shared library for Oracle 8.0.4, 8.0.5, and 8.0.6
oramod8i.so	*e*Health AIM for Oracle shared library for Oracle 8i (verions 8.1.5, 8.1.6, and 8.1.7)
relnotes.txt	Release notes for the *e*Health AIM for Oracle module

Configuring *e*Health AIM for Oracle

After you install *e*Health AIM for Oracle, you must configure it by editing the following files:

- sysedge.cf (page 21)
- oramod.cf (page 22)
- SystemEDGE startup file (page 24)

Editing the sysedge.cf File

You must edit the sysedge.cf file to use the correct shared library file for your system and to enable the SystemEDGE agent to load *e*Health AIM for Oracle. You can use the **sysedge_plugin** keyword in the sysedge.cf configuration file to specify which *e*Health AIMs the SystemEDGE agent will load at system initialization. By default, the SystemEDGE agent does not load any AIMs at initialization, but you can edit the sysedge.cf file to configure the agent to load any *e*Health AIMs that you have installed.

The sysedge.cf file is located in your system directory by default; for example, it is located in the /etc/sysedge.cf directory on UNIX systems. For more information about the sysedge.cf file, refer to the *eHealth SystemEDGE User Guide*.

NOTE

To configure the SystemEDGE agent to start *e*Health AIM for Oracle, you must provide the complete pathname to the shared library file for your version of Oracle.

Enabling *e*Health AIM for Oracle for Oracle 8.0.4, 8.0.5, or 8.0.6 (Solaris)

To enable the *e*Health AIM for Oracle module in the SystemEDGE agent for Oracle 8.0.4, 8.0.5, or 8.0.6 on Solaris systems, add the following line to /etc/sysedge.cf:

```
sysedge_plugin /opt/EMPsysedge/plugins/oramod/oramod8.so
```

Enabling *e*Health AIM for Oracle for Oracle 8i (Solaris and HP-UX)

To enable the *e*Health AIM for Oracle module in the SystemEDGE agent for Oracle 8i (versions 8.1.5, 8.1.6, or 8.1.7) on Solaris and HP-UX systems, add the following line to /etc/sysedge.cf:

```
sysedge_plugin /opt/EMPsysedge/plugins/oramod/oramod8i.so
```

Enabling *e*Health AIM for Oracle for Oracle 8i (AIX)

To enable the *e*Health AIM for Oracle module in the SystemEDGE agent for Oracle 8i for AIX systems, add the following line to /etc/sysedge.cf:

```
sysedge_plugin /usr/lpp/EMPsysedge/plugins/oramod/oramod8i.so
```

Editing the oramod.cf File

The oramod.cf file describes the *e*Health AIM for Oracle configuration. You can edit the oramod.cf file to indicate the following:

- User name and password.
- Name (SID) of the database that you are monitoring. This value is contained in the oramodDbCfgSID MIB object.

  NOTE

  If you are using Transparent Network Substrate (TNS) names, use the TNS name that matches your database name in the oramod.cf file.

- SID index. This value is also the value of the oramodDbCfgSIDINDX MIB object. This value is user-configurable. You can set it to any integer greater than zero. Each instance must have a unique index for the platform.
- SID-home. Installation directory for Oracle, or ORACLE_HOME. This value is also the value of the oramodDbCfgHOME MIB object.
- SID-base. Base directory for Oracle, or ORACLE_BASE. This value is also the value of the oramodDbCfgBASE MIB object.
- File Check Interval. This value is the interval for checking files, in seconds.
- Tablespace Check Interval. This value is the interval for checking tablespaces.

To use *e*Health AIM for Oracle, you must have a user ID that has either DBA privileges or SELECT_CATALOG_ROLE permissions for Oracle Version 8i and later. For earlier versions of Oracle, the SELECT_ANY_TABLE permissions should suffice.

*e*Health AIM for Oracle can monitor different versions of Oracle databases on the same platform *only* if you are running multiple versions of the SystemEDGE agent on different ports. Otherwise, *e*Health AIM for Oracle can simultaneously monitor *only* instances of Oracle that are the *same Oracle version.*

Sample oramod.cf File

The following is a sample oramod.cf file.

```
# oramod.cf
# Configuration file for the eHealth AIM for Oracle Module
# Concord Communications, Copyright 2001
#
# For each Oracle database running on your system, specify the following:
#
# oramod username passwd sid sid-index sid-home sid-base
#  file-check-interval table-space-check-interval
#
oramod fred elTsdim VIS 15 /u01/app/oracle/8.0.5 /u01/app/oracle 60 60
```

NOTE

After you make any changes to the oramod.cf file, you must restart the SystemEDGE agent to ensure that the changes take effect.

Editing the SystemEDGE Startup File

The SystemEDGE startup file is the shell script for starting and stopping the SystemEDGE agent. This file was installed with the SystemEDGE agent. You must edit the file for your system to match your Oracle installation environment.

For Solaris, edit the following file:

`/etc/rc2.d/S99sysedge`

For HP-UX, edit the following file:

`/sbin/rc2.d/S990sysedge`

For AIX, edit the following file:

`/etc/rc.tcpip`

You must set the following environment variables in the SystemEDGE startup file to export the environment variables that Oracle requires:

- ORACLE_BASE=/oracle; export ORACLE_BASE
- ORACLE_SID=NHTD; export ORACLE_SID
- ORACLE_HOME=/oracle/product/8.1.5; export ORACLE_HOME
- LD_LIBRARY_PATH=$ORACLE_HOME/lib; export LD_LIBRARY_PATH

For more information, refer to the following sections.

NOTE

The *e*Health AIM for Oracle installation includes a sample SystemEDGE startup file. Do *not* install this sample file in place of your existing file. Use the sample file only as an example to help you edit the existing startup file to export the Oracle environment variables.

Setting Environment Variables for Solaris Systems

Before you start SystemEDGE, add the following to your site's /etc/rc2.d/S99sysedge to customize directory locations for your Oracle installation for Solaris systems:


```
ORACLE_BASE=/export/ahab3/oracle/oracle.8.1.7
export ORACLE_BASE
ORACLE_SID=EH55
export ORACLE_SID
ORACLE_HOME=$ORACLE_BASE
export ORACLE_HOME
LD_LIBRARY_PATH=$ORACLE_HOME/lib:$ORACLE_HOME/jdbc/lib:/usr/dt/lib
export LD_LIBRARY_PATH
```

Setting Environment Variables for AIX Systems

Before you start SystemEDGE, add the following to your site's /etc/rc.tcpip file to customize directory locations for your Oracle installation for AIX systems:

```
ORACLE_BASE=/oracle/u01/app/oracle
export ORACLE_BASE
ORACLE_SID=POS1
export ORACLE_SID
ORACLE_HOME=$ORACLE_BASE/8i
export ORACLE_HOME
LD_LIBRARY_PATH=$ORACLE_HOME/lib
export LD_LIBRARY_PATH
```

Setting Environment Variables for HP-UX Systems

Before you start SystemEDGE, add the following to your site's /etc/rc2.d/S990sysedge file to customize directory locations for your Oracle installation:

```
ORACLE_BASE=/export/ahab3/oracle/oracle.8.1.7
```

```
export ORACLE_BASE
ORACLE_SID=EH55
export ORACLE_SID
ORACLE_HOME=$ORACLE_BASE
export ORACLE_HOME
LD_LIBRARY_PATH=$ORACLE_HOME/lib:$ORACLE_HOME/jdbc/lib:/usr/dt/lib
export LD_LIBRARY_PATH
SHLIB_PATH=$ORACLE_HOME/lib:$ORACLE_HOME/jdbc/lib:/usr/dt/lib
export SHLIB_PATH
LD_PRELOAD=/usr/lib/libpthread.sl:/usr/lib/libcl.sl:/export/ahab3/
oracle/oracle.8.1.7/JRE/lib/PA_RISC/native_threads/libjava.sl
export LD_PRELOAD
```

Verifying that the Startup File is Set Up Correctly

If your SystemEDGE startup file is not set up correctly, you will receive an error message similar to the following:

```
brahma# ../../bin/sysedge
SystemEDGE Version 4.0 Patchlevel 3
Copyright 2001 by Concord Communications, Inc.
load_plugin: dlopen of /opt/EMPsysedge/plugins/oramod/oramod8.so failed, 9,
ld.so.1: ../../bin/sysedge: fatal: libclntsh.so.1.0: open failed: No such file
or directory
sysedge: load plugin /opt/EMPsysedge/plugins/oramod/oramod8.so failed
sysedge: using port 161, config file /etc/sysedge.cf
```

If you receive an error message, verify that you have set up the SystemEDGE startup file correctly and that you have loaded the correct shared library file for your version of Oracle.

Licensing *e*Health AIM for Oracle

Like the SystemEDGE agent, *e*Health AIM for Oracle utilizes a host-based license method. Copies of *e*Health AIM for Oracle can run only on systems that possess a valid license key. This license key is separate from the one used for the SystemEDGE agent.

The first time that you attempt to start the SystemEDGE agent after installing *e*Health AIM for Oracle, the agent displays a message stating that it could not find a valid license for *e*Health AIM for Oracle. It then provides you with a **public key** that is used to generate a permanent license key for your host machine.

A license key is composed of four space-separated, 8-character sequences, totaling 32 characters. The sysedge.lic file contains the *e*Health AIM for Oracle license, as well as the SystemEDGE agent license and other *e*Health AIM licenses. For an example, refer to the sample license file in "Sample License File" on page 33.

Obtaining a License

To obtain a license, you can do any of the following:

- Run the Concord-supplied licenseutil.pl script.
- Run the licenseme.exe license utility.
- Use AdvantEDGE View to receive an SNMP license trap or to query and license the plug-in without a trap. For more information, refer to "Generating a License through AdvantEDGE View Event Processing" on page 30 or "Generating a License through AdvantEDGE View Host Administration" on page 32.
- Send an e-mail request to licenses@concord.com and place the returned license key in the appropriate license file.
- Complete the online license form through the Internet, as described in the next section, "Generating the License through the Web-based License Form."

For more information, refer to the *eHealth SystemEDGE User Guide* and the *Automating the Licensing of SystemEDGE and AdvantEDGE Point Plug-in Modules* white paper.

Generating the License through the Web-based License Form

This section describes how to generate the license using the Web-based license form.

NOTE

If you are using an evaluation copy of *e*Health AIM for Oracle, you must request a temporary license that will enable it to operate during the evaluation period.

To generate a license for *e*Health AIM for Oracle:

1. Start the SystemEDGE agent as follows:
   a. Log in as **root**.
   b. Change directory (cd) to /opt/EMPsysedge.
   c. Enter the following:

```
./bin/sysedge -b
```

   The SystemEDGE agent displays a message indicating that you need a license for the *e*Health AIM for Oracle module on this host machine. It displays a message similar to the following:

```
SystemEDGE Version 4.1 Patchlevel 1
Copyright 2001 by Concord Communications, Inc.
Please contact Concord Communications, Inc. to obtain a license
http://www.concord.com/support, Email: licenses@concord.com
Provide this: sysedge neptune sol2 5.8 346561363366b19c 1.3 Patchlevel 1
```

2. Using a Web browser, go to the licensing Web site at http://license.concord.com, and select the **Create License** option that matches your use of the agent:
   - **Create SystemEDGE/AdvantEDGE Eval License** (if you are evaluating the AIM or are a Concord partner or reseller)
   - **Create SystemEDGE Outsource License** (if you are outsourcing the AIM)

- **Create SystemEDGE/AdvantEDGE License** (if you have purchased the AIM)

NOTE

You must supply a user name and password to access the license form.

If you do not have Web access, fill out the license request form, /config/license.txt (available as part of the *e*Health AIM for Oracle installation), with the complete string generated by the SystemEDGE agent, and e-mail the completed form to licenses@concord.com.

3. Fill out the license form, entering the information that was printed by the SystemEDGE agent. You must supply the following information:
   - Name
   - E-mail address
   - Software version number (1.3 in the example on page 28)
   - Patchlevel (1 in the example on page 28)
   - System name (neptune in the example on page 28)
   - Operating system name (sol2 in the example on page 28)
   - Operating system version (5.8 in the example on page 28)
   - System identifier (346561363366b19c in the example on page 28)

NOTE

Select the option for *e*Health AIM for Oracle from the product list on the licensing form.

After you submit the license request form, the Concord Web server generates a license, displays it on your Web browser, and e-mails it to the contact person in your organization.

4. Copy the license into /etc/sysedge.lic, and save that file.
5. Restart the SystemEDGE agent as root by entering the following:

```
./bin/sysedge -b
```

Generating a License through AdvantEDGE View Event Processing

In order to use AdvantEDGE View event processing to license *e*Health AIM for Oracle, your system must meet the following requirements:

- You must be using SystemEDGE Release 4.0 Patchlevel 3 or later with AdvantEDGE View.
- You must configure the SystemEDGE agent to send SNMP traps to AdvantEDGE View. For more information, refer to the section on configuring the SystemEDGE agent in the *eHealth SystemEDGE User Guide*.
- You must configure the SystemEDGE agent with a read-write community so that AdvantEDGE View can issue an SNMP Set to transmit the license key to it. For more information, refer to the section on configuring the SystemEDGE agent in the *eHealth SystemEDGE User Guide*.
- Your AdvantEDGE View system must have access to the Internet, either directly or through a Web proxy.
- The AdvantEDGE View user who is generating the license must have either write or admin permissions.

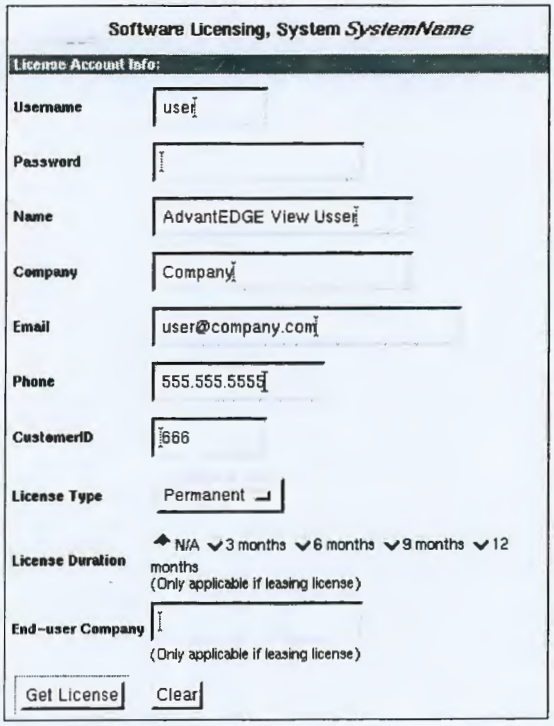
To generate a license through AdvantEDGE View:

1. Start the SystemEDGE agent with *e*Health AIM for Oracle in unlicensed mode. SystemEDGE sends a license trap to AdvantEDGE View for that module.

2. Start AdvantEDGE View, and click the **Events** icon to display the Event Processing screen.

AdvantEDGE View displays a license trap for the system that requires a license.

3. Click the index number for that system to view the Trap Details form for **License Software** to display the AdvantEDGE View Software Licensing form.
4. Complete the licensing form, and click **Get License**.



NOTE

If you have configured AdvantEDGE View preferences, AdvantEDGE View fills in all of the information (except password) on this form.

AdvantEDGE View contacts the Web-based license server, obtains a license for *e*Health AIM for Oracle, and issues an SNMP Set to the target SystemEDGE agent to inform it of the new software license key.

Generating a License through AdvantEDGE View Host Administration

You can also license systems through AdvantEDGE View Host Administration.

To access Host Administration:

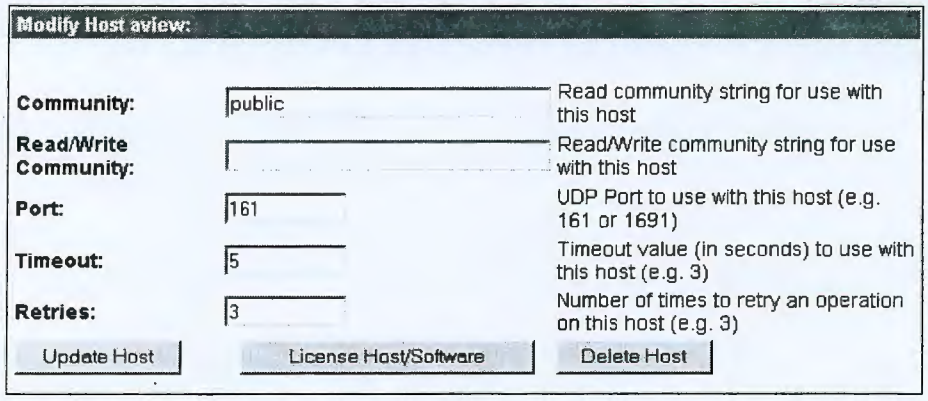
1. Start AdvantEDGE View, and click the **Administration** icon. AdvantEDGE View displays the Administration page.
2. Click the **Host Administration** icon. AdvantEDGE View displays the host list.

SystemEDGE Host Configuration

System Name	Community	Read/Write Community	Port	Timeout	Retries
aviewdemo	public		161	2	2
mailserver	public		161	6	3
nethealth	public		161	3	3
ntclient	public		161	6	3
ntserver	public		161	3	2
unixclient	public		161	6	3
unixserver	public		161	3	3
win2kclient	public		161	5	3
www	public		161	6	3

Add New Host

3. Click the name of the system that you want to license from the **System Name** column. AdvantEDGE View displays the Modify Host form.



4. Click **License Host/Software** to display the licensing form.
5. Select the option for *e*Health AIM for Oracle from the **Product** list, and then click **License Software**.

   AdvantEDGE View contacts the Web-based license server, obtains a license for the software, and issues an SNMP Set to the target SystemEDGE agent, informing it of the new software license key.

Sample License File

The following is a sample SystemEDGE agent license file. A pound character (#) in column 1 indicates that the entire line is a comment.

```
# license file for SystemEDGE Agent
# Concord Communications, Inc.
# http://www.concord.com
# file /etc/sysedge.lic or %SystemRoot%\system32\sysedge.lic
# A valid license key has four parts of 8 characters per part
# parts are separated by space(s) with one license key per line
# sysedge jupiter sol2 5.8 807cb1da007cb1da 4.1 PL 1
e13311d3 0F2a7cb1 abC512dc fF8C923a
# oramod jupiter sol2 5.8 807cb1da007cb1da 1.3 PL 1
a7943fde 098a87ij a4kiuf39 afafEkj4
```

Using the eHealth AIM for Oracle MIB

This chapter explains the organization and content of the Concord Communications MIB for the Oracle application. The MIB specification (oramod.asn1) defines a collection of objects for monitoring and managing Oracle. You must configure the SystemEDGE agent to monitor the *e*Health AIM for Oracle MIB objects that are relevant for your configuration. For more information, refer to Chapter 4, "Using eHealth AIM for Oracle." Figure 3 shows part of the *e*Health AIM for Oracle MIB.

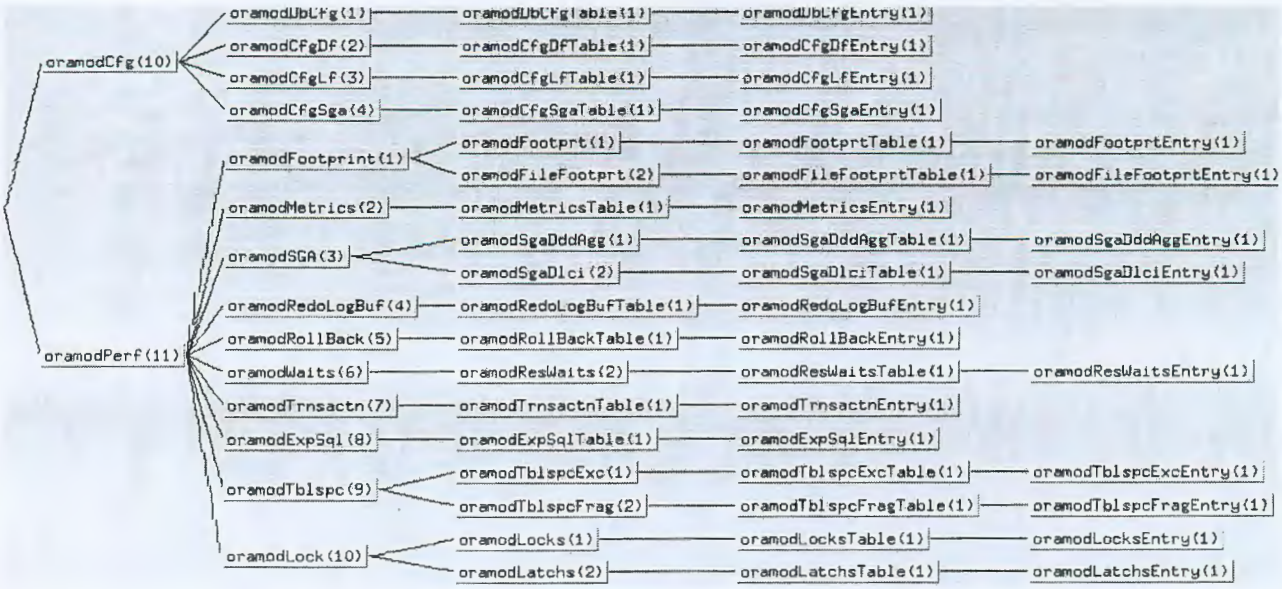


Figure 3. *e*Health AIM for Oracle MIB

The *e*Health AIM for Oracle MIB is organized into sections for database configuration and performance. Within the performance section, a footprint section defines MIB objects that show how much of the underlying system's resources Oracle is consuming. The following sections describe the *e*Health AIM for Oracle MIB. For the most current list of MIB objects, refer to the *e*Health AIM for Oracle MIB specification (oramod.asn1).

Configuration Section

The Configuration section of the *e*Health AIM for Oracle MIB contains configuration parameters and settings that are important for monitoring the health and performance of the Oracle database. The Configuration section includes groups for database, database files, redo logs, and the System Global Area (SGA).

Database Configuration Group

The Database Configuration group contains instance names, index numbers, and initial startup information. Table 3 defines the Database Configuration parameters.

Table 3. MIB Objects – Oracle Database Configuration Group (Page 1 of 3)

MIB Object	Description
oramodDbCfgSIDINDX	Specifies the SID index number.
oramodDbCfgSID	Specifies the database name.
oramodDbCfgVERSION	Provides the description and version of this Oracle installation.
oramodDbCfgHOME	Specifies the installation directory for Oracle.
oramodDbCfgBASE	Specifies the base directory for Oracle, or ORACLEBASE.

Table 3. MIB Objects – Oracle Database Configuration Group (Page 2 of 3)

MIB Object	Description
oramodDbCfgID	Specifies the database ID that was calculated when the database was created; this value is stored in all file headers.
oramodDbCfgCRTDT	Specifies the original creation date and time of the database.
oramodDbCfgLOGMODE	Specifies the archive log mode: NOARCHIVELOG or ARCHIVELOG.
oramodDbCfgCTRLFILETYPE	Specifies the control file type: CURRENT, STANDBY, CLONE, BACKUP, or CREATED.
oramodDbCfgOPENMODE	Indicates whether the database is set to READ WRITE or READ ONLY mode.
oramodDbCfgMAXPROCESS	Specifies the maximum number of user processes that can simultaneously connect to an Oracle server for a multi-process operation.
oramodDbCfgMAXSESSION	Specifies the maximum number of user and system sessions.
ormodDbCfgTIMEDSTATISTICS	Specifies whether timing is on. Set this variable to FALSE for optimum performance.
oramodDbCfgCPUCNT	Specifies the maximum number of CPUs for this instance.
oramodDbCfgSHAREDPOOLSIZE	Specifies the shared pool size in KB. This variable controls the size of the memory area that is used for parsing and executing SQL statements.
oramodDbCfgSHAREDPOOLRSSSIZE	Specifies the shared pool reserved size in KB.
oramodDbCfgLARGEPOOLSIZE	Specifies the large pool reserved size in KB.

Table 3. MIB Objects – Oracle Database Configuration Group (Page 3 of 3)

MIB Object	Description
oramodDbCfgCPUJAVAPOOLSIZE	Specifies the Java pool size in KB. The default value is 20,000 KB.
oramodDbCfgCPUCNTRLFILES	Specifies the name and path of the control files.
oramodDbCfgCPUDBBLKBUFF	Specifies the number of database block buffers in blocks.
oramodDbCfgBLKSIZE	Specifies the size of the database blocks.
oramodDbCfgCKPTINTRVL	Specifies the redo log checkpoint interval.
oramodDBCfgDBFILES	Specifies the maximum number of database files.
oramodDbCfgSORTAREASIZE	Specifies the maximum sort area size. This object controls the amount of memory allocated to each process in the Process Global Area for any sorting activity.
oramodDBCfgOPENCURSORS	Specifies the maximum number of simultaneous open cursors that a single-user process can have.
oramodDBCfgTRNSACTNS	Specifies the maximum number of simultaneous, concurrent transactions.
oramodDBCfgTRNSACTNSPERSEG	Specifies the maximum number of concurrent transactions per segment.
oramodDBCfgMAXROLLSEG	Specifies the maximum number of rollback segments.

Database File Configuration Group

The Database File Configuration group describes the Oracle database files. Table 4 defines the Database File Configuration parameters.

Table 4. MIB Objects – Oracle Database File Configuration Group (Page 1 of 2)

MIB Object	Description
oramodCfgDfFILENUM	Specifies the file identification number.
oramodCfgDfSTATUS	Specifies the type of file (system or user) and its status. The value can be OFFLINE, ONLINE, SYSTEM, RECOVER, or SYSOFF.
oramodCfgDfENABLED	Describes how accessible a file is from SQL. The value can be DISABLED, READ ONLY, READ WRITE, or UNKNOWN.
oramodCfgDfUNRCVRBLECHG	Specifies the last unrecoverable change number that was made to this data file.
oramodCfgDfUNRCVRBLETIME	Specifies the last unrecoverable change time that was made to this data file.
oramodCfgDfKBYTES	Specifies the current size of the file in kilobytes (KB).
oramodCfgDfCRTKBYTES	Specifies the size of the data file when it was created.
oramodCfgDfFNAME	Specifies the file name.
oramodCfgDfCRTTIME	Specifies the time at which the data file was created.
oramodCfgDfTBLSPACENUM	Specifies the tablespace number.
oramodCfgDfTBLESPACERFILENUM	Specifies the tablespace relative data file number.
oramodCfgDfBLOCKS	Specifies the current size of the data file in blocks.

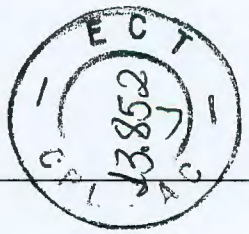


Table 4. MIB Objects – Oracle Database File Configuration Group (Page 2 of 2)

MIB Object	Description
oramodCfgDfBLOCKSIZE	Specifies the block size of the data file.
oramodCfgDfERROR	Indicates whether the datafile header read an error. If so, a restore is required. A value of NULL indicates success.
oramodCfgDfRECOVER	Indicates whether the file needs media recovery. The value can be YES or NO.
oramodCfgDfRSTLOGSCHGNUM	Specifies the reset log change number.
oramodCfgDfRSTLOGSTIME	Specifies the reset log timestamp.

Redo Log File Configuration Group

The Redo Log File Configuration group describes the redo log file locations and status for each Oracle installation. Table 5 defines the Redo Log File Configuration parameters.

Table 5. MIB Objects – Oracle Redo Log File Configuration Group

MIB Object	Description
oramodCfgLfMEMBERINDX	Specifies the log file member index.
oramodCfgLfGROUPNUM	Specifies the log file group number.
oramodCfgLfSTATUS	Specifies the log file status.
oramodCfgLfMEMBER	Specifies the log file name and path.

System Global Area Configuration Group

The System Global Area (SGA) Configuration group summarizes the Oracle system global area. Table 6 defines the SGA Configuration parameters.

Table 6. MIB Objects – Oracle SGA Configuration Group

MIB Object	Description
oramodCfgSgaTOTALMEMALLOC	Specifies the total real memory allocated.
oramodCfgSgaFIXEDSGA	Specifies the fixed memory allocated in KB.
oramodCfgSgaVARIABLE	Specifies the variable memory that is allocated in the SGA.
oramodCfgSgaDBBUFF	Specifies the database buffers allocated in KB. The typical range is from 4 KB to 2 GB.
oramodCfgSgaREDOBUFF	Specifies the redo buffers allocated in KB.

Performance Section

The Performance section of the *e*Health AIM for Oracle MIB contains performance data that is necessary for capacity planning and trend analysis, as well as real-time performance and availability monitoring. The Performance group is divided into subgroups for footprint data, metrics, the SGA, redo logs, rollback segments, waits, expensive SQL, tablespaces, and locks.

Oracle Footprint Group

The Footprint group provides information about the Oracle CPU, memory, data flow, and disk-resource consumption, more commonly called the **footprint**. Long-term trending analysis of footprint information is useful for anticipating and avoiding problems due to resource exhaustion. You can also monitor footprint information in real time to detect and correct temporary resource exhaustion due to viruses, security incidents, and hardware failures. The Footprint group includes subgroups for footprint and file footprint.

Footprint Group

The Footprint group describes the performance footprint for each Oracle service. Table 7 defines the Oracle Footprint parameters.

Table 7. MIB Objects – Oracle Footprint Group (Page 1 of 2)

MIB Object	Description
oramodFootprtCPUTIME	Specifies the CPU time in seconds accumulated by Oracle. This time includes all core components and the database instance.
oramodFootprtPERCENTCPU	Specifies the percentage of CPU utilization by Oracle over the last sample interval. This value is reported as the percentage multiplied by 100. It is the sum of the CPU utilization of all Oracle core services and components, and provides a good indication of the CPU resource consumption by the entire Oracle application. Do **not** use this variable as a counter.
oramodFootprtMEMSIZE	Specifies the combined size of all Oracle text, data, and stack segments in KB. This value is the sum of all process sizes for all core Oracle services and optional connectors.
oramodFootprtRSS	Specifies the total real memory (resident size set [RSS]) of Oracle in KB. This value is the sum of process RSS for all core Oracle services and optional connectors.
oramodFootprtPERCENTMEM	Specifies the percentage (0-100) of real memory used by Oracle, including core services and optional connectors.
oramodFootprtTHREADS	Specifies the total number of threads operating within the respective Oracle components as seen by the operating system.
oramodFootprtINBLKS	Specifies the number of blocks of data input by the processes.
oramodFootprtOUTBLKS	Specifies the number of blocks of data output by the processes.
oramodFootprtMSGSSENT	Specifies the number of messages sent by the processes.

Table 7. MIB Objects – Oracle Footprint Group (Page 2 of 2)

MIB Object	Description
oramodFootprtMSGSRCVD	Specifies the number of messages received by the processes.
oramodFootprtSYSCALLS	Specifies the number of system calls invoked by the processes.
oramodFootprtMINORPGFLTS	Specifies the number of minor page faults incurred by the process.
oramodFootprtMAJORPGFLTS	Specifies the number of major page faults incurred by the process.
oramodFootprtNUMSWAPS	Specifies the number of times the processes have been swapped.
oramodFootprtVOLCNTX	Specifies the number of voluntary context switches incurred by the processes.
oramodFootprtINVOLCNTX	Specifies the number of involuntary context switches incurred by the processes.
oramodFootprtHOMESIZE	Specifies the size in KB of the Oracle root directory and all files beneath it.
oramodFootprtDBDISKSIZE	Specifies the size in KB of all Oracle database disk storage areas. This value is a sum of all database files.
oramodFootprtSTARTUPTIME	Specifies the date and time that the Oracle instance was started.
oramodFootprtSTATUS	Specifies the status of the instance: STARTED, MOUNTED, or OPEN.
oramodFootprtDATABASESTATUS	Specifies the database status of the instance.
oramodFootprtSHUTDOWNPENDING	Specifies whether the database is about to be shut down: YES or NO.

File Footprint Group

The File Footprint group describes the Oracle file footprint. Table 7 defines the Oracle File Footprint parameters.

Table 8. MIB Objects – Oracle File Footprint Group

MIB Object	Description
oramodFFootprtFILEINDX	Specifies the file index number.
oramodFFootprtFILETYPE	Specifies the file type.
oramodFFootprtFILENAME	Specifies the file name.
oramodFFootprtCRTTS	Specifies the timestamp of the last update.
oramodFFootprtCRTKBYTES	Specifies the file creation size in KB.
oramodFFootprtKBYTES	Specifies the file size in KB.
oramodFFootprtBLOCKS	Specifies the file blocks.
oramodFFootprtSTATUS	Specifies the file status.
oramodFFootprtRECOVER	Indicates whether the file needs recovering.
oramodFFootprtAVGIOTIM	Specifies the average input/output time for the file.

Metrics Group

The Metrics Group describes the Oracle database metrics. Table 9 defines the Oracle Metrics parameters.

Table 9. MIB Objects – Oracle Metrics Group (Page 1 of 4)

MIB Object	Description
oramodMetricsBCPT	Block Changes Per Transaction (scaled by 100). Measures the amount of data manipulation language (DML) work that each transaction performs.
oramodMetricsBGR	Block Get Rate per second (scaled by 100). Measures the rate at which application systems reference the database.
oramodMetricsBVPT	Block Visits Per Transaction (scaled by 100). Measures the database load imposed for each transaction.
oramodMetricsCHR	Cache Hit Ratio (scaled by 100). Measures the effectiveness of the hits against the buffer cache.
oramodMetricsCR	Call Rate (user and recursive) over time. Measures the work demand rate that all work sources are placing on the database instance.
oramodMetricsCPT	Calls Per Transaction (scaled by 100). Indicates the number of database requests per committed transaction.
oramodMetricsCBR	Changed Blocks (scaled by 100). Measures the balance between queries and DML and can indicate changes in application use or indexes.
oramodMetricsCCR	Consistent Change Ratio (scaled by 100). Measures consistent database changes and gets, or the extent to which applications are exercising the read-consistency mechanism.
oramodMetricsCRR	Continued Row Ratio (scaled by 100). Measures the space usage of data blocks.
oramodMetricsLCM	Library Cache Miss Ratio (scaled by 100). Measures the missed requests and reloads to access library-cached objects since instance startup. Monitor the library cache to help determine whether you should resize the shared pool.

Table 9. MIB Objects – Oracle Metrics Group (Page 2 of 4)

MIB Object	Description
oramodMetricsRTUC	Recursive To User Call Ratio (scaled by 100). Measures the ratio of recursive and user to application calls.
oramodMetricsRLSW	Redo Log Space Wait Ratio (scaled by 100). Shows the rate at which failures are occurring in writing to the redo log space. It can measure memory allocation.
oramodMetricsRSR	Row Source Ratio (scaled by 100). Specifies the percentage of total rows retrieved from full table scans.
oramodMetricsSOR	Sort Overflow Ratio (scaled by 100). Indicates the number of sorts that are using temporary segments.
oramodMetricsTRR	Transaction Rate Ratio (scaled by 100). Indicates the rate at which users or applications are committing transactions.
oramodMetricsUCR	User Call Rate Ratio (scaled by 100). Indicates the rate at which client users or applications are requesting SQL statements.
oramodMetricsUCPP	User Calls Per Parse Ratio (scaled by 100). Specifies the ratio of user calls to parses in the shared SQL area. This value indicates how well the application is managing its context area.
oramodMetricsURR	User Rollback Ratio (scaled by 100). Indicates the rate at which application transactions are failing.
oramodMetricsSGALCE	Library Cache Efficiency Percentage (scaled by 100). Specifies the percentage of times that an SQL statement did not need to be reloaded because it was already in the library cache.
oramodMetricsSGADDCE	Data Dictionary Cache Efficiency Percentage (scaled by 100). Shows the ratio of gets to misses within the shared pool.
oramodMetricsDBTOTALRW	Specifies the total number of physical reads and writes since the instance started.
oramodMetricsDBBLKCHG	Specifies the total number of database block changes.

Table 9. MIB Objects – Oracle Metrics Group (Page 3 of 4)

MIB Object	Description
oramodMetricsDBBLKGET	Specifies the total number of database block gets since the instance started.
oramodMetricsDBCNSTGET	Specifies the total number of consistent gets since the instance started.
oramodMetricsDBPHYSREAD	Specifies the total number of physical reads since the instance started.
oramodMetricsDBSORTDISK	Specifies the total number of database disk sorts since the instance started.
oramodMetricsDBSORTMEM	Specifies the total number of database memory sorts since the instance started.
oramodMetricsBLKFREEWAIT	Specifies the percentage of times that a request resulted in a wait for a free block.
oramodMetricsMTHRDQUEUEWAIT	Specifies the number of seconds that a request waited in the queue for multi-threaded servers.
oramodMetricsSESSHIWTRMEM	Specifies the maximum high-water amount of session memory that has been used.
oramodMetricsSESSCURRMEM	Specifies the current maximum amount of session memory that has been used.
oramodMetricsSESSHIWTR	Specifies the high-water mark for the number of sessions.
oramodMetricsSESSCURRENT	Specifies the current number of sessions.
oramodMetricsUSERCOMMITS	Specifies the number of successfully completed and aborted database transactions.
oramodMetricsUSERROLLBACK	Specifies the number of transactions that have been rolled back since the instance started.
oramodMetricsUSERCALLS	Specifies the number of transactions that have been started since the instance started.
oramodMetricsDBPHYSWRTS	Specifies the total number of physical writes since the instance started.

Table 9. MIB Objects – Oracle Metrics Group (Page 4 of 4)

MIB Object	Description
oramodMetricsTBLSCANROWS	Specifies the number of rows that were retrieved through table scans since the instance started.
oramodMetricsTBLFTCHROWID	Specifies the number of rows that were retrieved through table fetches by row ID since the instance started.
oramodMetricsTBLFTCHCROW	Specifies the number of rows that were retrieved through table fetches by row since the instance started.
oramodMetricsRECRSVCALLS	Specifies the number of recursive calls since the instance started.
oramodMetricsCNSTCHGS	Specifies the number of consistence changes since the instance started.
oramodMetricsPARSECNT	Specifies the number of parses since the instance started.
oramodMetricsCPUTM	Specifies the amount of time that was taken to work requests.
oramodMetricsLOGFILESWTCH	Specifies the number of redo log file switches.

SGA Group

The SGA area of the Oracle MIB stores aggregate information about the performance of the dictionary cache. Each user and data request that connects to the database references this data dictionary. Retaining as much of the data dictionary information as possible in memory contributes to database efficiency. The SGA Group includes subgroups for Data Dictionary Aggregate (DDA) and Detailed Library Cache Information (DLCI).

SGA DDA Group

The SGA DDA group describes the data dictionary aggregates. Table 10 defines the Oracle SGA DDA parameters.

Table 10. MIB Objects – Oracle SGA DDA Group

MIB Object	Description
oramodSGAAGGCNT	Specifies the total number of entries in the data dictionary cache since the instance started.
oramodSGAAGGUSGE	Specifies the total number of cache entries with valid data since the instance started.
oramodSGAAGGFIX	Specifies the total number of fixed entries in the data dictionary cache since the instance started.
oramodSGAAGGGET	Specifies the total number of information requests since the instance started.
oramodSGAAGGGETMISS	Specifies the total number of information requests that resulted in cache misses since the instance started.
oramodSGAAGGSCAN	Specifies the total number of scan requests since the instance started.
oramodSGAAGGSCANMISS	Specifies the total number of scan requests that resulted in misses since the instance started.
oramodSGAAGGSCANCPLT	Specifies the total number of times that the list was scanned completely since the instance started.
oramodSGAAGGMODS	Specifies the total number of insertions, updates, and deletions since the instance started.
oramodSGAAGGFLUSH	Specifies the total number of times the data was flushed to disk since the instance started.

SGA DLCI Group

The SGA DLCI group describes the detailed library cache information. Table 11 defines the Oracle SGA DLCI parameters.

Table 11. MIB Objects – Oracle SGA DLCI Group

MIB Object	Description
oramodSGADLCINAME	Specifies the Library Cache Namespace: SQL AREA, TABLE/PROCEDURE, BODY, TRIGGER, INDEX, CLUSTER, OBJECT, or PIPE.
oramodSGADLCIGET	Specifies the total number of request handles to the library namespace since instance startup.
oramodSGADLCIGETHIT	Specifies the total number of times that handles were already allocated in the cache.
oramodSGADLCIGETHITRT	Specifies the Get/Hit ratio that indicates the percentage of parse calls that find a cursor to share.
oramodSGADLCIPIN	Specifies the number of pin requests for objects in the cache since the instance started.
oramodSGADLCIPINHIT	Specifies the number of pin hits or executions of objects that are already allocated and initiated in the cache.
oramodSGADLCIPINHITRT	Specifies the ratio of pin hits to pins.
oramodSGADLCIRELOAD	Specifies the number of times a statement had to be reparsed in order to be executed.
oramodSGADLCIINVALID	Specifies the number of times that non-persistent library objects have been invalidated.

Redo Logs Group

Oracle stores data that is being changed by transactions in redo logs. The application can later use these redo logs to perform database recoveries, if necessary. Table 12 defines the Oracle Redo Log parameters.

Table 12. MIB Objects – Oracle Redo Log Group

MIB Object	Description
oramodREDOBLKWRT	Specifies the total number of redo blocks written since instance startup.
oramodREDOENTRIES	Specifies the total number of redo entries in the redo log since instance startup.
oramodREDOSIZE	Specifies the size of the redo log.
oramodREDOSPACERQST	Specifies the number of redo log space requests. If this value is not close to zero, the buffer is too small.
oramodREDOSPACEWAIT	Specifies the total number of redo log space wait times since the instance started.
oramodREDOSYNCHWRT	Specifies the total number of redo synch writes since the instance started.
oramodREDOSSYNCHTM	Specifies the total amount of redo synch time.
oramodREDOWASTAGE	Specifies the total amount of redo log waste.
oramodREDORETRIES	Specifies the total number of redo retries.

Rollback Segment Group

The Rollback Segment section of the Oracle MIB records cumulative statistics about the use of all rollback segments since the database was last started. These segments contain records of data that have not yet been modified in a transaction. The database can use these segments to remove changes that were performed for a transaction that was canceled. That is, they can return the record to the state it was in before any changes were

made. For best performance, try to size the rollback segment so that each of its extents is large enough to support a typical transaction. Table 13 defines the Oracle Rollback Segment parameters.

Table 13. MIB Objects – Oracle Rollback Segment Group (Page 1 of 2)

MIB Object	Description
oramodRollBackSEGNAME	Specifies the rollback segment name.
oramodRollBackEXTENTS	Specifies the total number of rollback segment extends since the instance started.
oramodRollBackRSSIZE	Specifies the size of the rollback segment.
oramodRollBackWRITES	Specifies the total number of segment Writes since the instance started.
oramodRollBackGETS	Specifies the total number of rollback segment Gets since the instance started.
oramodRollBackWAITS	Specifies the total number of rollback segment Waits since the instance started.
oramodRollBackOPTSIZE	Specifies the optimal size of the rollback segment. Base this value on application use to minimize space management issues.
oramodRollBackSHRINKS	Specifies the total number of rollback segment shrinks (return to normal size after an extend) since the instance started.
oramodRollBackWRAPS	Specifies the total number of rollback segment wraps since instance startup. If this value is not equal to zero, recreate the rollback segments with larger extent sizes.
oramodRollBackEXTENDS	Specifies the number of rollback segments extends (extensions for handling larger transactions that what the segment was designed to handle).

Table 13. MIB Objects – Oracle Rollback Segment Group (Page 2 of 2)

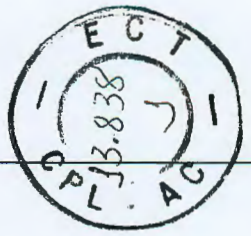
MIB Object	Description
oramodRollBackAVESHRINK	Specifies the average shrink size of this rollback segment since the instance started.
oramodRollBackAVEACTIVE	Specifies the average activity for this rollback segment since the instance started.
oramodRollBackSTATUS	Specifies the rollback segment status.

Waits Group

Wait time contributes most significantly to total response time. The Waits table identifies the events that are contributing to the longest wait times. Table 14 defines the Oracle Waits parameters.

Table 14. MIB Objects – Oracle Waits Group

MIB Object	Description
oramodWaitsEVENT	Specifies the name of the resource that is experiencing waits.
oramodWaitsTOTALWAITS	Specifies the total number of waits for the resource.
oramodWaitsTOTALTIMOUT	Specifies the total number of timeouts for the resource.
oramodWaitsTIMEWAITED	Specifies the total time the resource waited.
oramodWaitsAVGWAIT	Specifies the average time the resource waited.



Expensive SQL Group

SQL queries that are not optimized can significantly reduce the overall performance of a system. The Expensive SQL table identifies statements that require too many disk reads or parses. Table 15 defines the Oracle Expensive SQL parameters.

Table 15. MIB Objects – Oracle Expensive SQL Group

MIB Object	Description
oramodExpSqlEXECUTION	Specifies the number of executions of expensive SQL.
oramodExpSqlDISKREAD	Specifies the number of disk reads.
oramodExpSqlPARSECNT	Specifies the number of parses. A large number of hard parses requires more memory for the shared pool.
oramodExpSqlBUFFGETS	Specifies the number of Buffer Gets.
oramodExpSqlSORTS	Specifies the number of Sorts.
oramodExpSqlSQL	Specifies the SQL statement.

Tablespace Group

The Tablespace group identifies the fragmentation within each database tablespace. For best performance, you must have enough free block space to fill database requests. The Tablespace table describes the amount of space left in a tablespace after the next largest extent of any table in the tablespace is allocated. Table 16 defines the Oracle Tablespace parameters.

Table 16. MIB Objects – Oracle Tablespace Group

MIB Object	Description
oramodTblspTBLSPINDX	Specifies the tablespace index number.
oramodTblspTBLSPNAME	Specifies the tablespace name.
oramodTblspKBYTESLEFT	Specifies the number of KB that are left after the next largest extent is allocated.
oramodTblspFILNAME	Specifies the tablespace file name.
oramodTblspEXTENTS	Specifies the number of extents.
oramodTblspLRGEXTENT	Specifies the size in bytes of the largest extent.
oramodTblspSMEXTENT	Specifies the size in bytes of the smallest extent.
oramodTblspINCREMENTBY	Specifies the size in bytes of the next extent increment.
oramodTblspBYTESCOALSD	Specifies the number of free bytes that were coalesced.
oramodTblspBYTESFREE	Specifies the number of free bytes that are available.

Lock Group

Locks are access restrictions in a multi-user environment. They can maintain security and protect the integrity of the data by remaining in place until a commit (which saves all changes to a database since the start of a transaction) or rollback (which removes updates performed by a partially completed transaction) takes place. The Lock Group includes subgroups for locks and latches.

Locks Group

The Locks table identifies lock holders and requestors. Table 17 defines the Oracle Locks parameters.

Table 17. MIB Objects – Oracle Locks Group

MIB Object	Description
oramodLockUSERINDX	Specifies the user's index number.
oramodLockUSERNAME	Specifies the name of the user who is holding the lock.
oramodLockOBJECT	Specifies the name of the locked object.
oramodLockTYPE	Specifies the object type of the locked object.
oramodLockMODE	Specifies the type of lock mode that is being held: Null, Row share, Row exclusive, Share, Share row exclusive, or Exclusive.
oramodLockCTIME	Specifies the amount of time since the current mode was granted.
oramodLockBLOCK	Indicates whether the lock is blocking another lock.

Latches Group

Latches are subsets of locks that can prevent access to Oracle internal memory structures while a process is accessing them. If the database spends too much time waiting for latches, it can affect performance. The Latch table identifies latches held per instance. Table 18 defines the Oracle Latch parameters.

Table 18. MIB Objects – Oracle Latch Group (Page 1 of 2)

MIB Object	Description
oramodLatchLATCHNUM	Specifies the latch number.
oramodLatchLATCHNAME	Specifies the latch name.
oramodLatchGETS	Specifies the number of times that Oracle satisfied requests for latches without waiting.

Table 18. MIB Objects – Oracle Latch Group (Page 2 of 2)

MIB Object	Description
oramodLatchMISSES	Specifies the number of times that Oracle did not satisfy latch requests.
oramodLatchSLEEPS	Specifies the number of latch sleeps.
oramodLatchIMDGETS	Specifies the number of latch immediate gets.
oramodLatchIMDMISSES	Specifies the number of latch immediate misses.
oramodLatchWAITSHOLDING	Specifies the number of latch waits that are holding.
oramodLatchSPINGETS	Specifies the number of latch spin gets.

Backup Group

The Backup group provides physical backup information. Table 19 defines the Backup parameters.

Table 19. MIB Objects – Oracle Backup Group

MIB Object	Description
oramodBackupFILENUM	Specifies the backup file index number.
oramodBackupSTATUS	Specifies the status of the backup.
oramodBackupCHANGENUM	Specifies the change number of the backup file.
oramodBackupDATE	Specifies the date of the backup.

Archive Group

The Archive group provides physical backup information. Table 20 defines the Backup parameters.

Table 20. MIB Objects – Oracle Archive Group

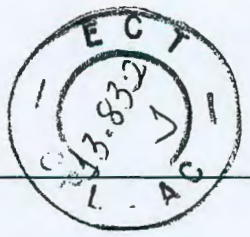
MIB Object	Description
oramodArcDestARCMODE	Specifies the mode of the archive log.
oramodArcDestSTATUS	Specifies the status of the archive log file.
oramodArcDestDEST	Specifies the archive log file destination.

Using eHealth AIM for Oracle

This chapter describes how to configure and use *e*Health AIM for Oracle. This module is implemented as a SystemEDGE agent plug-in. After you enable this plug-in in the sysedge.cf file and obtain a license for it, SystemEDGE will load it automatically at startup. For more information, refer to "Editing the sysedge.cf File" on page 21 and "Licensing eHealth AIM for Oracle" on page 26.

*e*Health AIM for Oracle implements additional MIB objects that provide advanced information about the health and availability of Oracle databases. It can operate with any SNMP-compliant management software such as Concord's *e*Health suite of products, AdvantEDGE View, HP OpenView, and others. If you are using *e*Health AIM for Oracle with *e*Health, refer to the *e*Health Web Help for more information about the reports that you can generate.

The default configuration settings of the *e*Health AIM for Oracle plug-in enable you to use the advanced self-monitoring capabilities of the SystemEDGE agent in conjunction with *e*Health AIM for Oracle.



*e*Health AIM for Oracle MIB Branch

You can use AdvantEDGE View or another SNMP tool to edit the SystemEDGE configuration file to utilize the *e*Health AIM for Oracle MIB objects with the process-monitoring, threshold-monitoring, and history-collection features of the SystemEDGE agent. All MIB objects that are related to *e*Health AIM for Oracle exist at object identifier (OID) branch *1.3.6.1.4.1.546.16.4* in the Concord Systems Management MIB. The MIB is defined in the `oramod.asn1` file, which is available in the *e*Health AIM for Oracle product installation.

Assigning Entry Rows in the SystemEDGE Self-Monitoring Tables

All SystemEDGE self-monitoring tables (including log monitoring, process/service monitoring, threshold monitoring, and history collection) require the use of unique row numbers. Each table contains an **Index** column which acts as a **key field** to distinguish rows in the table. This section describes the benefits of reserving a block of rows (in the range of 11 to the maximum number of rows in your table) for use by the system or application administrator.

Setting Local Policy

You may choose, as a matter of local policy, to reserve a block of rows for system administration. This policy allows you to define entries within a reserved block of rows without being concerned that the row might already be taken by another user's entry. In compliance with the local policy, all other users should use row indices that are outside the reserved range when they define user-configured entries.

Reserving Blocks of Rows

By reserving a block of rows, you can define a consistent set of conditions (row entries) to be monitored across all machines such that the same condition is defined in the same row number on each machine. For example, you can use row 3000

in each table to define entries monitoring the MIB object for total number of SQL disk reads (oramodExpSqlDISKREAD). You can then distribute this configuration to every host so that every system that is running Oracle uses row 3000 for monitoring the number of SQL disk reads, for each SystemEDGE self-monitoring table.

To reserve a block of rows for monitoring Oracle:

1. Decide which block of rows you want to reserve for use with monitoring Oracle.
2. Use that block of rows to define a set of row entries for each SystemEDGE self-monitoring table. For more information, refer to the chapter on self-monitoring in the *eHealth SystemEDGE User Guide*.
3. Distribute configuration file entries to all hosts that are running Oracle and *e*Health AIM for Oracle. For more information, refer to the *Automating the Deployment of SystemEDGE and the AdvantEDGE Point Plug-in Modules* white paper.

   NOTE

   As an alternative, you can use this row-number assignment policy with AdvantEDGE View for group-configuration operations.

4. Require end users to avoid your block of rows when defining their own self-monitoring table entries.

Using the SystemEDGE Self-Monitoring Features

This section provides examples of how to use SystemEDGE process, threshold, and history monitoring to monitor the Oracle application. Add these commands to the sysedge.cf file to enable monitoring of the MIB objects that they specify. Modify these examples as necessary to monitor the MIB objects that are relevant for your configuration.

The examples in this section use row numbers in the 5000 range; use a row number for your configuration that conforms to local policies. For more information on row assignment, refer to "Assigning Entry Rows in the SystemEDGE Self-Monitoring Tables" on page 60.

The following command, for example, instructs the SystemEDGE agent to monitor the RSS of the Oracle database every 60 seconds for values that are greater than 50,000 and to store the data in row 5001 of the Threshold Monitoring table:

```
monitor oid oramodFootprtRSS 5001 0x0 60 absolute > 50000 'Total
Resident Memory' ''
```

For more information about the syntax for the commands in this section, refer to the *eHealth SystemEDGE User Guide*. For more information about *e*Health AIM for Oracle MIB objects, refer to Chapter 3, "Using the eHealth AIM for Oracle MIB," or to the MIB specification (oramod.asn1).

NOTE

Enter the commands throughout this chapter on one line. Do *not* use a carriage return to match the formatting shown here.

Using SystemEDGE Process Monitoring

This section provides an example of how to use the SystemEDGE agent to monitor the availability of a critical Oracle process. For more information, refer to the chapter on process monitoring in the *eHealth SystemEDGE User Guide*.

Monitoring the Oracle database

To ensure that the Oracle database is running, enter the following command in the sysedge.cf file:

```
watch process procAlive 'oracle' 5000 30 'Oracle Database' ''
```


Using SystemEDGE Threshold Monitoring

This section provides examples of how to use the SystemEDGE agent to monitor important Oracle metrics. Add the commands that are provided in the following sections to the sysedge.cf file to monitor thresholds for these MIB objects. For more information, refer to the chapter on threshold monitoring in the *eHealth SystemEDGE User Guide.*

NOTE

The thresholds used in this section may not be appropriate for your Oracle application; select thresholds that are appropriate for your environment.

Monitoring Total Resident Memory Size of an Oracle Service

To monitor the total resident memory size of an Oracle service, enter the following:

```
monitor oid oramodFootprtRSS 5001 0x0 60 absolute > 50000 'Total
Resident Memory' ''
```

Monitoring Combined Size of Oracle Text, Data, and Stack Segments

To monitor the total size of the Oracle text, data, and stack segments, enter the following:

```
monitor oid oramodFootprtMEMSIZE 5002 0x0 60 absolute > 1000000 'Total
Memory Size' ''
```

Monitoring Total Size of Oracle Redo Log File

To monitor the total size of the Oracle redo log file, enter the following:

```
monitor oid oramodREDOSIZE 5003 0x0 60 absolute > 500000 'Total Redo
Log Size' ''
```

Monitoring Total Number of Database Disk Sorts

To monitor the total number of database disk sorts, enter the following:

```
monitor oid oramodMetricsDBSORTDISK 5004 0x0 60 absolute > 50000 'Total
Number Database Disk Sorts' ''
```

Using SystemEDGE History Collection

This section provides examples of how to use SystemEDGE history capabilities to track the value of important Oracle metrics over time. Add the commands that are provided in the following sections to the sysedge.cf file to collect history for these MIB objects. For more information about history collection, refer to the chapter on history collection in the *eHealth SystemEDGE User Guide.*

NOTE

The number of samples and the interval between samples used in this section may not be appropriate for your Oracle system; select values that are suitable for your environment.

Collecting History on Number of Hits to the Database

To collect history on the number hits to the database, enter the following:

```
emphistory 5000 60 oramodMetricsCHR 300 'Total Hits To Oracle Database'
```

Collecting History on Block Changes Per Transaction

To collect history on the number of block changes per transaction for the Oracle database, enter the following:

```
emphistory 5001 60 oramodMetricsBCPT 300 'Oracle Database Block Changes
Per Transaction'
```

Collecting History on the Number of Transactions Started

To collect history on the number of transactions started since the last instance startup, enter the following:

```
emphistory 5002 60 oramodMetricsUSERCALLS 300 'Total Transactions
Started Since Instance Startup'
```

Glossary

Abstract Notation One (ASN.1) A language that describes data types independent of computer structures and representations. For more information refer to ISO International Standard 8824.

AdvantEDGE View A Web-based management interface for use with the SystemEDGE agent that enables an administrator to use a Web browser to manage systems and applications.

agent In network management, a program that provides information from a management information base (MIB) for SNMP agents. *e*Health or a network management system (NMS) use the information about managed devices and take corrective action when appropriate.

American Standard Code for Information Interchange (ASCII) The most common format for character representation in computers and the Internet. Characters fit into a single byte. It was developed by the American National Standards Institute (ANSI).

application A program that performs a specific function for one or more users or for another application program. Types of applications include communication programs, management programs, word processors, databases, and drawing programs.

ASCII *See* American Standard Code for Information Interchange (ASCII).

ASN.1 *See* Abstract Notation One (ASN.1).

baseline A level of performance that is considered normal, average, or typical over a period of time such as a day, week, or month. Compare current performance metrics against baseline data to identify trends in performance levels and service delivery.

buffer A temporary storage area for data. Often implemented as holding areas between the backplane and an interface; data remains in the buffer until it can be transmitted on the interface or processed by the central processing unit (CPU).

capacity A measurement of the volume that an element can support. For interfaces, this is the bandwidth that can be carried. For hard disks, this is the disk size or the amount of information that can be stored on the disks. *See also* traffic.

central processing unit (CPU) The component within a device that performs the instruction execution for the applications and programs that run on the device. Also referred to as a processor or microprocessor.

client A computer system, usually a desktop computer or laptop, that presents data directly to a user and accepts input. They drive the computing process, supporting local processing and accessing remote servers as needed for data access and analysis.

Also refers to the application software residing on a machine that is used by an end user.

congestion A condition in which the network traffic is greater than the amount that the network can carry. Often causes performance problems and delays on a network.

CPU *See* central processing unit (CPU).

Database Management System (DBMS) A program such as Oracle, Microsoft SQL Server, or Sybase for creating and providing access to one or more databases.

delay The time required for a packet or frame to travel from the sending station (source) to the receiving station (destination).

disk thrashing A condition that results when a server performs high disk input /output (I/O) operations—reads and writes to the disk—without producing actual work. Often occurs when a server performs excessive paging and swapping due to physical memory limitations.

DNS *See* domain name system (DNS).

domain name system (DNS) The system that locates and translates Internet domain names such as concord.com into Internet Protocol (IP) addresses. A DNS server is typically a device that translates domain names to IP addresses within your network.

***e*Health AIM** *See* eHealth application insight module.

***e*Health application insight module** A plug-in (supplementary program) that extends the functionality of the SystemEDGE agent. AIMs add the capability to manage application-specific events, processes, thresholds, and health.

event An occurrence on a system that typically results in a message, such as an SNMP trap, being sent to a configured management system. Common events include system failures, system reboots, exceeded thresholds, or any user-configurable situation that the user wants to identify.

File Transfer Protocol (FTP) A means for uploading and downloading files on the Internet (the oldest Internet protocol for retrieving files). You can use an FTP client application to request files from or transfer files to an FTP server.

FTP *See* File Transfer Protocol (FTP).

Host Resources MIB A MIB (management information base) that defines a set of objects that are useful for the management of host computers. For example, it defines host storage areas, devices, and file systems. This MIB is defined in RFC 1514.

hostname The name for an individual IP (Internet Protocol) address on a computer. While many computers have only one hostname, some machines, such as network servers have multiple hostnames.

HTML *See* Hypertext Markup Language (HTML).

HTTP *See* Hypertext Transfer Protocol (HTTP).

Hypertext Markup Language (HTML) A programmatic language used for controlling the way that text and images appear when a file is displayed on the World Wide Web.

Hypertext Transfer Protocol (HTTP) An application protocol that defines the set of rules for exchanging files (text, graphics, multimedia, and other files) on the World Wide Web.

Hertz (Hz) A unit of frequency of one cycle per second that measures the change in the state of an alternating current, sound wave, or other cyclical wave form.

I/O *See* input/output (I/O).

Information Technology (IT) A widely-used term to describe all of the technologies used for creating, exchanging, managing, and using information in various forms.

input/output (I/O) Any operation, program, or device that transfers data to or from a computer.

internet infrastructure The applications, systems, and networks that a company uses to run its business, for both internal use and for interfaces to the outside world.

Internet Protocol (IP) The method (or protocol) by which packets of information are sent across the Internet. IP defines addressing, error handling, routing, and option codes for data transmission. IP requires no continuing connection between the endpoints that are communicating.

IP *See* Internet Protocol (IP).

IT *See* Information Technology (IT).

KB Kilobytes.

latency A measure of delay, often network delay. Depending on the type of element, *e*Health reports can show two types of latency: round-trip latency, which is the length of time in milliseconds for a ping packet to travel from the *e*Health system to a polled element and back. Alternate latency, which is the length of time in milliseconds for a ping packet to travel from a network resource (the alternate latency source) such as a router to other critical network resources such as routers and servers (the alternate latency partner).

management information base (MIB) A formal description of a set of network objects that can be managed using Simple Network Management Protocol (SNMP).

MB Megabytes.

MIB *See* management information base (MIB).

network A collection of computers, printers, routers, switches, and other devices that are able to communicate using a common transmission media such as TCP/IP.

network management system (NMS) An application program usually residing on a computer that manages at least part of a network, including systems and applications. The NMS communicates with agents to monitor network statistics and resources, control network device configuration, and analyze network problems. *See also* agent.

NMS *See* network management system (NMS).

object identifier (OID) a unique identifier of a managed object in a MIB hierarchy. *See also* management information base (MIB).

OID *See* object identifier (OID).

operating system (OS) The program that manages all other programs (applications or application programs) on a computer. Provides the following services: determining the order in which each application runs and the time allotted for that application, managing the sharing of internal memory among multiple applications and handling input to and output from attached hardware devices.

OS *See* operating system (OS).

packet A logical unit of data routed between an origin and a destination on the Internet or any other packet-switched network. On the Internet, the Transmission Control Protocol (TCP) layer of TCP/IP divides a file into packets of manageable size for routing.

page In computers that utilize virtual memory, a unit of data storage. Systems transfer pages of data from disk storage to memory and back again.

On the World Wide Web, a file written using Hypertext Markup Language (HTML) that specifies how text, images, and other multimedia will be presented to the user. A Web site delivers information to the user one page at a time.

paging The process by which a computer moves portions of programs between random access memory and auxiliary storage (on disk).

partition A logical division of a hard disk on a PC that is created so that each partition can have a different operating system or can be used for different purposes (for example, file management or multiple users).

path In networking, a path is a route from one location to another in a network. In an Asynchronous Transfer Mode (ATM) network, a path is a virtual pipe that can carry a number of channels.

PC *See* personal computer (PC).

performance threshold The upper limit of acceptable response time.

personal computer (PC) A computer designed for individual use. Prior to the PC, computers were designed to be used by many individuals and system resources were shared by all. A PC often refers to a computer with an Intel microprocessor architecture and an operating system such as Microsoft DOS or Windows.

ping An Internet echo message used to confirm the reachability of a network device. An abbreviation for Packet Internet or Inter-Network Groper.

port The physical (hardware) connection on a device that connects the device to a network.

process Typically, an instance of a program or application that is running on a server. Applications can have one or more associated processes. *See also* Database Management System (DBMS).

process set A collection of one or more processes that relate to a specific application. Using *e*Health – System At-a-Glance reports, you can obtain information about the impact and performance of process sets running on systems that have Concord SystemEDGE agents.

protocol The set of rules by which the endpoints in a telecommunication connection communicate. The protocol defines the packet format of the transmitted information. On the Internet, common protocols are TCP, IP, HTTP and FTP.

queue In a system, a set of jobs awaiting resources. In a network device such as a router, a collection of packets waiting to be processed or forwarded. Insufficient central processing unit (CPU) speed, memory, or interface speeds can contribute to long queues, and therefore, to delay on the network.

real-time A level of computer responsiveness that an end user would deem as immediate or fast enough to show incremental changes of an external process (for example, to present visualizations of the weather as it constantly changes).

Request For Comments (RFC) The name of the document series regarding Internet design. Most RFCs define protocol specifications such as Telnet and FTP. RFCs are widely available online.

RFC *See* Request For Comments (RFC).

server A program that provides services to other programs in the same and other computers.

Also a computer that performs file storage and application hosting as well as provides computing services to other devices and users on the network. Typically has one or more central processing units (CPUs), disks, interfaces, and storage partitions.

server process A server-side part of a distributed application.

Simple Network Management Protocol (SNMP) The network management protocol used almost exclusively in data networks. A method for monitoring and controlling network devices, as well as managing configurations, statistics collection, performance, and security.

SNMP *See* Simple Network Management Protocol (SNMP).

SNMP agent A program such as the SystemEDGE agent that conforms to a management information base (MIB) specification to collect information about managed devices and to take corrective action (using SNMP traps) when appropriate.

speed The capacity (bandwidth) of an interface in bits per second (bps).

swapping The process in which a computer moves entire programs in and out of random access memory to and from auxiliary storage (swap partition or pagefile).

SystemEDGE agent Concord's SNMP agent that autonomously monitors system configuration, status, performance, users, applications, file systems, and other critical resources.

Systems Management MIB A set of MIB (management information base) objects that extends the capabilities of the Host Resources MIB. It provides greater visibility into systems and specific information about Windows NT and UNIX systems.

TCP/IP *See* Transmission Control Protocol (TCP) and "Internet Protocol (IP).

threshold *See* performance threshold.

throughput The rate of data transfer on an interface over time. At each poll, *e*Health calculates throughput by dividing the total number of bits for an interface by the elapsed time in seconds since the previous poll.

traffic The data that travels over a network.

Transmission Control Protocol (TCP) A connection-based protocol used along with the Internet Protocol (IP) to send data in the form of message units between computers over the Internet. While IP is responsible for the actual delivery of the data, TCP is responsible for dividing data into packets at the sending system and constructing the data message from individual packets at the receiving system.

trap A message sent by an SNMP agent to a console or network management system (NMS) to indicate that a threshold has been reached or another user-defined condition has occurred. The SystemEDGE agent defines a number of traps for system and application management.

UDP *See* User Datagram Protocol (UDP).

User Datagram Protocol (UDP) A communications protocol that uses Internet Protocol (IP) to send and receive data and is similar to Transmission Control Protocol (TCP), but provides fewer packet management services.

variable A performance metric for an element. A characteristic or behavior upon which *e*Health gathers data and evaluates the performance of the element. SystemEDGE agents can also monitor local variables to reduce network polls and increase scalability.

Web *See* World Wide Web (WWW, Web).

workstation A powerful computer that is equipped with a fast processor, a large amount of random access memory, and other features such as high-speed graphical rendering that make it suitable for business users such as engineers, graphic designers, and architects.

World Wide Web (WWW, Web) All of the resources on the Internet that use Hypertext Transfer Protocol (HTTP). Users of the Web access information through browser software.

Index

F

G

H

I

L

M

O

Manual 32

ADVANTEDGE FOR MICROSOFT IIS User Guide

ADVANTEDGE™

FOR MICROSOFT® IIS

User Guide

Release 1.0 Patchlevel 2
or Later

09-16040-003
April 2001

Important Notice

Application Health, System Health, Live Health, SystemEDGE, AdvantEDGE, *e*Health, Infrasense, MIB Manager, State-of-the-World, and the FirstSense logo are trademarks of Concord Communications, Inc.

The Total View, Concord, the Concord logo, Empire Technologies, Network Health, TRAKKER, FirstSense, and We See It Happening are registered trademarks of Concord Communications, Inc.

Adobe, Acrobat, and the Acrobat logo are trademarks, which may be registered in certain jurisdictions, and PostScript is a registered trademark of Adobe Systems Incorporated.
Intel is a registered trademark of Intel Corporation.
Windows, Windows NT, Windows 2000, Internet Information Server, and Internet Information Services are trademarks of Microsoft Corporation.

General Notice: Some of the product names used herein have been used for identification purposes only and may be trademarks of their respective companies.

Proprietary Notice

The information and descriptions contained herein are the property of Concord Communications, Inc. Such information and descriptions may not be copied, disseminated, or distributed without the express written consent of Concord Communications, Inc. Concord Communications, Inc., assumes no responsibility for any inaccuracies that may appear in this document. Concord Communications, Inc., reserves the right to improve its products and change specifications at any time without notice.

U. S. Government Restricted Rights

Use, reproduction, and disclosure by the U.S. Government are subject to the restrictions set forth in FAR §52.227-19 (c) (1) and (2) and DFARS §252.227-7013 (c) (1) (ii).

Patent Information

U. S. Patent 5,615,323
Patents Pending

Table of Contents

About This Guide

Chapter 1
Introduction

Chapter 2
Installing AdvantEDGE for Microsoft IIS

Chapter 3
Using the AdvantEDGE for Microsoft IIS MIB

Chapter 4
Using AdvantEDGE for Microsoft IIS

Index

About This Guide

The *AdvantEDGE for Microsoft IIS User Guide* provides instructions for installing and using AdvantEDGE for Microsoft IIS for Windows NT x86 and Windows 2000 systems. This guide is intended for the person responsible for installing and configuring AdvantEDGE for Microsoft IIS.

This version supports AdvantEDGE for Microsoft IIS Release 1.0 Patchlevel 2 or later, and the SystemEDGE agent Release 4.0, Patchlevel 3 and later.

NOTE

The acronym IIS stands for Internet Information Server in version 4.0 for Windows NT, and for Internet Information Services in version 5.0 for Windows 2000.

To use AdvantEDGE for Microsoft IIS, you should have a basic understanding of the Microsoft IIS application, the Concord SystemEDGE agent, and your host's operating systems environment. Refer to Microsoft documentation and the *SystemEDGE Agent User Guide* for more information.

How This Guide Is Organized

This guide is organized as follows:

- Chapter 1, "Introduction," provides an overview of AdvantEDGE for Microsoft IIS and its capabilities for monitoring Microsoft IIS.
- Chapter 2, "Installing AdvantEDGE for Microsoft IIS," explains how to install, configure, and license the Concord AdvantEDGE for Microsoft IIS software on a host system.
- Chapter 3, "Using the AdvantEDGE for Microsoft IIS MIB," describes the information that is available through the Concord AdvantEDGE for Microsoft IIS MIB.
- Chapter 4, "Using AdvantEDGE for Microsoft IIS," explains how to configure and use Concord's AdvantEDGE for Microsoft IIS in your host environment.

Conventions in This Guide

The following paragraph shows a sample command. Due to space limitations in this guide, some commands wrap from one line to the next. Disregard these line breaks, and **enter each command as one line**. Otherwise, your command syntax will be incorrect.

For example, when you see a command such as the following:

```
watch process procAlive 'inetinfo|INETINFO' 5000 0x0
  30 'IIS' ''
```

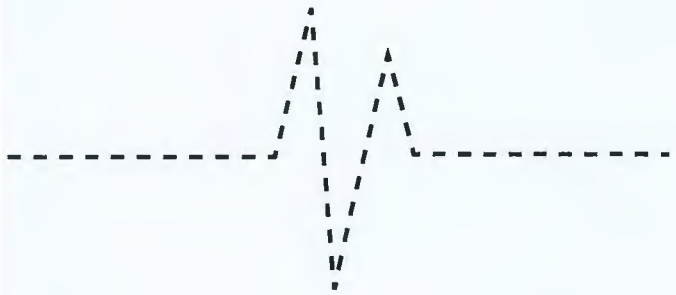
You **must** enter the command on one line, as shown here:

```
watch process procAlive 'inetinfo|INETINFO' 5000 0x0 30 'IIS' ''
```

Contact Information

If you need any assistance with the SystemEDGE agent or the AdvantEDGE for Microsoft IIS Point module, contact Customer Support, using one of the following methods:

Phone:	(888) 832-4340 (for calls from the USA and Canada) (508) 303-4300 (for calls from other countries)
Fax:	(508) 303-4343
E-mail:	support@concord.com
Web site:	http://www.concord.com
Licensing:	http://license.concord.com



1 Introduction

This chapter provides an overview of how you can use the AdvantEDGE for Microsoft IIS Point module to monitor the Microsoft IIS application. You must install this Point module on every IIS workstation that you want to monitor.

NOTE

Unless otherwise stated, the term *IIS*, as used throughout this guide and the Management Information Base (MIB) specification, refers to the Microsoft IIS application in its entirety, which encompasses all of the services and optional components.

Introducing AdvantEDGE for Microsoft IIS

AdvantEDGE for Microsoft IIS is a plug-in module for the SystemEDGE agent. This plug-in enables information technology (IT) operators to monitor the performance and availability of Microsoft IIS on Microsoft Windows NT 4.0 and Windows 2000. Microsoft IIS is a super server that consists of several services, which are described in the next section, "Microsoft IIS Architecture".

AdvantEDGE for Microsoft IIS makes important information about IIS available to management software through the SystemEDGE agent and Simple Network Management Protocol (SNMP). The SystemEDGE agent enables the monitoring of important IIS metrics, processes, and services, as well as the sending of SNMP traps when exceptions or exception conditions occur.

NOTE

This document is not intended as a manual on how to install, administer, or use Microsoft IIS. For help with IIS, refer to your Microsoft documentation.

Microsoft IIS Architecture

Microsoft IIS is a complex piece of software with many components. At the core of IIS are the following services:

- World Wide Web (WWW) service, which services the Web content to and from users
- File Transfer Protocol (FTP) service, which services file transfer requests to and from users
- Simple Mail Transfer Protocol (SMTP) service, which provides a mail transport mechanism for IIS
- Network News Transfer Protocol (NNTP) service, which provides news groups for IIS

Figure 1-1 shows the core components of AdvantEDGE for Microsoft IIS.

Figure 1-1: AdvantEDGE for Microsoft IIS Components

IIS controls worker threads, and it can use each worker thread to provide a specific service that the user has requested. This architecture requires the monitoring of the IIS process and other processes in order to obtain sufficient information on the performance of IIS. Because IIS includes so many components, its proper functioning requires the availability of a variety of processes; configuration parameters and settings; and Windows NT services, queues, and system resources.

Using AdvantEDGE for Microsoft IIS

AdvantEDGE for Microsoft IIS provides you with the tools and information that you need to monitor and respond to the IIS application and its use of your system resources. With AdvantEDGE for Microsoft IIS, you can fix potential problems before users—and your business—are affected.

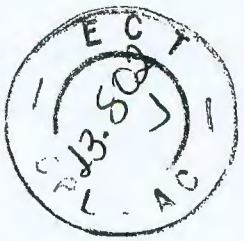
You can use AdvantEDGE for Microsoft IIS with any SNMP-compliant management software, including Concord's *e*Health suite of products, AdvantEDGE View, HP OpenView, and others. With AdvantEDGE for Microsoft IIS and the SystemEDGE agent, you can perform the following types of tasks:

- Monitor the availability of IIS and its various services.
- Automatically restart any service that fails.
- Alert IT staff when IIS starts to consume significant levels of system resources, including CPU, disk space, and memory.
- Monitor logs for security, system, and application events across the Web, FTP, SMTP, and NNTP services.
- Detect error statistics across the Active Server Pages (ASP), Common Gateway Interface (CGI), and Internet Server Application Program Interface (ISAPI) application extension pages, including Web 404 (page not found) errors and ASP script errors.

Using AdvantEDGE for Microsoft IIS with *e*Health

You can use AdvantEDGE for Microsoft IIS and the SystemEDGE agent with the *e*Health product suite to provide the historical data for long-term trending analysis and capacity planning. With *e*Health – Application Assessment, you can run At-a-Glance, Trend, Top N, and MyHealth reports for the following types of information:

- Amount of Central Processing Unit (CPU), total memory, and disk space the IIS application is using
- Size of the IIS service logs
- Number of times the IIS application is using the database cache to redisplay information
- Number of bytes and number of files processed by the WWW and FTP services
- Number of users for the WWW and FTP services



- Number of WWW requests the IIS application is processing per second
- Number of page not found errors the WWW service is encountering

For more information about the variables that you can monitor and reports that you can run when you integrate AdvantEDGE for Microsoft IIS with *e*Health, refer to the *e*Health Web Help.

Using AdvantEDGE for Microsoft IIS with Live Health

You can also use AdvantEDGE for Microsoft IIS and the SystemEDGE agent with Live Health for real-time detection of potential problems. Live Health applies intelligent algorithms to the data, resulting in precise assessments of application health and performance. For more information about how Live Health can detect "brownouts" and service delays across applications, systems, and networks, refer to the Live Health Web Help.

2

Installing AdvantEDGE for Microsoft IIS

This chapter explains how to install, configure, and license AdvantEDGE for Microsoft IIS.

NOTE

For the most current information about installing the AdvantEDGE for Microsoft IIS module, refer to the release notes (relnotes.txt) that ship on the installation CD.

Installation Requirements

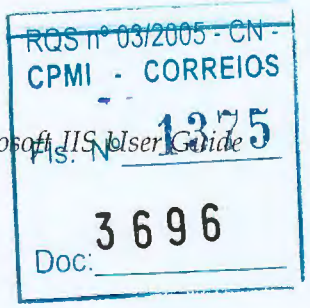
Before you install AdvantEDGE for Microsoft IIS, you must first install, license, and configure the SystemEDGE agent Release 4.0, Patchlevel 3 or later. For more information, refer to the *SystemEDGE Agent User Guide*.

Your system must also be running the Microsoft IIS application. Use Table 2-1 to determine which version of IIS and which service packs are required for your operating system.

Table 2-1: Required IIS Version and Service Pack by Operating System

Operating System	Required Software	Required Service Pack
Windows NT 4.0 x86	Microsoft Internet Information Server Version 4.0	6a
Windows 2000	Microsoft Internet Information Services Version 5.0	1

For more information, refer to Microsoft documentation.



Installing the Software

AdvantEDGE for Microsoft IIS is distributed as a self-extracting executable named **iismod.exe** for Windows NT and Windows 2000.

Follow these steps to install AdvantEDGE for Microsoft IIS:

1. Locate the IIS workstation that needs to be monitored.
2. Log on to the system as administrator.
3. Click **Start**.
4. Select **Programs** → **Command Prompt**.
5. Insert the CD containing the Concord software distributions into the CD-ROM drive.

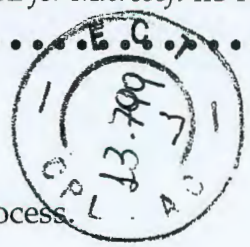
   The operating system automatically mounts the drive using the CD-ROM drive's corresponding drive letter. The particular drive letter is specific to your system and depends on the number and types of disks attached to your system.
6. Determine which directory you want to use as the installation directory for AdvantEDGE for Microsoft IIS. If the SystemEDGE agent is installed at C:\sysedge, the recommended installation directory is C:\sysedge\plugins.
7. Run the self-extracting executable by entering the following at the command prompt, where *D:* is the CD-ROM drive for your system, and *C:\sysedge\plugins* is the installation directory:

   ```
   D:\iismod\ntx86\iismod.exe -dir C:\sysedge\plugins
   ```

   The -dir option is important because it instructs the self-extracting executable to create the intended subdirectory hierarchy that is used throughout this guide. The distribution is then placed in an iismod subdirectory within the specified target directory (for example, C:\sysedge\plugins\iismod).

NOTE
You cannot execute iismod.exe directly from the CD-ROM.

AdvantEDGE for Microsoft IIS is now installed.



AdvantEDGE for Microsoft IIS Files

Table 2-2 describes the files created by the installation process.

Table 2-2: Files Installed by AdvantEDGE for Microsoft IIS

File Name	Description
iismod.dll	AdvantEDGE for Microsoft IIS dynamic link library (DLL) module for Windows NT and Windows 2000
iismod.pdf	*AdvantEDGE for Microsoft IIS User Guide*
iismod.asn1	AdvantEDGE for Microsoft IIS MIB specification
examples	AdvantEDGE for Microsoft IIS monitoring examples
relnotes.txt	Release notes for AdvantEDGE for Microsoft IIS

Configuring AdvantEDGE for Microsoft IIS

The SystemEDGE agent uses the configuration file sysedge.cf and the *sysedge_plugin* keyword to specify which AdvantEDGE modules to load at system initialization. By default, the SystemEDGE agent does not load any plug-ins at initialization time, but you can edit the sysedge.cf file to configure the agent to load any AdvantEDGE Point modules that you have installed.

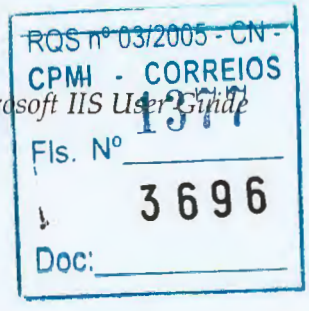
The sysedge.cf file is located, by default, in your system directory; for example, C:\winnt\system32. To configure the SystemEDGE agent to start AdvantEDGE for Microsoft IIS, you must provide the complete path name to iismod.dll, the AdvantEDGE for Microsoft IIS dynamic link library. The actual path depends on the location you selected when you installed the AdvantEDGE for Microsoft IIS files. For example, enter this command if you installed the files in the C:\sysedge\plugins\iismod directory:

```
sysedge plugin C:\sysedge\plugins\iismod\iismod.dll
```

For more information about the sysedge.cf file, refer to the *SystemEDGE Agent User Guide*.

Licensing AdvantEDGE for Microsoft IIS

Like the SystemEDGE agent, AdvantEDGE for Microsoft IIS utilizes a host-based license method. Copies of AdvantEDGE for Microsoft IIS can run only on systems that possess a valid license key. This license is separate from the one used for the SystemEDGE agent.



The first time that you attempt to start the SystemEDGE agent after installing AdvantEDGE for Microsoft IIS, the agent will display a message saying that a valid license was not found for AdvantEDGE for Microsoft IIS. It then provides you with a *public key* that is used to generate a permanent license key for your host machine.

A license key is made up of four space-separated, 8-character sequences, totaling 32 characters. The AdvantEDGE for Microsoft IIS license is stored in the sysedge.lic file, the same file that contains the SystemEDGE agent licenses. Refer to the sample license file on page 2-6.

Obtaining a License

To obtain a license, you can do any of the following:

- Run the Concord-supplied licenseutil.pl script.
- Run the licenseme.exe license utility.
- Use the AdvantEDGE View licensing procedure, which uses SNMP traps. For more information, refer to the AdvantEDGE View Web Help.
- Send an e-mail request to license@concord.com and place the returned license key in the appropriate license file.

NOTE

Always include the Customer ID and user name in license requests that you send through e-mail.

- Complete the online license form through the Internet, as described in the next section, "Generating the License"."

For more information about licensing, refer to the *SystemEDGE Agent User Guide* and the *Automating the Licensing of SystemEDGE and AdvantEDGE Point Plug-in Modules* white paper.

Generating the License

This section describes how to generate the license using the Web-based license form. The SystemEDGE setup program can generate the licensing information for your system.

NOTE

If you are using an evaluation copy of AdvantEDGE for Microsoft IIS, you must request a temporary license that will enable it to operate during the evaluation period.

To generate a license, follow these steps:

1. Run the SystemEDGE agent setup command by entering the following at the command prompt:

   ```
   sysedge\setup -l
   ```

   The setup program displays a message similar to the following:

```
SystemEDGE Version 4.0 Patchlevel 3
Copyright 2001 by Concord Communications, Inc.
Please contact Concord Communications, Inc. to obtain a license
http://www.concord.com/support, Email: license@concord.com
Provide: sysedge neptune NTx86 4.0 346561363366b19c 4.0 Patchlevel 3
```

2. To obtain a license for AdvantEDGE for Microsoft IIS, fill out the online Web-based license form available from Concord's licensing Web server at the following URL:

   ```
   http://license.concord.com
   ```

   NOTE

   You must supply a user name and password to access the license form.

   The license form asks you to supply the following information:

   - Customer ID
   - Name
   - E-mail address
   - Software version number (4.0 in the example above)
   - Patchlevel
   - System name (neptune in the example above)
   - Operating system name (NTx86 in the example above)
   - Operating system version (4.0 in the example above)
   - System identifier (346561363366b19c in the example above)

NOTE

When you are licensing AdvantEDGE for Microsoft IIS, select **iismod** as the product on the licensing form.

After you submit the license request, the Concord Web server generates a license and displays it to your Web browser. It also e-mails the license to the contact person in your organization.

3. Copy the generated license key into the sysedge.lic file in the system32 subdirectory (for example, C:\winnt\system32), and then save the file.

   The license key is case sensitive. Copy it exactly as it appears. If possible, use your system's cut-and-paste facility instead of entering it by hand. If you do enter the license key by hand, be careful not to confuse characters such as the letters l and **I** and the number **1**,or the letter **O** and the number **0**.

4. Stop and then restart the Windows NT Master agent by entering the following commands at the command prompt:

   ```
   net stop snmp
   net start snmp
   ```

The AdvantEDGE for Microsoft IIS module is now licensed and ready to use.

Sample License File

The following is a sample SystemEDGE agent license file. A pound character (#) in column 1 indicates that the entire line is a comment.

```
# license file for SystemEDGE Agent
# Empire Technologies, Inc.
# A Concord Communications Company
# http://www.concord.com
#
# file /etc/sysedge.lic or %SystemRoot%\system32\sysedge.lic
# A valid license key has four parts of 8 characters per part
# parts are separated by space(s) with one license key per line
# sysedge neptune NT/x86 4.0 807cb1da007cb1da 4.0
e13311d3 0F2a7cb1 abC512dc fF8C923a

# iismod neptune NT/x86 4.0 807cb1da007cb1da 1.0
a7943fde 098a87ij a4kiuf39 afafEkj4
```


3

Using the AdvantEDGE for Microsoft IIS MIB

This chapter explains the organization and content of the Concord Communications MIB for Microsoft IIS. This MIB specification (iismod.asn1) defines a collection of objects for monitoring and managing IIS. You must configure the SystemEDGE agent to monitor the AdvantEDGE for Microsoft IIS MIB objects that are relevant for your configuration. For more information about configuring the SystemEDGE agent to monitor the IIS application, refer to Chapter 4, "Using AdvantEDGE for Microsoft IIS."

Figure 3-1 shows the organization of the AdvantEDGE for Microsoft IIS MIB.

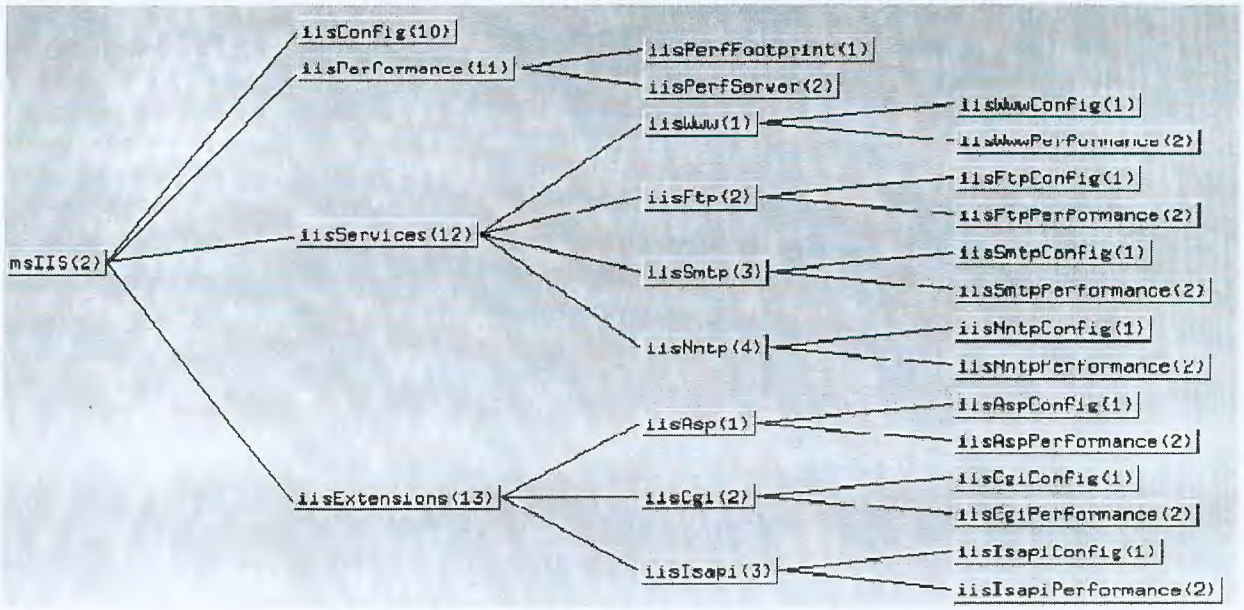


Figure 3-1: AdvantEDGE for Microsoft IIS MIB

The MIB is organized into broad sections for server, services, and extension information. Within those broad sections are subsections for configuration and performance. Within the performance section, a footprint section defines MIB objects that convey how much of the underlying system's resources are consumed by IIS.

The following sections highlight important MIB objects from the IIS MIB. This chapter defines all sections of the IIS MIB, but it does **not** define all of the MIB objects. For a complete list of MIB objects, refer to the AdvantEDGE for Microsoft IIS MIB specification (iismod.asn1).

Configuration Section

The Configuration section of the AdvantEDGE for Microsoft IIS MIB contains configuration parameters and settings that are important for streamlining the health and performance of IIS. It also includes information about server configuration.

Server Configuration

The Server Configuration group contains configuration parameters, process IDs, and version numbers. Table 3-1 defines important Server Configuration parameters.

Table 3-1: Selected MIB Objects – IIS Server Configuration Group

MIB Object	Description
iisVersion	IIS version.
iisPid	IIS process ID.
iisObjectCacheTTL	How often the cache scavenger runs.
iisMAXPoolThreads	How many threads IIS will use to perform tasks.
iisListenBackLog	Maximum number of connection requests in the queue for each service.
iisOpenFilesInCache	Number of files IIS will keep open in the cache.

Figure 3-2 shows a sample AdvantEDGE View process-status window for IIS.

Process	Status	PID	Start–Time
IIS	Up	278	Wed Jul 12 19:09:02 2000

Figure 3-2: Sample IIS Process ID and Status

Performance Section

The Performance section of the AdvantEDGE for Microsoft IIS MIB contains performance data that is necessary for capacity planning and trend analysis, as well as for real-time performance and availability monitoring. The Performance group is divided into subgroups for footprint data and server performance.

IIS Footprint

This group provides information about IIS CPU, memory, and disk resource consumption, more commonly called its *footprint*. Long-term trending analysis of footprint information is useful for anticipating and avoiding problems due to resource exhaustion. You can also monitor footprint information in real time to detect and correct temporary resource exhaustion due to viruses, security incidents, and hardware failures. Table 3-2 defines important IIS Footprint metrics.

Table 3-2: Selected MIB Objects – IIS Footprint Group

MIB Object	Description
iisCPUTime	IIS total accumulated CPU time.
iisPercentCPU	Percentage of CPU, over the last interval, used by IIS.
iisTotalRSS	Total real memory currently in use by IIS.
iisPercentMEM	Percentage of real memory currently in use by IIS.
iisTotalLogSize	Estimate of the current disk space used by all IIS services.
iisTotalDiskSize	Estimate of the current total disk space used by IIS.
iisTotalThreads	Total number of system threads [illegible] IIS.

The following figures show sample AdvantEDGE View footprints for an IIS machine serving a medium-sized company. They represent real data collected from live IIS servers and displayed in AdvantEDGE View reports.

Figure 3-3 shows an example of disk usage by service:

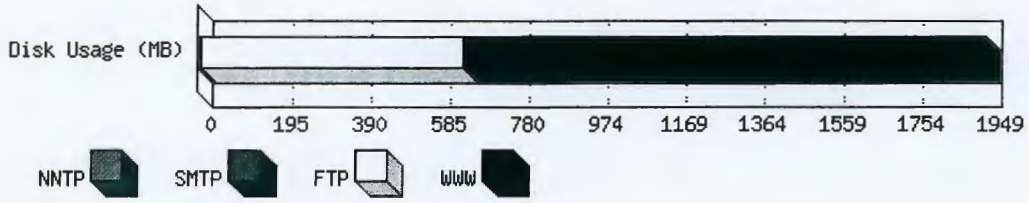


Figure 3-3: IIS Disk Usage by Service

Figure 3-4 shows an example of memory usage:

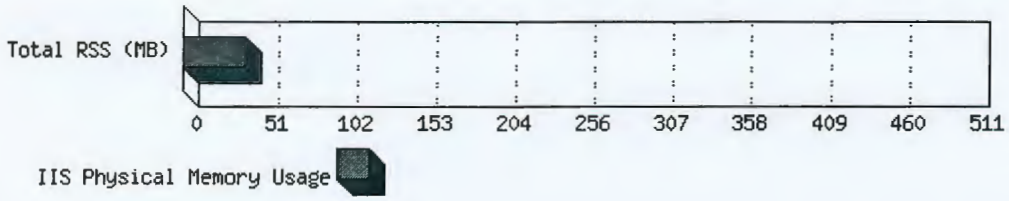


Figure 3-4: IIS Memory Usage

Figure 3-5 shows a sample IIS footprint summary:

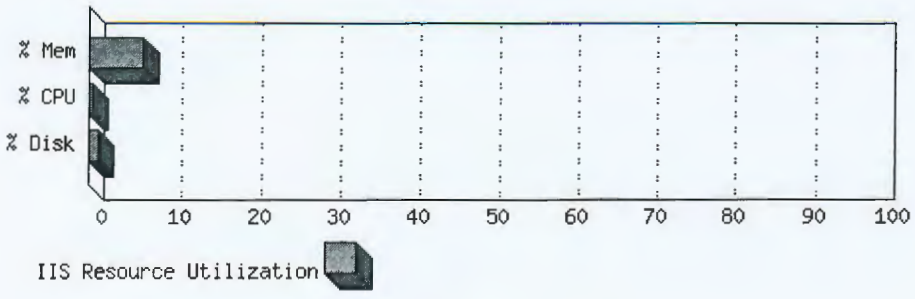


Figure 3-5: IIS Footprint Summary

Server Performance

The Server Performance group provides performance metrics and counters for IIS, including user statistics and transfer statistics. These metrics include those useful for real-time management and longer-term capacity planning and trend analysis. Table 3-3 defines important Server Performance metrics.

Table 3-3: Selected MIB Objects – IIS Server Performance Group (Page 1 of 2)

MIB Object	Description
iisCacheHits	Total number of times an item was found by IIS in the object cache.
iisCacheMisses	Total number of times an item was not found by IIS in the object cache.
iisCacheFlushes	Number of times an item was deleted from the IIS object cache.
iisTtlCurAnonUsr	Total number of current anonymous users maintained by all IIS services.
iisTtlCurNAnonUsr	Total number of current non-anonymous users maintained by all IIS services.
iisTtlCurUsr	Total number of users maintained by all IIS services.
iisTtlMaxAnonUsr	Total maximum number of anonymous users maintained by all IIS services.
iisTtlMaxNAnonUsr	Total maximum number of non-anonymous users maintained by all IIS services.
iisTtlMaxUsr	Total maximum number of users maintained by all IIS services.
iisTtlAnonUsr	Running count of anonymous users maintained by all IIS services.
iisTtlNAnonUsr	Running count of non-anonymous users maintained by all IIS services.
iisTtlUsr	Running count of all users maintained by all IIS services.
iisTtlBytesSent	Count of KB sent by all IIS services.
iisTtlBytesRecv	Count of KB received by all IIS services.
iisTtlBytes	Count of KB transferred by all IIS services.
iisTtlFilesSent	Count of files sent by all IIS services.

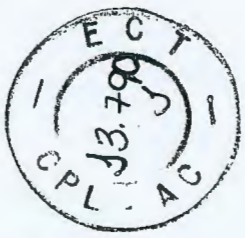


Table 3-3: Selected MIB Objects – IIS Server Performance Group (Page 2 of 2)

MIB Object	Description
iisTtlFilesRecv	Count of files received by all IIS services.
iisTtlFiles	Count of files transferred by all IIS services.
iisWebAppReqTtl	Total number of Web requests made by IIS.

Figure 3-6 shows a sample user statistics summary:

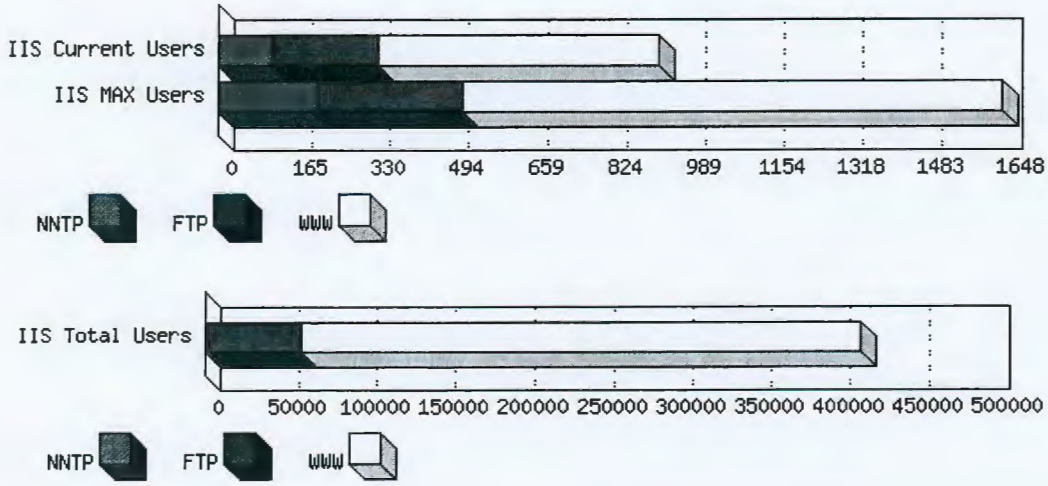


Figure 3-6: IIS User Statistics Summary

Services Group

The Services group provides configuration information, performance metrics, and counters for IIS services, including WWW, FTP, SMTP, and NNTP. These metrics include those useful for real-time management and longer-term capacity planning and trend analysis.

WWW Group

The World Wide Web (WWW) group provides configuration information, performance metrics, and counters for the IIS WWW Service. It looks at the WWW Service as a whole and provides totals of all WWW service activities in IIS.

WWW Configuration Group

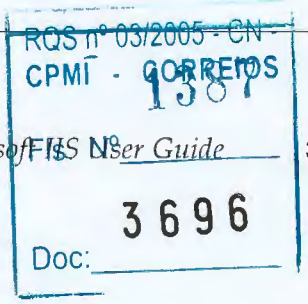
The WWW Configuration group provides version information for the IIS WWW service.

WWW Performance Group

The WWW Performance group provides performance metrics and counters for the IIS WWW service, including user statistics and transfer statistics. These metrics include those useful for real-time management and longer-term capacity planning and trend analysis. Table 3-4 defines important WWW Performance metrics.

Table 3-4: Selected MIB Objects – IIS WWW Performance Group (Page 1 of 2)

MIB Object	Description
iisWwwLogSize	Estimate of the current disk space used by the WWW service logs.
iisWwwTtlDiskSize	Total size in KB of log and service directories.
iisWwwRezSysSize	Size in KB of the WWW service resident system code.
iisWwwTtlNotFoundErr	Total count of the page-not-found errors for the WWW service.
iisWwwTtlConnAtempt	Total number of connections to the well-known port of the WWW service.
iisWwwTtlLogonAtempt	Total number of logins that have been attempted to the WWW service.
iisWwwTtlCurAnonUsr	Total number of current anonymous users maintained by the WWW service.
iisWwwTtlCurNAnonUsr	Total number of current non-anonymous users maintained by the WWW service.
iisWwwTtlCurUsr	Total number of users maintained by the WWW service.
iisWwwTtlMaxAnonUsr	Maximum number of anonymous users maintained by the WWW service.
iisWwwTtlMaxNAnonUsr	Maximum number of non-anonymous users maintained by the WWW service.
iisWwwTtlMaxUsr	Maximum number of users maintained by the WWW service.



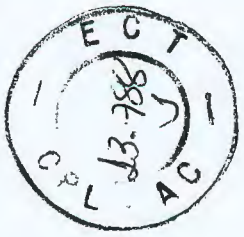


Table 3-4: Selected MIB Objects – IIS WWW Performance Group (Page 2 of 2)

MIB Object	Description
iisWwwTtlAnonUsr	Running count of anonymous users maintained by the WWW service.
iisWwwTtlNAnonUsr	Running count of non-anonymous users maintained by the WWW service.
iisWwwTtlUsr	Running count of all users maintained by the WWW service.
iisWwwTtlBytesSent	Count of KB sent by the WWW service.
iisWwwTtlBytesRecv	Count of KB received by the WWW service.
iisWwwTtlBytes	Count of KB transferred by the WWW service.
iisWwwTtlFilesSent	Count of files sent by the WWW service.
iisWwwTtlFilesRecv	Count of files received by the WWW service.
iisWwwTtlFiles	Count of files transferred by the WWW service.
iisWwwTtlGetReq	Total GET methods on the WWW service.
iisWwwTtlHeadReq	Total HEAD methods on the WWW service.
iisWwwTtlPostReq	Total POST methods on the WWW service.
iisWwwTtlPutReq	Total PUT methods on the WWW service.
iisWwwTtlTraceReq	Total TRACE methods on the WWW service.
iisWwwTtlDeleteReq	Total DELETE methods on the WWW service.
iisWwwTtlOtherReq	Total methods that are not using GET, POST, PUT, DELETE, TRACE, or HEAD.
iisWwwTtlMethodReq	Total methods that are using GET, POST, PUT, DELETE, TRACE, and HEAD.

FTP Group

The FTP group provides performance metrics and counters for the IIS FTP service. It includes information such as user statistics and transfer statistics. This group looks at the FTP Service as a whole and provides totals of all FTP service activities in IIS.

FTP Configuration Group

The FTP Configuration group provides version information for the IIS FTP service.

FTP Performance Group

The FTP Performance group provides performance metrics and counters for the IIS FTP service, including the total current users, total users, total files transferred, and total KB transferred. These metrics include those useful for real-time management and longer-term capacity planning and trend analysis. Table 3-5 defines important FTP Performance metrics.

Table 3-5: Selected MIB Objects – IIS FTP Performance Group (Page 1 of 2)

MIB Object	Description
iisFtpLogSize	Estimate of the current disk space used by the FTP service logs.
iisFtpTtlDiskSize	Total size in KB of log and service directories.
iisFtpTtlConnAtempt	Total number of connections to the well-known port of the FTP service.
iisFtpTtlLogonAtempt	Total number of logins that have been attempted to the FTP service.
iisFtpTtlCurAnonUsr	Total number of current anonymous users maintained by the FTP service.
iisFtpTtlCurNAnonUsr	Total number of current non-anonymous users maintained by the FTP service.
iisFtpTtlCurUsr	Total number of users maintained by the FTP service.
iisFtpTtlMaxAnonUsr	Maximum number of anonymous users maintained by the FTP service.
iisFtpTtlMaxNAnonUsr	Maximum number of non-anonymous users maintained by the FTP service.
iisFtpTtlMaxUsr	Maximum number of users maintained by the FTP service.
iisFtpTtlAnonUsr	Running count of anonymous users maintained by the FTP service.
iisFtpTtlNAnonUsr	Running count of non-anonymous users maintained by the FTP service.

Table 3-5: Selected MIB Objects – IIS FTP Performance Group (Page 2 of 2)

MIB Object	Description
iisFtpTtlUsr	Running count of all users maintained by the FTP service.
iisFtpTtlBytesSent	Count of KB sent by the FTP service.
iisFtpTtlBytesRecv	Count of KB received by the FTP service.
iisFtpTtlBytes	Count of KB transferred by the FTP service.
iisFtpTtlFilesSent	Count of files sent by the FTP service.
iisFtpTtlFilesRecv	Count of files received by the FTP service.
iisFtpTtlFiles	Count of files transferred by the FTP service.

SMTP Group

The SMTP group provides configuration information, performance metrics, and counters for the IIS SMTP Service. This group contains information such as transfer statistics and queue lengths. It looks at the SMTP service as a whole and provides totals of all SMTP service activities in IIS.

SMTP Configuration Group

The SMTP Configuration group provides version information for the IIS SMTP service.

SMTP Performance Group

The SMTP Performance group provides performance metrics and counters for the IIS SMTP service, including total messages transferred, total KB transferred, and various queue lengths. These metrics include those useful for real-time management and longer-term capacity planning and trend analysis. Table 3-6 defines important SMTP Performance metrics.

Table 3-6: Selected MIB Objects – IIS SMTP Performance Group

MIB Object	Description
iisSmtpLogSize	Estimate of the current disk space used by the SMTP service logs.
iisSmtpTtlDiskSize	Total size in KB of log and service directories.
iisSmtpTtlConErr	Total connection errors for the SMTP service.

Table 3-6: Selected MIB Objects – IIS SMTP Performance Group

MIB Object	Description
iisSmtpTtlBytesSent	Count of KB sent by the SMTP service.
iisSmtpTtlBytesRecv	Count of KB received by the SMTP service.
iisSmtpTtlBytes	Count of KB transferred by the SMTP service.
iisSmtpTtlMsgSent	Count of messages sent by the SMTP service.
iisSmtpTtlMsgRecv	Count of messages received by the SMTP service.
iisSmtpTtlMsg	Count of messages transferred by the SMTP service.
iisSmtpCurInConn	Number of connections that are currently inbound.
iisSmtpCurOutConn	Number of connections that are currently outbound.
iisSmtpTtlInConn	Total number of inbound connections received.
iisSmtpTtlOutConn	Total number of outbound connections attempted.
iisSmtpLocQueLen	Number of messages in the local queue.
iisSmtpRtryQueLen	Number of messages in the local retry queue.
iisSmtpRemtQueLen	Number of messages in the remote queue.
iisSmtpRemtRtryQueLen	Number of messages in the remote retry queue for remote delivery.
iisSmtpPicupQueLen	Number of messages in the directory pickup queue.

NNTP Group

The NNTP group provides configuration information, performance metrics, and counters for the IIS NNTP service. This group contains information such as transfer statistics and article statistics. It looks at the NNTP service as a whole and provides totals of all NNTP service activities in IIS.

NNTP Configuration Group

The NNTP Configuration group provides version information for the IIS NNTP service.

NNTP Performance Group

The NNTP Performance group provides performance metrics and counters for the IIS NNTP service, including total current users, total users, total KB transferred, and total articles transferred. Table 3-7 defines important NNTP Performance metrics.

Table 3-7: Selected MIB Objects – IIS NNTP Performance Group (Page 1 of 2)

MIB Object	Description
iisNntpLogSize	Estimate of the current disk space used by the NNTP service logs.
iisNntpTtlDiskSize	Total size in KB of log and service directories.
iisNntpTtlLogonAtempt	Total number of logins that have been attempted to the NNTP service.
iisNntpTtlCurAnonUsr	Total number of current anonymous users maintained by the NNTP service.
iisNntpTtlCurNAnonUsr	Total number of current non-anonymous users maintained by the NNTP service.
iisNntpTtlCurUsr	Total number of users maintained by the NNTP service.
iisNntpTtlMaxAnonUsr	Maximum number of anonymous users maintained by the NNTP service.
iisNntpTtlMaxNAnonUsr	Maximum number of non-anonymous users maintained by the NNTP service.
iisNntpTtlMaxUsr	Maximum number of users maintained by the NNTP service.
iisNntpTtlAnonUsr	Running count of anonymous users maintained by the NNTP service.
iisNntpTtlNAnonUsr	Running count of non-anonymous users maintained by the NNTP service.
iisNntpTtlUsr	Running count of all users maintained by the NNTP service.
iisNntpTtlBytesSent	Count of KB sent by the NNTP service.
iisNntpTtlBytesRecv	Count of KB received by the NNTP service.
iisNntpTtlBytes	Count of KB transferred by the NNTP service.

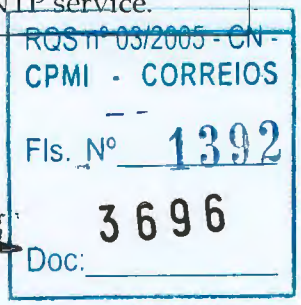


Table 3-7: Selected MIB Objects – IIS NNTP Performance Group (Page 2 of 2)

MIB Object	Description
iisNntpTtlArtclSent	Total articles sent for the NNTP service.
iisNntpTtlArtclRecv	Total articles received for the NNTP service.
iisNntpTtlArtcl	Total articles for the NNTP service.

Extensions Group

The Extensions group provides performance metrics and counters that extend IIS services. This group contains metrics for ASP, CGI, and ISAPI.

ASP Group

The ASP group contains ASP extension configuration and performance data. ASP is a server-side scripting environment used in Web-based applications. This group looks at ASP as a whole and provides totals of all ASP activities in IIS.

ASP Performance Group

The ASP Performance group provides performance metrics and counters for Active Server Pages, including total requests, total requests that succeeded, and total number of script errors. These metrics include those useful for real-time management and longer-term capacity planning and trend analysis. Table 3-8 defines important ASP Performance metrics.

Table 3-8: Selected MIB Objects – IIS ASP Performance Group (Page 1 of 2)

MIB Object	Description
iisAspMemAlcated	Total memory in KB that is currently allocated to ASP.
iisAspReqExecuting	Current number of ASP requests that are executing.
iisAspReqQued	Current number of ASP requests that are waiting for service from the queue.
iisAspReqDiscnt	Number of requests that were disconnected due to communications failure.
iisAspReqNAuth	Number of requests that failed due to insufficient access rights.

Table 3-8: Selected MIB Objects – IIS ASP Performance Group (Page 2 of 2)

MIB Object	Description
iisAspReqNFnd	Number of requests for files that were not found.
iisAspReqRej	Number of requests that were not executed because of insufficient processing resources.
iisAspReqWaitTime	Number of milliseconds that the most recent request waited in the queue.
iisAspReqExecTime	Total number of milliseconds to execute the most recent request.
iisAspReqSucceeded	Number of requests that executed successfully.
iisAspReqTtl	Total number of requests since the service was started.
iisAspSessCur	Number of sessions being serviced.
iisAspSessDur	Number of milliseconds that the most recent session persisted.
iisAspSessTmdOut	Number of sessions that timed out.
iisAspSessTtl	Number of sessions since the service was started.
iisAspTrnsPending	Number of transactions in progress.
iisAspTrnsCommitted	Number of transactions committed.
iisAspTrnsAbort	Number of transactions aborted.
iisAspTrnsTtl	Total number of transactions since the service started.
iisAspErrScrptRun	Number of requests that failed due to runtime errors.
iisAspErrScrptCmp	Number of requests that failed due to script-compilation errors.
iisAspErrScrptTtl	Total number of script errors, both runtime and compilation.

CGI Group

The CGI group contains CGI extension configuration and performance data. CGI is a server-side gateway interface used in Web-based applications. This group looks at CGI as a whole and provides totals of all CGI activities in IIS.

CGI Performance Group

The CGI Performance group provides performance metrics and counters for the Common Gateway Interface, including number of current requests, maximum number of requests, and total number of requests. These metrics include those useful for real-time management and longer-term capacity planning and trend analysis. Table 3-9 defines important CGI Performance metrics.

Table 3-9: Selected MIB Objects – IIS CGI Performance Group

MIB Object	Description
iisCgiReqCur	Number of current CGI requests.
iisCgiReqMax	Maximum number of simultaneous CGI requests.
iisCgiReqTtl	Total number of CGI requests since the service started.

ISAPI Group

The ISAPI group contains ISAPI extension configuration and performance data. ISAPI is a server-side program interface used in Web-based applications. This group looks at ISAPI as a whole and provides totals of all ISAPI activities in IIS.

ISAPI Performance Group

The ISAPI group provides performance metrics and counters for the ISAPI, including number of current requests, maximum number of requests, and total number of requests. These metrics include those useful for real-time management and longer-term capacity planning and trend analysis. Table 3-10 defines important ISAPI Performance metrics.

Table 3-10: Selected MIB Objects – IIS ISAPI Performance Group

MIB Object	Description
iisIsapiReqCur	Number of current ISAPI requests.
iisIsapiReqMax	Maximum number of simultaneous ISAPI requests.
iisIsapiReqTtl	Total number of ISAPI requests since service startup.

4

Using AdvantEDGE for Microsoft IIS

This chapter describes how to configure and use AdvantEDGE for Microsoft IIS. This Point module is implemented as a SystemEDGE agent plug-in. After you enable this plug-in in the sysedge.cf file and obtain a license for it, it will load automatically at SystemEDGE start time. For more information, refer to "Configuring AdvantEDGE for Microsoft IIS" on page 2-3 and "Licensing AdvantEDGE for Microsoft IIS" on page 2-3.

The AdvantEDGE for Microsoft IIS plug-in implements additional MIB objects that provide advanced information about the health and availability of IIS. AdvantEDGE for Microsoft IIS can operate with any SNMP-compliant management software, such as Concord's *e*Health suite of products, AdvantEDGE View, HP OpenView, and others. If you are using AdvantEDGE for Apache with *e*Health, refer to the *e*Health Web Help for more information about the reports that you can generate.

The default configuration settings of the AdvantEDGE for Microsoft IIS plug-in enable you to use the advanced self-monitoring capabilities of the SystemEDGE agent in conjunction with AdvantEDGE for Microsoft IIS.

Editing the SystemEDGE Configuration File

You can use AdvantEDGE View or another SNMP management tool to edit the SystemEDGE configuration file to utilize the MIB objects that exist in AdvantEDGE for Microsoft IIS with the process-monitoring, threshold-monitoring, Windows NT event-monitoring, and history-collection features of the SystemEDGE agent. All MIB objects related to AdvantEDGE for Microsoft IIS exist at object identifier (OID) branch 1.3.6.1.4.1.546.16.2 in the Concord Systems Management MIB. The MIB is defined in the iismod.asn1 file, which is available in the AdvantEDGE for Microsoft IIS product installation.

Assigning Entry Rows for the SystemEDGE Self-Monitoring Tables

All SystemEDGE self-monitoring tables (for example, log monitoring, Windows NT event monitoring, process/service monitoring, threshold monitoring, and history collection) require the use of unique row numbers. Each table contains an *Index* column which acts as a *key field* to distinguish rows in the table. This section describes the benefits of reserving a block of rows (somewhere in the range of 11 to the maximum number of rows in your table) for use by the system or application administrator.

Setting Local Policy

You may choose, as a matter of local policy, to reserve a block of rows for system administration. This policy allows you to define row entries within a reserved block of rows without worrying about the row already being taken by another user's entry. In compliance with the local policy, all other users should use row indices that are outside of the reserved range when they define user-configured entries.

By reserving a block of rows, you can define a consistent set of conditions (row entries) to be monitored across all machines such that the same condition is defined in the same row number on each of the machines. For example, you can use row 3000 in each table to define entries monitoring the page-not-found errors (iisWwwTtlNotFoundErr). You can then distribute this configuration out to every host so that every machine running IIS uses row 3000 for monitoring page-not-found errors, whether it is the threshold monitoring table or the history table. Further, every machine can use row 3000 for monitoring the WWW service in the process/service monitoring table.

Reserving Blocks of Rows

To reserve a block of rows for monitoring Microsoft IIS:

1. Decide on a block of rows that you want to reserve for use with monitoring Microsoft IIS.
2. Using that block of rows, define a set of row entries for each of the respective SystemEDGE self-monitoring tables. For more information, refer to the chapter on self-monitoring in the *SystemEDGE Agent User Guide*.

3. Distribute configuration file entries out to all hosts that are running IIS and AdvantEDGE for Microsoft IIS. For more information, refer to the *Automating the Deployment of SystemEDGE and AdvantEDGE Point Plug-in Modules* white paper.

NOTE

As an alternative, you can use this row-number assignment policy with AdvantEDGE View for group configuration operations.

4. Require end users to avoid your block of rows when defining their own self-monitoring table entries.

Using the SystemEDGE Self-Monitoring Features

The examples in this section show SystemEDGE configuration-file commands for monitoring Microsoft IIS. Add these commands to the sysedge.cf file to enable monitoring of the MIB objects that they specify. Modify these examples as necessary to monitor the MIB objects that are relevant for your configuration.

The examples in the following sections present row numbers in the 5000 range; select a row number for your configuration that conforms to local policies. For more information on row assignment, refer to "Assigning Entry Rows for the SystemEDGE Self-Monitoring Tables" on page 4-2.

The following command, for example, instructs the SystemEDGE agent to monitor whether the IIS process is alive every 30 seconds and to store the data in row 5000 of the Process Monitoring table:

```
watch process procAlive 'inetinfo|INETINFO' 5000 0x0
 30 'IIS' ''
```

For more information about the syntax for the commands in this section, refer to the *SystemEDGE Agent User Guide*.

NOTE

Enter the commands throughout this chapter as one line. Do **not** use a carriage return to match the formatting shown here.

Using SystemEDGE Process Monitoring

This section provides examples of how to use the SystemEDGE process- and service-monitoring capabilities to monitor the availability of crucial IIS processes and services. Add the commands in the following sections to the sysedge.cf file to monitor these processes. For more information on the SystemEDGE process- and service-monitoring capabilities, refer to the chapter on process and service monitoring in the *SystemEDGE Agent User Guide*.

Monitoring IIS

To make sure IIS is running, enter the following command:

```
watch process procAlive 'inetinfo|INETINFO' 5000 0x0
 30 'IIS' ''
```

Monitoring the IIS WWW Service

To make sure the IIS WWW Service is running, enter the following command:

```
watch ntservice 'World Wide Web Publishing Service' 5002 0x0
 30 'IIS WWW Service' ''
```

Monitoring the IIS FTP Service

To make sure the IIS FTP Service is running, enter the following command:

```
watch ntservice 'FTP Publishing Service' 5003 0x0 30 'IIS FTP
 Service' ''
```

Monitoring the IIS SMTP Service

To make sure the IIS SMTP Service is running, enter the following command:

```
watch ntservice 'Microsoft SMTP Service' 5004 0x0 30 'IIS SMTP
 Service' ''
```

Monitoring the IIS NNTP Service

To make sure the IIS NNTP Service is running, enter the following command:

```
watch ntservice 'Microsoft NNTP Service' 5005 0x0 30 'IIS NNTP
 Service' ''
```

Using SystemEDGE Threshold Monitoring

This section outlines the use of SystemEDGE threshold-monitoring capabilities to monitor important IIS metrics. Add the commands in the following sections to the sysedge.cf file to monitor thresholds for these MIB objects. For more information on SystemEDGE threshold monitoring, refer to the chapter on threshold monitoring in the *SystemEDGE Agent User Guide*.

NOTE

The choice of thresholds used in these examples may not be appropriate for your configuration; select thresholds that are appropriate for your environment.

Monitoring the Total Current Users

To monitor the total number of current users, enter the following command:

```
monitor oid iisTtlCurUsr.0 5002 0x0 60 delta > 100 'Total
  Current Users exceeds threshold'
```

Monitoring the KB Transferred

To monitor the number of KB transferred, enter the following command:

```
monitor oid iisTtlBytes.0 5003 0x0 60 delta > 524288 'Total
  KBytes Transferred exceeds threshold'
```

Monitoring the Number of WWW 404 Errors

To monitor the number of WWW 404 (page-not-found) errors, enter the following command:

```
monitor oid iisWwwTtlNotFoundErr.0 5004 0x0 60 delta > 100
  'WWW Total 404 Errors exceeds threshold'
```

Monitoring the Number of Web Application Requests

To monitor the number of Web application requests, enter the following command:

```
monitor oid iisWebAppReqTtl.0 5005 0x0 60 delta > 100 'Web
  Application Requests exceeds threshold'
```

Monitoring the Number of ASP Script Errors

To monitor the number of ASP script errors, enter the following command:

```
monitor oid iisAspErrScript.0 5006 0x0 60 absolute > 40 'ASP
  Total Script Errors exceeds threshold'
```

Monitoring WWW 404 Errors on an Individual Web Site

To monitor the number of WWW 404 (page not found) errors on an individual Web site, enter the following command:

```
monitor oid ntRegPerf.50.0 5007 0x0 60 absolute > 200 'WWW
  Total 404 Errors on WebA exceeds threshold'
```

NOTE

If you are monitoring WWW 404 errors on an individual Web site, you must use the corresponding ntRegPerf item. Refer to "Using the Windows NT RegPerf Extensions" on page 4-12.

Monitoring the Number of Web Logon Failures Over Time

To monitor for 20 Web Logon Failure events in the system log within one minute, enter the following command:

```
monitor oid ntEventMonMatches.5012 50010 0x0 60 delta > 20
  'More than 20 Logon Failures in Web Server in 1 Min' ''
```

NOTE

To use this Web Logon Failure example, you need a corresponding Windows NT Event Monitor 5012 to monitor Web Logon Failures. For the corresponding entry, refer to "Monitoring IIS Web Logon Failure Events for IIS WWW Service in the System Event Log" on page 4-11.

Monitoring the Number of FTP Logon Failures Over Time

To monitor for 20 FTP Logon Failure events in the system log within one minute, enter the following command:

```
monitor oid ntEventMonMatches.5013 50011 0x0 60 delta > 20
  'More than 20 Logon Failures on FTP Server in 1 Min' ''
```

NOTE

To use this FTP Logon Failure example, you need a corresponding Windows NT Event Monitor 5013 looking at FTP Logon Failures. For the corresponding entry, refer to "Monitoring IIS FTP Logon Failure Events for IIS FTP Service in the System Event Log" on page 4-11.

Using SystemEDGE History Collection

This section outlines the use of SystemEDGE history capabilities to track the value of important IIS metrics over time. Add the commands in the following sections to the sysedge.cf file to collect history for these MIB objects. For more information, refer to the chapter on history collection in the *SystemEDGE Agent User Guide*.

NOTE

The number of samples and the interval between samples used in these examples may not be appropriate for your IIS system; select values that are appropriate for your environment.

Collecting History for Current Number of Users for the IIS Service

To collect history for the current number of users for the WWW service, enter the following command:

```
emphistory 5002 60 iisWwwCurUsrs.0 400 'WWW Num Current Users
 History'
```

Collecting History for Current Number of Users for the IIS FTP Service

To collect history for the current number of users for the FTP service, enter the following command:

```
emphistory 5003 60 iisFtpCurUsrs.0 200 'FTP Num Current Users
 History'
```

Figure 4-1 shows a sample history for total current users.

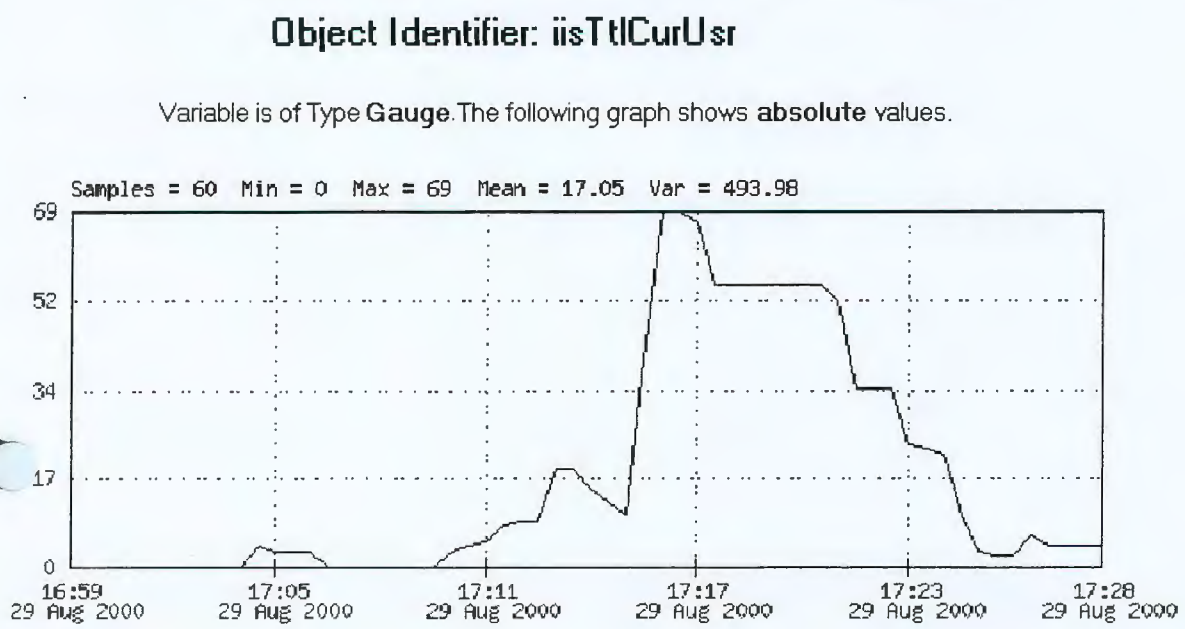


Figure 4-1: IIS Total Current Users Count History

Collecting History for Local Queue Length for the SMTP Service

To collect history for the local queue length for the SMTP service, enter the following command:

```
emphistory 5004 60 iisSmtpLocQueLen.0 480 'SMTP Local Queue
 Len History'
```

Collecting History for the Local Retry Queue Length for the SMTP Service

To collect history for the local retry queue length for the SMTP service, enter the following command:

```
emphistory 5005 60 iisSmtpRtryQueLen.0 480 'SMTP Local Retry
 Queue Len History'
```

Using SystemEDGE Windows NT Event Monitoring

This section outlines the use of SystemEDGE Windows NT event monitoring to capture important IIS-related Windows NT events and forward them to the appropriate management software as SNMP traps. The examples in this section show SystemEDGE configuration-file commands that instruct the SystemEDGE agent to monitor for certain types of Windows NT events that are related to IIS. Add the commands in the following sections to the sysedge.cf file to monitor for these Windows NT events. For more information, refer to the chapter on Windows NT event monitoring in the *SystemEDGE Agent User Guide*.

Monitoring IIS WWW Service Events in the System Event Log

To monitor for WWW service events in the system event log, enter the following command:

```
watch ntevent 5000 0x00 System All 'W3SVC' '.*' 'Monitor IIS
  WWW Service System Events' ''
```

Monitoring IIS WWW Service Events in the Security Event Log

To monitor for WWW service events in the security event log, enter the following command:

```
watch ntevent 5001 0x00 Security All 'W3SVC' '.*' 'Monitor IIS
  WWW Service Security Events' ''
```

Monitoring IIS WWW Service Events in the Application Event Log

To monitor for WWW service events in the application event log, enter the following command:

```
watch ntevent 5002 0x00 Application All 'W3SVC' '.*' 'Monitor
  IIS WWW Service Application Events' ''
```

Monitoring IIS FTP Service Events in the System Event Log

To monitor for FTP service events in the system event log, enter the following command:

```
watch ntevent 5003 0x00 System All 'MSFTPSVC' '.*' 'Monitor
  IIS FTP Service System Events' ''
```

Monitoring IIS FTP Service Events in the Security Event Log

To monitor for FTP service events in the security event log, enter the following command:

```
watch ntevent 5004 0x00 Security All 'MSFTPSVC' '.*' 'Monitor
  IIS FTP Service Security Events' ''
```

Monitoring IIS FTP Service Events in the Application Event Log

To monitor for FTP service events in the application event log, enter the following command:

```
watch ntevent 5005 0x00 Application All 'MSFTPSVC' '.*' 'Monitor
IIS FTP Service Application Events' ''
```

Monitoring IIS SMTP Service Events in the System Event Log

To monitor for SMTP service events in the system event log, enter the following command:

```
watch ntevent 5006 0x00 System All 'SMTPSVC' '.*' 'Monitor IIS
  SMTP Service System Events' ''
```

Monitoring IIS SMTP Service Events in the Security Event Log

To monitor for SMTP service events in the security event log, enter the following command:

```
watch ntevent 5007 0x00 Security All 'SMTPSVC' '.*' 'Monitor
  IIS SMTP Service Security Events' ''
```

Monitoring IIS SMTP Service Events in the Application Event Log

To monitor for SMTP service events in the application event log, enter the following command:

```
watch ntevent 5008 0x00 Application All 'SMTPSVC' '.*'
  'Monitor IIS SMTP Service Application Events' ''
```

Monitoring IIS NNTP Service Events in the System Event Log

To monitor for NNTP service events in the system event log, enter the following command:

```
watch ntevent 5009 0x00 System All 'NNTPSVC' '.*' 'Monitor IIS
  NNTP Service System Events' ''
```

Monitoring IIS NNTP Service Events in the Security Event Log

To monitor for NNTP service events in the security event log, enter the following command:

```
watch ntevent 5010 0x00 Security All 'NNTPSVC' '.*' 'Monitor
  IIS NNTP Service Security Events' ''
```

Monitoring IIS NNTP Service Events in the Application Event Log

To monitor for NNTP service events in the application event log, enter the following command:

```
watch ntevent 5011 0x00 Application All 'NNTPSVC' '.*'
  'Monitor IIS NNTP Service Application Events' ''
```

Monitoring IIS Web Logon Failure Events for IIS WWW Service in the System Event Log

To monitor for Web Logon Failure events in the system event log, enter the following command:

```
watch ntevent 5012 0x00 System All 'W3SVC'
  '.*Logon.*failure.*' 'Web Logon Failure' ''
```

Monitoring IIS FTP Logon Failure Events for IIS FTP Service in the System Event Log

To monitor for FTP Logon Failure events in the system event log, enter the following command:

```
watch ntevent 5013 0x00 System All 'MSFTPSVC'
  '.*Logon.*failure.*' 'FTP Logon Failure' ''
```

Monitoring IIS FTP Timeouts for IIS FTP Service in the System Event Log

To monitor for FTP Timeout events in the system event log, enter the following command:

```
watch ntevent 5014 0x00 System All 'MSFTPSVC'
  '.*User.*timed-out.*' 'FTP User Time-out' ''
```

Using the Windows NT RegPerf Extensions

This section outlines the use of SystemEDGE Windows NT RegPerf extension-monitoring capabilities to capture extended IIS-related information. The examples in this section show the SystemEDGE configuration-file commands that instruct the SystemEDGE agent to provide information on an individual Web site. You can use this variable with threshold monitoring to provide traps on specific user sites. Place these commands in the SystemEDGE configuration file, sysedge.cf.

Add the commands in the following sections to the sysedge.cf file to monitor these Windows NT RegPerf extensions. The following examples use values of 50 and 51; select values for your system that conform to local policies.

For more information, refer to the chapter on Windows NT Registry MIB objects in the *SystemEDGE Agent User Guide*.

Monitoring IIS WWW 404 Errors

To monitor for WWW 404 errors on Web site A (WebA), enter the following command:

```
ntregperf 50 Integer Performance 'Web Service' 'Total Not
  Found Errors' 'WebA'
```

Monitoring Unauthorized ASP Requests

To monitor for ASP requests that are not authorized on Web site B (Web B), enter the following command:

```
ntregperf 51 Integer Performance 'Active Server Pages'
  'Requests Not Authorized' 'WebB'
```

Index

Manual 33

ADVANTEDGE FOR MICROSOFT EXCHANGE User Guide

ADVANTEDGE™

FOR MICROSOFT® EXCHANGE

User Guide

Release 1.1 or Later

09-16030-002
April 2001

Important Notice

Application Health, System Health, Live Health, SystemEDGE, AdvantEDGE, *e*Health, Infrasense, MIB Manager, State-of-the-World, and the FirstSense logo are trademarks of Concord Communications, Inc.

The Total View, Concord, the Concord logo, Empire Technologies, Network Health, TRAKKER, FirstSense, and We See It Happening are registered trademarks of Concord Communications, Inc.

Microsoft, Active Directory, Windows, Windows 2000, and Windows NT are trademarks or registered trademarks of Microsoft Corporation.

General Notice: Some of the product names used herein have been used for identification purposes only and may be trademarks of their respective companies.

Proprietary Notice

The information and descriptions contained herein are the property of Concord Communications, Inc. Such information and descriptions may not be copied, disseminated, or distributed without the express written consent of Concord Communications, Inc. Concord Communications, Inc., assumes no responsibility for any inaccuracies that may appear in this document. Concord Communications, Inc., reserves the right to improve its products and change specifications at any time without notice.

U. S. Government Restricted Rights

Use, reproduction, and disclosure by the U.S. Government are subject to the restrictions set forth in FAR §52.227-19 (c) (1) and (2) and DFARS §252.227-7013 (c) (1) (ii).

Patent Information

U. S. Patent 5,615,323
Patents Pending

Printed on recycled paper in the USA

Table of Contents

About This Guide

Chapter 1
Introduction

Chapter 2
Installing AdvantEDGE for Microsoft Exchange

Chapter 3
Using the AdvantEDGE for Microsoft Exchange MIB

Chapter 4
Using AdvantEDGE for Microsoft Exchange

About This Guide

The *AdvantEDGE for Microsoft Exchange User Guide* provides instructions for installing and using AdvantEDGE for Microsoft Exchange for Windows NT x86 and Windows 2000 systems.

NOTE

AdvantEDGE for Microsoft Exchange supports Exchange 5.5 and Exchange 2000.

This guide is intended for the person responsible for installing and configuring AdvantEDGE for Microsoft Exchange. This version supports AdvantEDGE for Microsoft Exchange Release 1.1 or later, and the SystemEDGE Agent Release 4.0, Patchlevel 3 and later.

To use AdvantEDGE for Microsoft Exchange, you should be familiar with the Microsoft Exchange application and the Concord SystemEDGE agent. Refer to Microsoft documentation and the *SystemEDGE Agent User Guide* for more information.

NOTE

Unless otherwise specified, the content of this guide applies to both Exchange 5.5 and Exchange 2000. In areas where there are differences, this guide specifies to which version the content applies.

How This Guide Is Organized

This guide is organized as follows:

- Chapter 1, "Introduction," provides an overview of AdvantEDGE for Microsoft Exchange and its features.
- Chapter 2, "Installing AdvantEDGE for Microsoft Exchange," explains how to install, configure, and license the AdvantEDGE for Microsoft Exchange software on a host system.

- Chapter 3, "Using the AdvantEDGE for Microsoft Exchange MIB," describes the information that is available through the AdvantEDGE for Microsoft Exchange MIB.
- Chapter 4, "Using AdvantEDGE for Microsoft Exchange," explains how to configure and use AdvantEDGE for Microsoft Exchange in your host environment.

Conventions Used in This Guide

This section describes conventions used in this guide.

System Root Text Convention

This guide uses the system root text convention that is used by Microsoft to denote the Windows NT root directory:

```
%SystemRoot%\system32\
```

where `%SystemRoot%` is `C:\winnt` for Windows NT 4.0 and Windows 2000.

Conventions for Commands

The following paragraph shows a sample command. Due to space limitations in this guide, some commands wrap from one line to the next. Disregard these line breaks, and **enter each command as one line**. Otherwise, your command syntax will be incorrect. For example, when you see a command such as the following:

```
watch process procAlive 'emsmta|EMSMTA' 5000 0x0 30
  'Exchange MTA' ''
```

You **must** enter the command on one line, as shown here:

```
watch process procAlive 'emsmta|EMSMTA' 5000 0x0 30 'Exchange MTA' ''
```

Contact Information

If you need any assistance with the SystemEDGE agent or the AdvantEDGE for Microsoft Exchange Point module, contact Customer Support, using one of the following methods:

Phone:	(888) 832-4340 (for calls from the USA and Canada) (508) 303-4300 (for calls from other countries)
Fax:	(508) 303-4343
E-mail:	support@concord.com
Web site:	http://www.concord.com
Licensing:	http://license.concord.com

1 Introduction

This chapter provides an overview of the AdvantEDGE Point module for Microsoft Exchange and of the Microsoft Exchange architecture.

NOTE

Unless otherwise stated, the term *Exchange*, as used throughout this guide and the Management Information Base (MIB) specification, refers to the Microsoft Exchange application in its entirety, which encompasses all the core services, connectors, and optional components.

Features of AdvantEDGE for Microsoft Exchange

AdvantEDGE for Microsoft Exchange is a plug-in for the SystemEDGE agent. It enables information technology (IT) operators to monitor the performance and availability of Microsoft Exchange. Microsoft Exchange is a groupware application that enables communication and collaborative work. At its core is an e-mail routing, distribution, and storage facility. Exchange serves as the e-mail backbone for many corporations. Therefore, monitoring its health and availability is crucial to ensuring the smooth functioning of today's corporate information infrastructure.

The AdvantEDGE for Microsoft Exchange Point module makes important information about Microsoft Exchange available to management software through the SystemEDGE agent and Simple Network Management Protocol (SNMP). The SystemEDGE agent's self-monitoring capabilities enable the monitoring of important Exchange metrics, processes, and services, as well as the sending of SNMP traps when exceptions or exception conditions occur.

This release of AdvantEDGE for Microsoft Exchange supports Exchange 5.5 and Exchange 2000.

NOTE

This document does not explain how to install, administer, or use Microsoft Exchange. For help with Microsoft Exchange, refer to the Microsoft documentation.

Microsoft Exchange Architecture

Microsoft Exchange is a complex piece of software containing many components. At the core of Microsoft Exchange are the following services:

- Mail transfer agent (MTA), which is responsible for routing e-mail messages to and from users.
- Directory service (DS), which maintains information about recipients, mailboxes, public and private folders, mailing lists, and other distribution lists (Exchange 5.5 only; Exchange 2000 uses Active Directory).
- Information store (IS), which serves as the repository of all messages on the Exchange server, and is composed of private and public areas.
- System attendant, which maintains the Exchange application's database and directory integrity, and on which all other Exchange services depend.
- Connectors, which transfer messages between sites, organizations, and non-native Exchange e-mail formats (for example, Internet, Lotus Notes, and Microsoft Mail). Several connectors are available from Microsoft and from third parties.
- Internet Information Services (IIS), which provides SMTP, IMAP, and POP services for Exchange 2000.

Figure 1-1 shows the relationships between the components of Microsoft Exchange 5.5. The architecture of Exchange 2000 is similar.

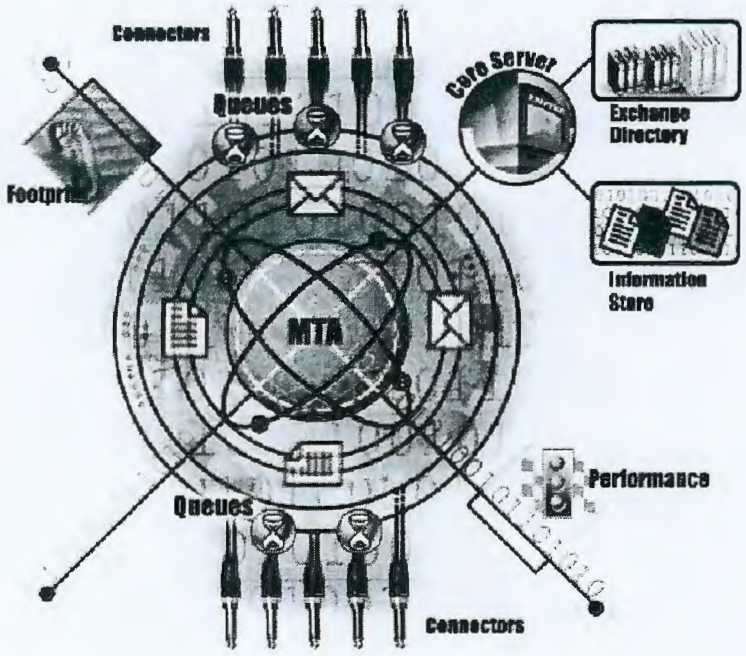


Figure 1-1: Microsoft Exchange 5.5 Architecture

Because Microsoft Exchange is a complex application, monitoring Exchange is more complex than ensuring that a single process or Windows NT service is up and running. The many components that make up Exchange can function properly only through the availability of a variety of configuration parameters, settings, processes, Windows NT services, queues, and system resources.

Using AdvantEDGE for Microsoft Exchange

AdvantEDGE for Microsoft Exchange can provide you with the tools and information that you need to monitor the health and availability of your Exchange server. It works with the SystemEDGE agent to closely manage the Microsoft Exchange application, providing real-time fault detection and automatically correcting problems, if necessary. You can use AdvantEDGE for Microsoft Exchange with any SNMP-compliant management software, including Concord's *e*Health suite of products, AdvantEDGE View, HP OpenView, and others.

You can use this plug-in with the SystemEDGE agent to perform the following tasks:

- Detect failed Exchange services (such as the Information Store or Message Transfer Agent) and restart them automatically.
- Alert an administrator when message queues become dangerously large, indicating potential security violations through SystemEDGE intelligent self-monitoring.
- Watch for Information Stores and disk partitions that are nearing capacity.
- Automatically delete temporary files when a threshold is reached to free up disk space and ensure continuous availability and performance.
- Detect types of Windows NT Events and forward them as SNMP traps to your network management system (NMS).

Using AdvantEDGE for Microsoft Exchange with *e*Health

You can use AdvantEDGE for Microsoft Exchange and the SystemEDGE agent with the *e*Health product suite to provide the historical data for long-term trending analysis and capacity planning. With *e*Health – Application Assessment, you can run At-a-Glance, Trend, Top N, or MyHealth reports for the following types of variables:

- Amount of Central Processing Unit (CPU), total memory, and disk space that the Exchange application is using
- Size of the MTA and DS logs (Exchange 5.5 only)
- Amount of data, and number and type (public or private) of messages being processed by the MTA service
- Number of messages waiting to be processed by the MTA service
- Number of users
- SMTP traffic

For more information about the variables that you can monitor and reports you can run when you integrate AdvantEDGE for Microsoft Exchange with *e*Health, refer to the *e*Health Web Help.

Using AdvantEDGE for Microsoft Exchange with Live Health

You can also use AdvantEDGE for Microsoft Exchange and the SystemEDGE agent with Live Health for real-time detection of potential problems. Live Health applies intelligent algorithms to the data, resulting in precise assessments of application health and performance. For more information about how Live Health can detect "brownouts" and service delays across applications, systems, and networks, refer to the Live Health Web Help.

2 Installing AdvantEDGE for Microsoft Exchange

This chapter explains how to install, configure, and license AdvantEDGE for Microsoft Exchange.

Installation Requirements

Before you install AdvantEDGE for Microsoft Exchange, you must first install, license, and configure the SystemEDGE agent Release 4.0, Patchlevel 3 or later. Refer to the *SystemEDGE Agent User Guide* for more information. Also, you must be running Windows NT 4.0 or Windows 2000. For more information, refer to your Microsoft documentation.

Installing the Software

AdvantEDGE for Microsoft Exchange is distributed as a self-extracting executable named **xchgmod.exe**.

Follow these steps to install AdvantEDGE for Microsoft Exchange:

1. Log on to the Windows NT system as administrator.
2. Click **Start**.
3. Select **Programs** → **Command Prompt**.
4. Insert the CD containing the Concord software distributions into the CD-ROM drive.

   Windows NT or Windows 2000 automatically mounts the drive using the CD-ROM drive's corresponding drive letter. The particular drive letter is specific to your system and depends on the number and types of disks attached to your system.

5. Determine which directory you want to use as the installation directory for AdvantEDGE for Microsoft Exchange. If the SystemEDGE agent is installed in C:\sysedge, the recommended installation directory is C:\sysedge\plugins.
6. Run the self-extracting executable by entering the following at the command prompt, where `D:` is the CD-ROM drive for your system, and `C:sysedge\plugins` is the installation directory:

   ```
   D:\xchgmod\ntx86\xchgmod.exe -dir C:\sysedge\plugins
   ```

   The -dir option instructs the self-extracting executable to create the intended subdirectory hierarchy that is described throughout this guide. It then places the distribution in an xchgmod subdirectory within the specified target directory (for example, C:\sysedge\plugins).

NOTE

You cannot run xchgmod.exe directly from the CD-ROM.

AdvantEDGE for Microsoft Exchange is now installed.

AdvantEDGE for Microsoft Exchange Files

Table 2-1 describes the files that are installed during the AdvantEDGE for Microsoft Exchange installation.

Table 2-1: Files Installed by AdvantEDGE for Microsoft Exchange

File Name	Description
xchgmod.dll	AdvantEDGE for Microsoft Exchange dynamic link library (DLL) module for Windows NT and Windows 2000
xchgmod.pdf	*AdvantEDGE for Microsoft Exchange User Guide*
xchgmod.asn1	AdvantEDGE for Microsoft Exchange MIB specification
examples	AdvantEDGE for Microsoft Exchange monitoring examples
relnotes.txt	Release notes for AdvantEDGE for Microsoft Exchange

Configuring AdvantEDGE for Microsoft Exchange

The SystemEDGE agent reads the configuration file sysedge.cf and uses the *sysedge_plugin* keyword to specify which AdvantEDGE Point modules to load at system initialization. By default, the SystemEDGE agent does not load any plug-ins at initialization time, but you can configure the agent to load any AdvantEDGE Point modules that you have installed by editing the sysedge.cf file as follows.

To configure the SystemEDGE agent to start AdvantEDGE for Microsoft Exchange, provide the complete path name to xchgmod.dll, the AdvantEDGE for Microsoft Exchange DLL. The actual path depends on the location you selected when installing AdvantEDGE for Microsoft Exchange files. For example, enter this command if you installed the files in the C:\sysedge\plugins\xchgmod directory:

```
sysedge_plugin C:\sysedge\plugins\xchgmod\xchgmod.dll
```

For more information about the sysedge.cf file, refer to the *SystemEDGE Agent User Guide*.

Licensing AdvantEDGE for Microsoft Exchange

Like the SystemEDGE agent, AdvantEDGE for Microsoft Exchange utilizes a *host-based* license method. Copies of AdvantEDGE for Microsoft Exchange can run only on systems that possess a valid license key. This license is separate from the one used for the SystemEDGE agent.

The first time that you attempt to start the SystemEDGE agent after installing AdvantEDGE for Microsoft Exchange, the agent displays a message that says that a valid license was not found for AdvantEDGE for Microsoft Exchange. It then provides you with a *public key* that is used to generate a permanent license key for your host machine.

A license key is made up of four space-separated, 8-character sequences, totaling 32 characters. The AdvantEDGE for Microsoft Exchange license is stored in the sysedge.lic file, the same file that is used for SystemEDGE agent licenses. Refer to the sample license file on page 2-6.

Obtaining a License

To obtain a license, you can do any of the following:

- Run the Concord-supplied licenseutil.pl script.
- Run the licenseme.exe license utility.
- Use the AdvantEDGE View licensing procedure, which is based on SNMP traps. For more information, refer to the AdvantEDGE View Web Help.
- Send an e-mail request to license@concord.com and place the returned license key in the appropriate license file.

NOTE

Always include the Customer ID and user name in license requests that you send through e-mail.

- Complete the online license form through the Internet, as described in the next section, "Generating the License".

For more information about licensing, refer to the *SystemEDGE Agent User Guide* and the *Automating the Licensing of SystemEDGE and AdvantEDGE Point Plug-in Modules* white paper.

NOTE

If you are using an evaluation copy of AdvantEDGE for Microsoft Exchange, you must request a temporary license that will enable it to operate during the evaluation period.

Generating the License

This section describes how to generate the license using the Web-based license form. For Windows NT and Windows 2000, the setup program generates the licensing information for your system.

1. Run the SystemEDGE agent setup command to request licensing information by entering the following at the command prompt:

   ```
   sysedge\setup -l
   ```

   The setup program displays a message similar to the following:

```
SystemEDGE Version 4.0 Patchlevel 3
Copyright 2001 by Concord Communications, Inc.
Please contact Concord Communications, Inc. to obtain a license
http://www.concord.com/support, Email: license@concord.com
Provide this: sysedge neptune NTx86 4.0 346561363366b19c 4.0 Patchlevel 3
```

2. Fill out the online Web-based license form that is available from Concord's licensing Web server at the following URL:

   `http://license.concord.com`

   NOTE

   You must supply a user name and password to access the license form.

   The license form asks you to supply the following information:

   - Customer ID
   - Name
   - E-mail address
   - Software version number (4.0 in the example above)
   - Patchlevel (3 in the example above)
   - System name (neptune in the example above)
   - Operating system name (NTx86 in the example above)
   - Version (4.0 in the example above)
   - System identifier (346561363366b19c in the example above)

   NOTE

   When you are licensing AdvantEDGE for Microsoft Exchange, select **xchgmod** as the product on the licensing form.

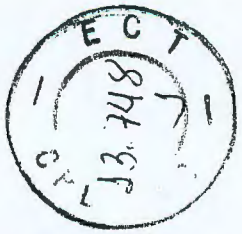
   After you submit the license request, the Concord Web server generates a license and displays it to your Web browser. It also e-mails the license to the contact person in your organization.

3. Copy the generated license key into the sysedge.lic file in the system32 subdirectory (for example, C:\winnt\system32), and then save the file.

   The license key is case sensitive. Copy it exactly as it appears. If possible, use your system's cut-and-paste facility instead of typing it by hand. If you are entering the license key by hand, be careful not to confuse characters such as the letters **l** and **I** and the number **1**, or the letter **O** and the number **0**.

4. Stop and restart the Windows NT Master agent by entering these commands at the command prompt:

   ```
   net stop snmp
   net start snmp
   ```



The AdvantEDGE for Microsoft Exchange Point module is now licensed and ready to use.

Sample License File

The following is a sample SystemEDGE agent license file. A pound character (#) in column 1 indicates that the entire line is a comment.

```
# license file for SystemEDGE Agent
# Empire Technologies, Inc.
# A Concord Communications Company
# http://www.concord.com
#
# file /etc/sysedge.lic or %SystemRoot%\system32\sysedge.lic
# A valid license key has four parts of 8 characters per part
# parts are separated by space(s) with one license key per line
# sysedge jupiter NTx86 4.0 807cb1da007cb1da 4.0
e13311d3 0F2a7cb1 abC512dc fF8C923a

# xchgmod jupiter NTx86 4.0 807cb1da007cb1da 4.0
a7943fde 098a87ij a4kiuf39 afafEkj4
```

3

Using the AdvantEDGE for Microsoft Exchange MIB

This chapter outlines the organization and content of the Concord Communications MIB for Microsoft Exchange. The MIB specification (xchgmod.asn1) defines a collection of objects for monitoring and managing Microsoft Exchange. You must configure the SystemEDGE agent to monitor the MIB objects that are relevant for your configuration. For more information, refer to Chapter 4, "Using AdvantEDGE for Microsoft Exchange."

Figure 3-1 shows the organization of the AdvantEDGE for Microsoft Exchange MIB.

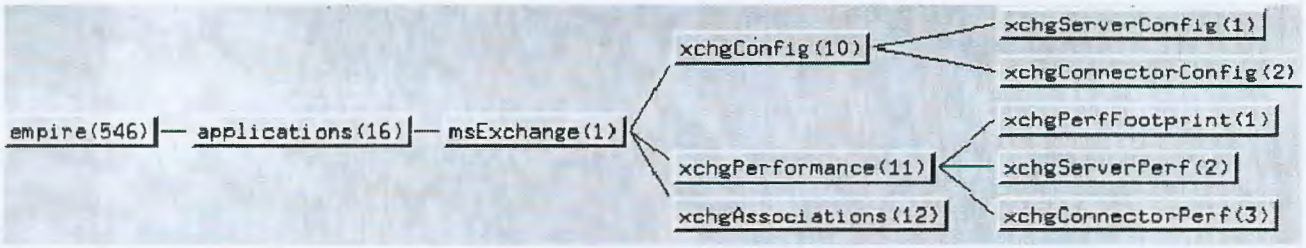


Figure 3-1: AdvantEDGE for Microsoft Exchange MIB

The MIB is organized into broad sections for configuration and performance. Within those broad sections are subsections for connector configuration and performance, and for core server configuration and performance. Within the performance section, a footprint section defines MIB objects that convey how much of the underlying system's resources are consumed by the Microsoft Exchange application.

The following sections define important MIB objects from the Exchange MIB. This chapter defines all sections of the AdvantEDGE for Microsoft Exchange MIB, but it does **not** define all of the MIB objects. For a complete list of MIB objects, refer to the AdvantEDGE for Microsoft Exchange MIB Specification (xchgmod.asn1).

NOTE

Unless otherwise noted, these MIB objects are supported for both Exchange 5.5 and Exchange 2000.

Configuration Section

The Configuration section of the AdvantEDGE for Microsoft Exchange MIB contains configuration parameters and settings that are important for streamlining the health and performance of your Exchange server. It also includes configuration information about core servers and connectors.

Server Configuration

The server configuration MIB group contains configuration parameters, process identifiers (IDs), and version and build numbers, as well as log and database locations. Table 3-1 defines important Server Configuration parameters.

Table 3-1: Selected MIB Objects – Exchange Server Configuration Group (Page 1 of 2)

MIB Object	Description
xchgVersion	Exchange version.
xchgBuildNumber	Exchange build number.
xchgInstallLocation	Location where Exchange is installed.
xchgStoreBuffers	Number of Exchange storage buffers configured. (Exchange 5.5 only)
xchgMinStoreThreads	Minimum number of information store (IS) threads. (Exchange 5.5 only)
xchgMaxStoreThreads	Maximum number of IS threads. (Exchange 5.5 only)
xchgPubStoreFile	Filename of the public IS.
xchgPrivStoreFile	Filename of the private IS.

Table 3-1: Selected MIB Objects – Exchange Server Configuration Group (Page 2 of 2)

MIB Object	Description
xchgISWorkDir	IS working directory.
xchgMTARunDir	Mail Transfer Agent (MTA) run directory where temporary and working files are stored.
xchgMTADBPath	Directory containing the MTA database file(s).
xchgDSDBFile	Directory database filename. (Exchange 5.5 only)
xchgDSWorkDir	Exchange working directory where temporary and working files are stored. (Exchange 5.5 only)
xchgSApid	Process ID of the Exchange system attendant.
xchgISpid	Process ID of the Exchange information store.
xchgMTApid	Process ID of the Exchange MTA.
xchgDSpid	Process ID of the Exchange Directory.
xchgCoreIISPID	Process ID of the core IIS service, which provides SMTP, IMAP4, POP3, NNTP, and the core message routing engine. (Exchange 2000 only)

Figure 3-2 shows an example of an AdvantEDGE View core server status for Microsoft Exchange 5.5.

Component	Status	Process ID	Start-Time
Directory	Up	251	Fri Jun 09 06:22:39 2000
MTA	Up	300	Fri Jun 09 06:22:45 2000
Information Store	Up	295	Fri Jun 09 06:22:39 2000
System Attendant	Up	234	Fri Jun 09 06:22:39 2000

Figure 3-2: Core Server Listing for Exchange 5.5

Figure 3-3 shows an example of an AdvantEDGE View core server status for Microsoft Exchange 2000.

Component	Status	Process ID	Start-Time
MTA	Up	1760	Sat Feb 17 17:02:47 2001
Information Store	Up	1636	Sat Feb 17 17:02:31 2001
System Attendant	Up	1176	Sat Feb 17 17:02:31 2001
Core IIS	Up	1108	Sat Feb 17 17:02:31 2001

Figure 3-3: Core Server Listing for Exchange 2000

Connector Configuration

The Connector Configuration MIB group contains the configuration parameters, process IDs, and installation status of the various Exchange connectors. Table 3-2 defines important Connector Configuration parameters.

Table 3-2: Selected MIB Objects – Exchange Connector Configuration Group (Page 1 of 2)

MIB Object	Description
xchgMMCInstalled	Indicates whether MS Mail connector is installed.
xchgMMCpid	Provides the process ID of the MS Mail connector.
xchgCCMCInstalled	Indicates whether Lotus cc:Mail connector is installed.
xchgCCMCpid	Provides the process ID of the cc:Mail connector.
xchgIMSInstalled	Indicates whether the Internet Mail connector is installed. On Exchange 2000, this object indicates whether the IIS/SMTP service is installed.
xchgIMSpid	Provides the process ID of the Internet Mail connector. On Exchange 2000, this object reports the PID of the IIS/SMTP service.
xchgKMSInstalled	Indicates whether Key Management Service connector is installed.
xchgKMSpid	Provides the process ID of the Key Management Service connector.

Table 3-2: Selected MIB Objects – Exchange Connector Configuration Group (Page 2 of 2)

MIB Object	Description
xchgNEWSInstalled	Indicates whether the Microsoft Exchange USENET/News connector is installed. On Exchange 2000, this object reports on whether the IIS/NNTP service is installed.
xchgNEWSpid	Provides the process ID of the USENET/News connector. On Exchange 2000, this object reports the PID of the IIS/NNTP service.
xchgIMAP4Installed	Indicates whether the Exchange 2000 IIS/IMAP 4 service is installed. (Exchange 2000 only)
xchgPOP3Installed	Indicates whether the Exchange 2000 IIS/POP3 service is installed. (Exchange 2000 only)
xchgRouteInstalled	Indicates whether the Exchange 2000 IIS/RoutingEngine service is installed. (Exchange 2000 only)
xchgSRSInstalled	Indicates whether the Exchange 2000 Site Replication Service is installed. SRS enables Exchange 2000 to emulate Exchange 5.5 directory services. (Exchange 2000 only)
xchgSRSPID	Provides the process ID of the Exchange 2000 Site Replication Service.

Figure 3-4 shows an example of an AdvantEDGE View connector configuration status for Microsoft Exchange 5.5.

Connector	Installed	Running	ProcessID
MS Mail	Yes	No	0
MS Mail (AppleTalk)	No	No	0
cc:Mail	Yes	No	0
Internet Mail Service	Yes	Yes	432
x400	No	No	0
Site	No	No	0
RAS	No	No	0
Web	No	No	(null)
Schedule Free/Busy	Yes	No	0
Key Management Server	No	No	0
USENET News	No	No	0

Figure 3-4: Exchange 5.5 Connector Configuration Listing

Figure 3-5 shows an example of an AdvantEDGE View connector configuration status for Microsoft Exchange 2000.

Connector	Installed	Running	ProcessID	Start-Time
MS Mail	No	No	0	
MS Mail (AppleTalk)	No	No	0	
cc:Mail	No	No	0	
Internet Mail or SMTP Service	Yes	Yes	1108	Sat Feb 17 17:02:31 2001
x400	Yes	Yes	1760	
Site	No	No	0	
RAS	No	No	0	
Schedule Free/Busy	No	No	0	
Key Management Server	No	No	0	
USENET News	Yes	Yes	1108	Sat Feb 17 17:02:31 2001
IRC Chat	No	No	0	
MS Conferencing	No	No	0	
Lotus Notes	No	No	0	
GroupWise	No	No	0	
IMAP4	Yes	Yes	1108	Sat Feb 17 17:02:31 2001
POP3	Yes	Yes	1108	Sat Feb 17 17:02:31 2001
Routing Engine	Yes	Yes	1108	Sat Feb 17 17:02:31 2001
Site Replication Service	Yes	No	0	
T.120	No	No	0	

Figure 3-5: Exchange 2000 Connector Configuration Listing

Performance

The Performance section of the Exchange MIB contains performance data that is necessary for capacity planning and trend analysis, as well as real-time performance and availability monitoring. The Performance group is divided into several subgroups for footprint data (page 3-8), server performance (page 3-10), and connector performance (page 3-11).

Exchange Footprint

The Exchange Footprint group provides information about the Exchange CPU, memory, and disk resource consumption, more commonly called its *footprint*. Long-term trending analysis of footprint information is useful for anticipating and avoiding email problems due to resource exhaustion. Footprint information can also be monitored in real time to detect and correct temporary resource exhaustion due to viruses, security incidents, and hardware failures. Table 3-3 defines important Footprint metrics.

Table 3-3: Selected MIB Objects – Exchange Footprint Group

MIB Object	Description
xchgCPUTime	Total accumulated central processing unit (CPU) time for Exchange.
xchgPercentCPU	Percentage of CPU, over the last interval, used by Exchange.
xchgTotalRSS	Total real memory currently in use by Exchange.
xchgPercentMEM	Percentage of real memory currently in use by Exchange.
xchgDirSize	Current size of the Exchange directory. (Exchange 5.5 only)
xchgPrivStoreSize	Current size of the private IS.
xchgPubStoreSize	Current size of the public IS.
xchgTotalDiskSize	Estimate of the current total disk space used by Exchange.
xchgTotalThreads	Total number of system threads used by Exchange.

The following figures show sample footprints for a live Exchange application that is serving a medium-sized company. They represent real data collected from live Exchange servers and displayed in AdvantEDGE View reports.

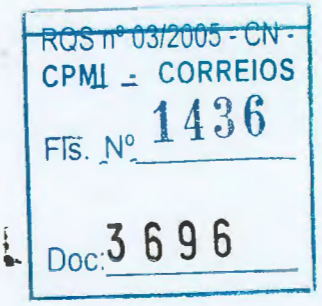


Figure 3-6 shows a sample AdvantEDGE View footprint for Exchange disk usage.

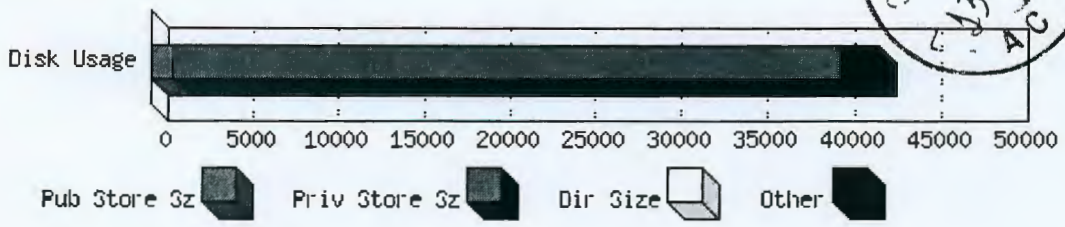


Figure 3-6: Exchange Disk Usage Footprint

Figure 3-7 shows a sample AdvantEDGE View footprint for Exchange memory usage (resident set size [RSS]).

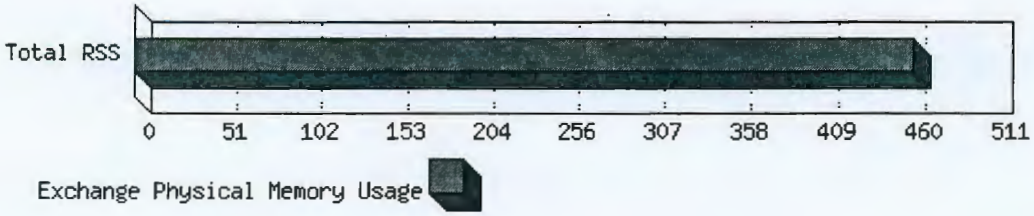


Figure 3-7: Exchange Memory Usage (RSS) Footprint

Figure 3-8 shows a sample AdvantEDGE View footprint summary for Exchange.

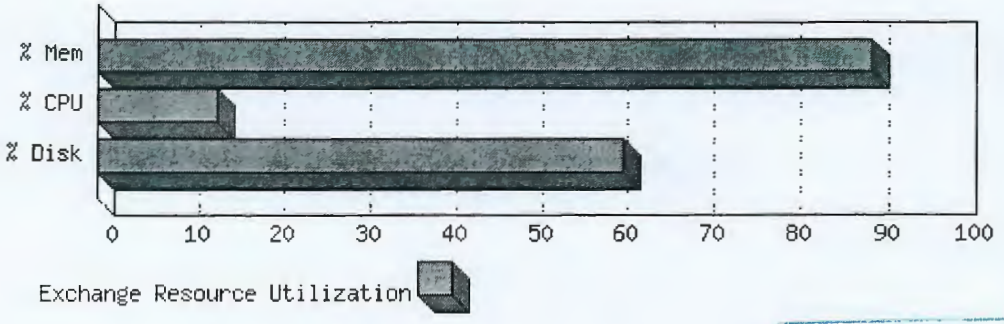


Figure 3-8: Exchange Footprint Summary

Server Performance

The Server Performance group provides performance metrics and counters for the core Exchange server including the information store, directory, MTA, and system attendant. These metrics include those useful for real-time management and longer-term capacity planning and trend analysis. Table 3-4 defines important Server Performance metrics.

Table 3-4: Selected MIB Objects – Exchange Server Performance Group (Page 1 of 2)

MIB Object	Description
xchgStoreUserCount	Current number of information store users/connections.
xchgMTAWorkQueueLen	Current number of messages waiting to be processed by the MTA.
xchgMTAAssoc	Current number of MTA-to-MTA associations.
xchgMTAMessages	Total number of messages sent and received by the MTA.
xchgISPubInMessages	Total number of public messages submitted to clients.
xchgISPubOutMessages	Total number of public messages delivered to recipients.
xchgISPubSendQueLen	Current length of the public message send queue.
xchgISPrivSendQueLen	Current length of the private message send queue.
xchgISPrivInMessages	Total number of private messages submitted to clients.
xchgISPrivOutMessages	Total number of private messages delivered to recipients.
xchgDirABbrowse	Number of address book browses processed by the Microsoft Exchange directory service. (Exchange 5.5 only; Exchange 2000 uses the Active Directory service.)
xchgDirABreads	Number of address book browses reads by the Microsoft Exchange directory service. (Exchange 5.5 only; Exchange 2000 uses the Active Directory service.)

Table 3-4: Selected MIB Objects – Exchange Server Performance Group (Page 2 of 2)

MIB Object	Description
xchgDirEXDSReads	Number of extended directory service client reads processed by this Exchange service. (Exchange 5.5 only; Exchange 2000 uses the Active Directory service.)
xchgDirReplUpdates	Number of replication updates processed by this Exchange server. (Exchange 5.5 only; Exchange 2000 uses the Active Directory service.)
xchgDirThreads	Number of directory threads currently allocated. (Exchange 5.5 only; Exchange 2000 uses the Active Directory service.)

Connector Performance

The Connector Performance group provides performance metrics and counters for Exchange connectors including the Internet Mail connector, Lotus Notes cc:Mail, and others. These metrics include those useful for real-time management and longer-term capacity planning and trend analysis. Table 3-5 defines important Connector Performance metrics.

Table 3-5: Selected MIB Objects – Exchange Connector Performance Group

MIB Object	Description
xchgMMCMTAMsgs	Total number of messages moved through the Microsoft Mail Connector.
xchgIMSInQueLen	Number of Internet messages awaiting delivery in the Exchange server. (Exchange 5.5 only; Exchange 2000 uses the IIS/SMTP service.)
xchgIMSOutQueLen	Number of messages awaiting conversion to Internet mail format. (Exchange 5.5 only; Exchange 2000 uses the IIS/SMTP service.)
xchgIMSTotQueLen	Total number of messages waiting in Internet Mail Service (IMS) queues. On Exchange 2000, this number represents the sum of the local and remote SMTP server queue lengths, plus the SMTP server local and remote retry queue lengths.

Table 3-5: Selected MIB Objects – Exchange Connector Performance Group

MIB Object	Description
xchgIMSTotalConn	Total number of successful Internet mail connections. On Exchange 2000, this object represents the sum of the SMTP server total incoming and outgoing connections.
xchgIMSQueOut	Number of messages waiting for delivery to the Internet. On Exchange 2000, this object represents the SMTP server local queue length.
xchgIMSTotalInMsgs	Total number of Internet messages delivered to Exchange. On Exchange 2000, this object represents the total number of messages received by the SMTP server.
xchgIMSTotalOutMsgs	Total number of outbound messages delivered to Exchange server. On Exchange 2000, this object represents the total number of messages sent by the SMTP server.
xchgCCMCQueIn	Number of messages in the cc:Mail connector queue awaiting delivery to Exchange.
xchgCCMCQueOut	Number of messages in Exchange awaiting delivery to cc:Mail connector.

Figure 3-9 shows a sample AdvantEDGE View Exchange 5.5 queue.

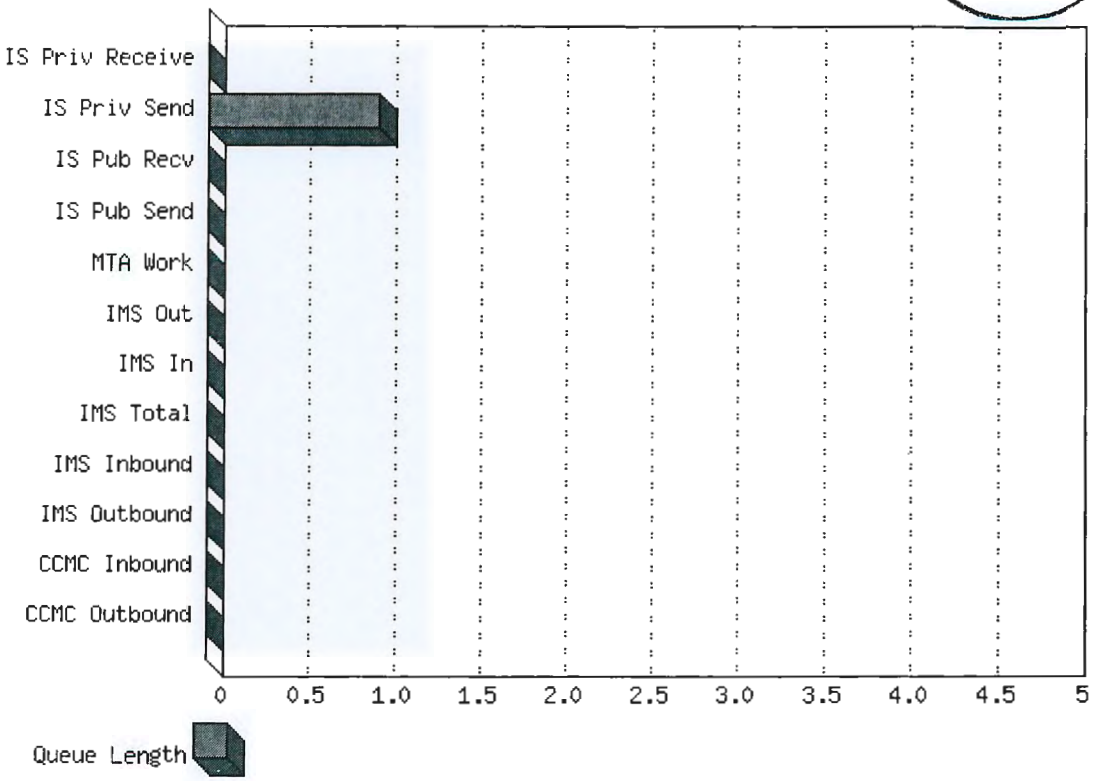


Figure 3-9: Exchange Queues for Exchange 5.5 Server

4 Using AdvantEDGE for Microsoft Exchange

This chapter describes how to configure and use AdvantEDGE for Microsoft Exchange. This Point module is implemented as a SystemEDGE plug-in. After you enable this Point module in the sysedge.cf file and license it, it will load automatically at SystemEDGE start time. For more information, refer to "Configuring AdvantEDGE for Microsoft Exchange" and "Licensing AdvantEDGE for Microsoft Exchange" on page 2-3.

The AdvantEDGE for Microsoft Exchange plug-in implements additional MIB objects that provide advanced information about the health and availability of the Microsoft Exchange groupware application. It can operate with any SNMP-compliant management software, such as Concord's *e*Health suite of products, AdvantEDGE View, HP OpenView, and others. If you are using AdvantEDGE for Microsoft Exchange with *e*Health, refer to the *e*Health Web Help for more information about the reports that are available.

The default configuration settings of the AdvantEDGE for Microsoft Exchange plug-in enable you to use the advanced self-monitoring capabilities of SystemEDGE in conjunction with AdvantEDGE for Microsoft Exchange.

Editing the SystemEDGE Configuration File

You can use AdvantEDGE View or another SNMP tool to edit the SystemEDGE configuration file to utilize the MIB objects found in AdvantEDGE for Microsoft Exchange with the process-monitoring, threshold-monitoring, Windows NT event-monitoring, and history-collection features of the SystemEDGE agent. All MIB objects that are related to AdvantEDGE for Microsoft Exchange exist at object identifier (OID) branch 1.3.6.1.4.1.546.16.1 in the Concord Systems Management MIB. The MIB is defined in the xchgmod.asn1 file, which is available in the AdvantEDGE for Microsoft Exchange product installation.

Assigning Entry Rows in the SystemEDGE Self-Monitoring Tables

All SystemEDGE self-monitoring tables (for example, log monitoring, Windows NT event monitoring, process/service monitoring, threshold monitoring, and history collection) require the use of unique row numbers. Each table contains an *Index* column which acts as a *key field* to distinguish rows in the table. This section describes the benefits of reserving a block of rows (somewhere in the range of 11 to the maximum number of rows in your table) for use by the system or application administrator.

Setting Local Policy

You may choose, as a matter of local policy, to reserve a block of rows for system administration. This policy allows you to define row entries within a reserved block of rows without worrying about the row already being taken by another user's entry. In compliance with the local policy, all other users should use row indices that are outside of the reserved range when they define user-configured entries.

By reserving a block of rows, you can define a consistent set of conditions (row entries) to be monitored across all machines such that the same condition is defined in the same row number on each of the machines. For example, you might use row 3000 in each table to define entries monitoring the Exchange MTA work queue length (xchgMTAWorkQueueLen). You can then distribute this configuration to every host so that every machine that is running Microsoft Exchange uses row 3000 for monitoring MTA work queue length, whether it is the threshold monitoring table or the history table. Further, every machine can also use row 3000 for monitoring the MTA service in the process/service monitoring table.

Reserving Blocks of Rows

To reserve a block of rows for monitoring Microsoft Exchange:

1. Decide on a block of rows that you want to reserve for your use with monitoring Microsoft Exchange.
2. Use that block of rows to define a set of row entries for each of the respective SystemEDGE self-monitoring tables. For more information, refer to the chapter on self-monitoring in the *SystemEDGE Agent User Guide*.

3. Distribute configuration file entries out to all hosts that are running Microsoft Exchange and AdvantEDGE for Microsoft Exchange. For more information, refer to the *Automating the Deployment of SystemEDGE and AdvantEDGE Point Plug-in Modules* white paper.

NOTE

As an alternative, you can use this row-number assignment policy with AdvantEDGE View for group configuration operations.

4. Require end-users to avoid your block of rows when defining their own self-monitoring table entries.

Using the SystemEDGE Self-Monitoring Features

The examples in this section show SystemEDGE configuration-file commands for monitoring Microsoft Exchange. Add these commands to the sysedge.cf file to enable monitoring of the MIB objects they specify. Modify these examples as necessary to monitor the MIB objects that are relevant for your configuration.

The examples in the following sections present row numbers in the 5000 range; select a row number for your configuration that conforms to local policies. For more information on row assignment, refer to "Assigning Entry Rows in the SystemEDGE Self-Monitoring Tables" on page 4-2.

The following command, for example, instructs the SystemEDGE agent to monitor whether the Exchange MTA process is alive every 30 seconds and to store the data in row 5000 of the Process Monitoring table:

```
watch process procAlive 'emsmta|EMSMTA' 5000 0x0 30
  'Exchange Dir' ''
```

For more information about the syntax for the commands in this section, refer to the *SystemEDGE Agent User Guide*.

NOTE

Enter the commands throughout this chapter on one line. Do **not** use a carriage return to match the formatting shown here.

Using SystemEDGE Process Monitoring

This section provides examples for monitoring the availability of critical Microsoft Exchange processes and services through SystemEDGE process and service monitoring. Enter the following commands in the sysedge.cf file to monitor these processes. For more information, refer to the chapter on process and service monitoring in the *SystemEDGE Agent User Guide*.

Monitoring the Exchange 5.5 Directory Service

To make sure the Exchange 5.5 Directory Service is running, enter the following command:

```
watch process procAlive 'dsamain|DSAMAIN' 5000 0x0 30
  'Exchange Dir' ''
```

Monitoring the Exchange MTA

To make sure the Exchange MTA is running, enter the following command:

```
watch process procAlive 'emsmta|EMSMTA' 5001 0x0 30 'Exchange
  MTA' ''
```

Monitoring the Exchange Information Store

To make sure the Exchange Information Store is running, enter the following command:

```
watch process procAlive 'store|STORE' 5002 0x0 30 'Exchange
  Info Store' ''
```

Monitoring the Exchange Attendant

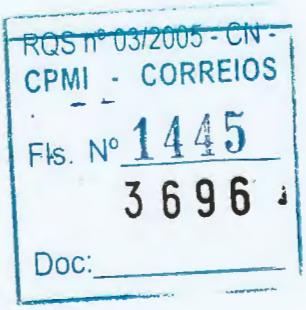
To make sure the Exchange Attendant is running, enter the following command:

```
watch process procAlive 'mad|MAD' 5003 0x0 30 'Exchange
  Attendant' ''
```

Monitoring the Exchange Event Service

To make sure the Exchange Event Service is running, enter the following command:

```
watch process procAlive 'events|EVENTS' 5004 0x0 30 'Exchange
  Event Service' ''
```



Monitoring the Exchange 2000 SMTP Service

To make sure the Exchange 2000 SMTP service is running, enter the following command:

```
watch process procAlive 'smtp|SMTP' 5005 0x0 30 'Exchange 2000
 SMTP Service' ''
```

Monitoring the Core IIS Service

To make sure the Core IIS Service is running, enter the following command:

```
watch process procAlive 'iis|IIS' 5006 0x0 30 'Core IIS
 Service' ''
```

Using SystemEDGE Threshold Monitoring

This section provides examples for monitoring important Exchange metrics through SystemEDGE threshold monitoring. Add the commands that are provided in the following sections to the sysedge.cf file to monitor thresholds for these MIB objects. For more information, refer to the chapter on threshold monitoring in the *SystemEDGE Agent User Guide*.

NOTE

The thresholds used in these examples may not be appropriate for your Microsoft Exchange server; select thresholds that are appropriate for your environment.

Monitoring the MTA Work Queue Length

To monitor MTA work queue length, enter the following command:

```
monitor oid xchgMTAWorkQueueLen.0 5002 0x0 60 absolute > 15
 'MTA Queue Len exceeds threshold' ''
```

Monitoring Messages Received by the MTA

To monitor the number of messages received by the MTA, enter the following command:

```
monitor oid xchgMTAInMessages.0 5003 0x0 60 delta > 35 'MTA
 In Messages exceeds threshold' ''
```

Monitoring Messages Sent by the MTA

To monitor the number of messages sent by the MTA, enter the following command:

```
monitor oid xchgMTAOutMessages.0 5004 0x0 60 delta > 35 'MTA
  Out Messages Exceeds threshold' ''
```

Monitoring Information Store Users

To monitor the number of Information Store users, enter the following command:

```
monitor oid xchgStoreUserCount.0 5005 0x0 60 absolute > 750
  'Store User Cnt exceeds threshold' ''
```

Monitoring Private Store Messages Submitted by Clients

To monitor the number of Private Store messages submitted by clients, enter the following command:

```
monitor oid xchgISPrivInMessages.0 5006 0x0 60 delta > 35
  'Priv Store In Msg crosses threshold' ''
```

Monitoring Private Store Messages Delivered to Recipients

To monitor the number of Private Store messages delivered to recipients, enter the following command:

```
monitor oid xchgISPrivOutMessages.0 5007 0x0 60 delta > 35
  'Priv Store Out Msg crosses threshold' ''
```

Monitoring SMTP Queue Length

To monitor the SMTP Queue Length, enter the following command:

```
monitor oid xchgIMSTotQueLen.0 5008 0x0 60 delta > 35 'SMTP
  Queue Length crosses threshold' ''
```

Using SystemEDGE History Collection

This section provides examples for tracking the value of important Microsoft Exchange metrics over time through SystemEDGE history collection. Add the commands in the following sections to the sysedge.cf file to collect history for these MIB objects. For more information, refer to the chapter on history collection in the *SystemEDGE Agent User Guide*.

NOTE

The number of samples and the interval between samples used in these examples may not be appropriate for your Microsoft Exchange server; choose values that are appropriate for your environment.

Collecting History for MTA Work Queue Length

To collect history for MTA work queue length, enter the following command:

```
emphistory 5002 60 xchgMTAWorkQueueLen.0 480 'MTA Queue Len
 History'
```

Figure 4-1 shows a sample AdvantEDGE View Exchange Work Queue Length History.

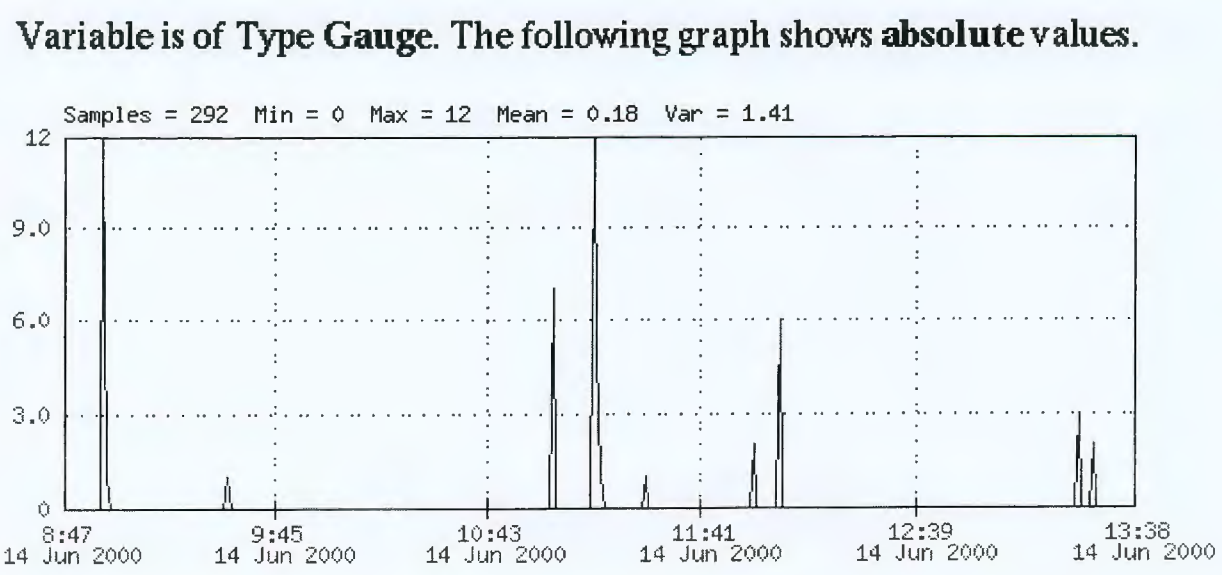


Figure 4-1: Exchange MTA Work Queue Length History

Collecting History for MTA Message Reception

To collect history for MTA message reception, enter the following command:

```
emphistory 5003 60 xchgMTAInMessages.0 180 'MTA In Messages
 History'
```

Collecting History for MTA Message Delivery

To collect history for MTA message delivery, enter the following command:

```
emphistory 5004 60 xchgMTAOutMessages.0 180 'MTA Out Messages
 History'
```

Collecting History for Information Store User Count

To collect history for the Information Store user count, enter the following command:

```
emphistory 5005 60 xchgStoreUserCount.0 120 'Store User Cnt
 History'
```

Figure 4-2 shows an AdvantEDGE View sample history for user count.

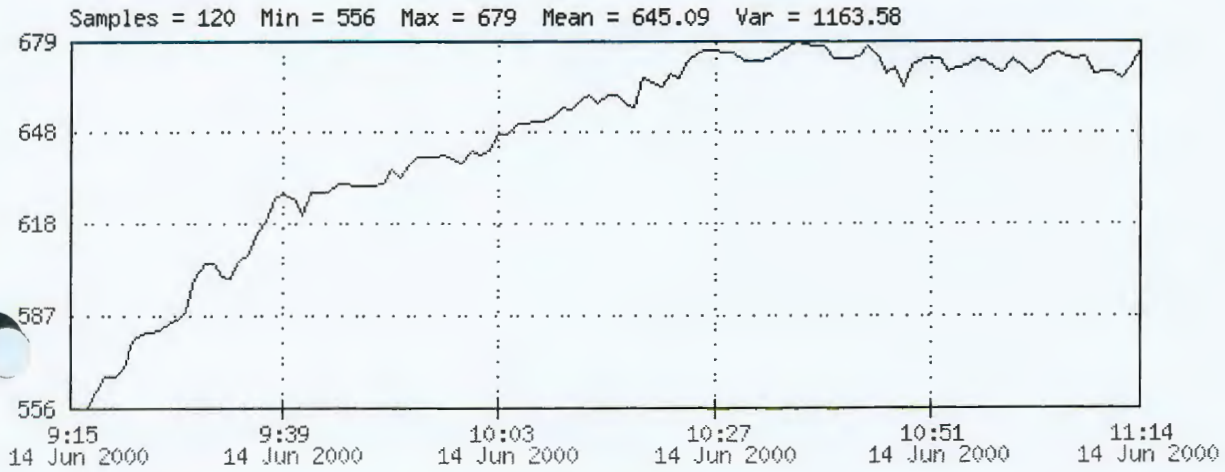


Figure 4-2: Sample History for Exchange User Count

Collecting History for Private Store Message Reception

To collect history for Private Store message reception, enter the following command:

```
emphistory 5006 60 xchgISPrivInMessages.0 120 'Priv Store In
 Msg History'
```

Collecting History for Private Store Message Delivery

To collect history for Private Store message delivery, enter the following command:

```
emphistory 5007 60 xchgISPrivOutMessages.0 120 'Priv Store
 Out Msg History'
```

Using SystemEDGE Windows NT Event Monitoring

This section provides examples for using the SystemEDGE Windows NT event-monitoring capabilities to capture important Microsoft Exchange-related Windows NT events and forward them to the appropriate configuration-management software as SNMP traps. Add the commands in the following sections to the sysedge.cf file to monitor these Windows NT events. For more information, refer to the chapter on Windows NT event monitoring in the *SystemEDGE Agent User Guide*.

Monitoring Exchange Events in the System Event Log

To watch for Exchange events in the system event log, enter the following command:

```
watch ntevent 5000 0x00 System All 'MSExchange' '.*'
 'Monitor Exchange System Events' ''
```

Monitoring Exchange Events in the Security Event Log

To watch for Exchange events in the security event log, enter the following command:

```
watch ntevent 5000 0x00 System All 'MSExchange' '.*'
 'Monitor Exchange Security Events' ''
```

Monitoring Exchange Events in the Application Event Log

To watch for Exchange events in the application event log, enter the following command:

```
watch ntevent 5000 0x00 System All 'MSExchange' '.*'
 'Monitor Exchange Application Events' ''
```

Monitoring Exchange Database Error Events in the System Event Log

To watch for Exchange database error events in the system event log, enter the following command:

```
watch ntevent 5003 0x00 System Error 'EDB' ' '.*' 'Monitor
  Exchange Database Events' ''
```

Monitoring Exchange Database Error Events in the Security Event Log

To watch for Exchange database error events in the security event log, enter the following command:

```
watch ntevent 5004 0x00 Security Error 'EDB' '.*' 'Monitor
  Exchange Database Events' ''
```

Monitoring Exchange Database Error Events in the Application Event Log

To watch for Exchange database error events in the application event log, enter the following command:

```
watch ntevent 5005 0x00 Application Error 'EDB' '.*' 'Monitor
  Exchange Database Events' ''
```

Index

Manual 34
Notebook

IBM ThinkPad G40

O ThinkPad G40 é perfeito para quem está acostumado com um computador desktop, mas deseja ter a flexibilidade de trabalhar fora do escritório. Possui um preço bastante atraente e já vem equipado com um poderoso processador Intel® Pentium® ou um Intel® Celeron™, 4 portas USB além de uma unidade de disquete e uma unidade ótica já integradas ao conjunto.

CARACTERÍSTICAS PRINCIPAIS

Modelo	2388-BP2
Sistema Operacional	Microsoft Windows XP Pro
Processador	Intel® Pentium® 4 2.4GHz
Tela	Tela matriz ativa TFT de 14.1 polegadas XGA (1024 x 768)
Disco Rígido	40GB
Unidade ótica	DVD-ROM 8X
Memória	256MB DDR-SDRAM
Teclado	Confortável, tamanho padrão com *Palm Rest* e botão *Access IBM*
Dispositivo Apontador	*TrackPoint* pointing com "Press-to-Select"
Modem	56K V.90
Rede	Ethernet 10/100

VANTAGENS

O novo ***IBM ThinkPad G40*** é a melhor alternativa para a substituição do PC tradicional pois combina, em um único gabinete, o conforto e poder de um desktop com o design e portabilidade de um notebook *IBM ThinkPad*. Ele foi desenhado para usuários que necessitam de um computador completo que ofereça mobilidade ocasional e, por isso, é perfeito para quem está acostumado com um computador desktop mas deseja ter a flexibilidade de trabalhar fora do escritório.

O ***IBM ThinkPad G40*** também incorporou todos os elementos que os usuários de notebooks mais experientes esperam da IBM.

Detalhes inteligentes que fazem toda a diferença.

Dentre os notebooks disponíveis no mercado, o ***IBM ThinkPad G40*** está entre os mais resistentes, seguros, confortáveis e fáceis de usar.

A nova família ***IBM ThinkPad G40*** oferece excelentes telas de cristal líquido com ampla área de visualização, gabinete e painel reforçados com dobradiças de aço, 4 portas USB, placa de vídeo integrada *Intel Extreme Graphics* com até 32MB de memória e a reconhecida ergonomia presente em toda a linha de notebooks *IBM ThinkPad* que, adicionalmente para esta nova família, apresenta as seguintes inovações:

- Teclado ***"ComfortSlant"*** - com teclas para controle do volume e botão *"Access IBM"*, para rápido acesso à todas as unções e informações que o usuário necessita. Possui um excelente apoio para as mãos (palm rest) e uma inclinação ergonômica que o torna ainda mais confortável.

- Apoio ***"Easy Pivot"*** - um ponto de apoio fixo que permite a fácil rotação do equipamento na mesa para ajustes de posicionamento.

- Dispositivo apontador ***"TrackPoint"*** com o recurso *"Press-to-Select"* (aperte para selecionar) e com três opções de revestimento cuidadosamente elaborados para oferecer o máximo de conforto e precisão, dependento da preferência do usuário:

Classic Dome

Soft Dome

Soft Rim

Melhor tecnologia por um preço acessível.

A IBM está comprometida a reduzir o tempo e dinheiro gastos na instalação de computadores, manutenção, inventário e reposição. A IBM combina tecnologias de alto desempenho com gerenciamento de sistemas de ponta e recursos de proteção ao investimento.

Um bom exemplo disso é o botão ***Access IBM***, um *"portal para o suporte IBM"*, que aproveita um rico conjunto de recursos internos, ferramentas de diagnósticos, soluções automatizadas e links para atualizações e serviços on-line.

Também podemos citar as vantagens da ferramenta ***Rapid Restore PC*** que oferece uma solução de backup inteligente com armazenamento de dados do usuário, aplicações e configurações críticas do sistema operacional em uma partição protegida do disco rígido, possibilitando a fácil recuperação destas informações (até mesmo em sistemas com problemas ou que não conseguem inicializar).

Tanto o ***Access IBM*** como o ***Rapid Restore PC*** ajudam a diminuir o tempo de paradas de sistemas, maximizando a produtividade e contribuindo para a redução dos altos custos de suporte técnico.

CONECTIVIDADE

Os recursos de comunicação convenientemente agregados ao ***IBM ThinkPad G40*** permitem fácil e rápida conexão onde quer que você esteja. Opcionais podem ser adicionados via slot *PCMCIA*.

- **Portas Padrão -** Quatro Portas **USB v.2.0**, uma porta paralela e uma PS/2.
- **Modem** - Modem de 56Kbps V.90 permite rápida conexão via linha discada para mantê-lo sempre conectado onde você estiver, trabalhando ou viajando.
- **Ethernet** - Rede Ethernet de 10/100 com PXE e Wake-on-LAN.

CONFIABILIDADE

Só o *ThinkPad* tem a garantia e a confiabilidade da IBM, que foi a pioneira na prestação de serviços para computadores portáteis no Brasil.

- **Suporte Técnico** - Suporte telefônico oferecido pelo ***HelpCenter*** grátis por **30** dias após a 1° ligação para o *SOFTWARE* pré-carregado, e para determinação de problemas de *HARDWARE* durante o período de garantia.
- **(*)EasyServ** - Um serviço inédito e exclusivo, com 98% de clientes satisfeitos, que utiliza um *courier* para retirar e entregar o *ThinkPad* a ser restaurado pela Central de Reparos da própria IBM. O *EasyServ* encontra-se disponível, gratuitamente, para pessoas jurídicas emitentes de nota fiscal, durante a vigência da Garantia.

DESCRIÇÃO TÉCNICA DETALHADA

Modelo	2388-BP2
Sistema Operacional	Microsoft Windows XP Pro
Processador	Intel® Pentium® 4 2.4GHz
Cache L2	512KB onboard (na velocidade do processador)
Memória	256MB DDR-SDRAM
Disco Rígido Padrão	40GB
Unidade ótica	DVD-ROM 8X
Disco Flexível	3.5" 1.44MB fixo
Tela	Tela matriz ativa TFT de 14.1" polegadas XGA (1024 x 768)
Dispositivo Apontador	TrackPoint pointing com "Press-to-Select"
Controladora de Video	Intel Extreme Graphics / Direct AGP / 8 a 32 MB DDR-SDRAM
Bateria	Lithium Ion 6-cell - inteligente
Bateria - Duração	1,75 hora
Bateria - Tempo de Carga	De 3 a 6 horas, dependendo da utilização
Áudio	AC97
Modem	56K V.90
Rede	Ethernet 10/100
Portas	4 USB v.2.0, 1 paralela, 1 DB-15 para monitor externo, 1 RJ-11 (modem), 1 RJ-45 (ethernet), 1 PS/2 (teclado/mouse)
Dimensões aprox.	Largura: 32,9cm Profundidade: 28,2cm Espessura: 3,71 (frente) – 5,09cm (atrás)
Peso aproximado	3,46Kg
Soquetes de memória	2 soquetes SO-DIMM (1 soquete livre)
Slots PCMCIA	1 slot (tipo I, II ou III)
Slot Mini-PCI	Não
Security Chip	Não
Garantia	**1 (um) ano** com o serviço e suporte **IBM EasyServ(*)**

SOFTWARE PRÉ-INSTALADO

2388-BP2
Microsoft Windows XP Pro em Português
Access IBM
Access Connections
Adobe Acrobat Reader
IBM Rapid Restore PC
PC Doctor
ThinkPad Utilities
IBM Update Connector
Disk-to-disk recovery

OPCIONAIS COMPATÍVEIS

Opcional	Part Number
Memórias:	
128 MB Memory DDR-SDRAM SO DIMM PC2100 266MHz	10K0028
256 MB Memory DDR-SDRAM SO DIMM PC2100 266MHz	10K0030
512 MB Memory DDR-SDRAM SO DIMM PC2100 266MHz	10K0032
Armazenamento:	
HD 20GB	08K9686
HD 40GB	08K9816
HD 60GB	08K9688
HD 80GB	08K9869
HD 20 GB portátil USB 2.0	09N4211
CD-RW 8X4X24X externo USB	22P5297
IBM Microdrive 1 GB	07N5574
Chaveiro - Memory Key 64MB USB 2.0	22P9024
Chaveiro - Memory Key 256MB USB 2.0	22P9025
Fontes de energia:	
Bateria de Li-ion p/ TP G40	08K8178
AC Adapter 120W p/ ThinkPad G40	22P9161
Rede:	
PC Card 16/4 Token-Ring	34L1401
CardBus 16/4 Token-Ring	34L4801
Acessórios:	
ThinkPad Monitor Stand	22P5265
Mini Scroll Point Mouse 800dpi Black Pro para Mini-Din/USB	31P7410
Teclado Português USB com hub de 2 portas preto	10K3852
Teclado Inglês USB com hub de 2 portas preto	10K3849
Wireless:	
IBM H Rate Wireless LAN PC Card 128	09N9904
IBM H R Wireless LAN Access Point 500	09N9906
Malas:	
Maleta de couro Targus para ThinkPad	10K0209
Maleta de nylon Targus para ThinkPad	10K0207

PREÇOS

Modelo	**Street Price* R$**
2388-BP2	Consulte
Maleta PCC0017	Consulte

ThinkPad Marketing Team - Brasil

Manual 35

www.concord.com

concord | applications systems networks

contact us site index login

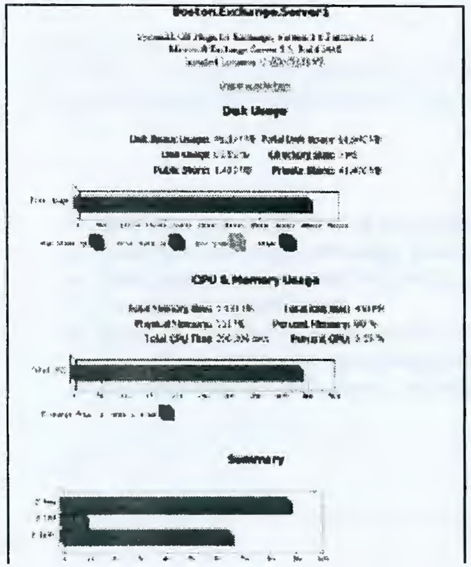
solution fast finder | solutions & services | support | partners | news & events | about us | careers | search

Home > Solutions > eHealth application insight module for Microsoft Exchange

eHealth Application Insight Module for Microsoft® Exchange

Product Quick List

eHealth application insight module for Microsoft Exchange is a plugin module that extends the functionality of *e*Health SystemEDGE by adding the capability to monitor and manage the Microsoft Exchange groupware application. Management functions are distributed out to the host system, helping you free up Exchange administrators to focus on more value-added initiatives. With *e*Health SystemEDGE's automatic local corrective action, you can now fix problems before your e-mail users - and your business - are affected.



Real-time queries, like the Exchange Footprint shown here, identify CPU, disk, and memory shortages that can affect your application's performance.

Contact

- **I'm interested** - Call me!

Resources

- Product Demo
- Download Data Sheet
- Request an Evaluation
- Current Evaluation Accounts
- Content Guide (pdf)

Don't have Acrobat Reader?

Download it for free now! Get Acrobat Reader

Certified

Microsoft CERTIFIED Partner

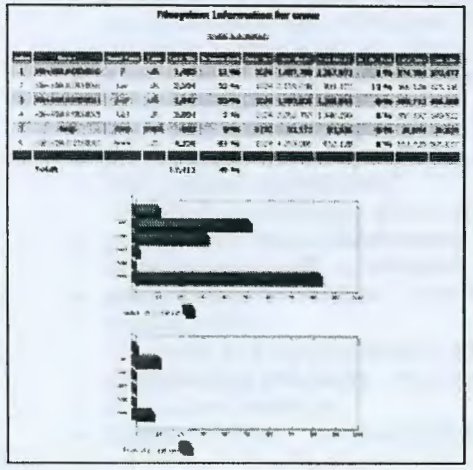
- Delivers real-time problem detection and self-healing corrective action for Microsoft Exchange
- Ensures maximum uptime and performance of business-critical e-mail services
- Improves service, and productivity through faster e-mail
- Identifies potential security breaches and vulnerabilities
- Reduces the total cost of ownership associated with Microsoft Exchange

Questions/Comments:info@concord.com or call (800) 851-8725

eHealth®—SystemEDGE

Product Quick List

With SystemEDGE agents, system administrators can distribute tedious management tasks away from overworked staff and down to the host systems - closest to where problems occur. SystemEDGE operates autonomously on a host workstation or server, continuously monitoring changing conditions and providing detailed information about the host's configuration, status, performance, users, applications, file systems, and other critical resources. SystemEDGE's real-time self-monitoring quickly detects system problems and automatically fixes them with pre-defined actions. SystemEDGE enables operators to fix problems before they impact users, free up valuable IT human resources, maximize ROI, and minimize costs.



eHealth SystemEDGE provides quick at-a-glance reports on systems and applications, disk and file system statistics, hardware/software inventories, and more.

Features

Contact

I'm interested - Call me!

Resources

- eHealth AdvantEDGE View
- eHealth Console
- eHealth—Live Health Fault Manager

Resources

- Product Demo
- Download Data Sheet (English)
- Download Data Sheet (French)
- Download Data Sheet (German)
- Request an Evaluation
- Current Evaluation Accounts
- Content Guide (pdf)

Don't have Acrobat Reader?

Download it for free now! Get Adobe Acrobat Reader

Certified

DELL

Microsoft CERTIFIED Partner

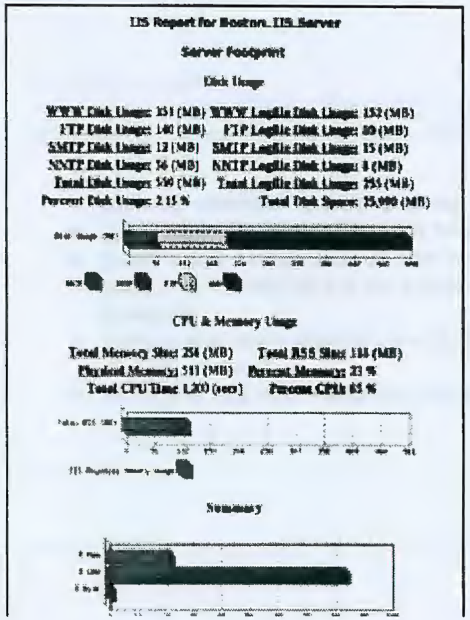
- **SNMP support** - SystemEDGE is a pure SNMP agent; no proprietary protocols
- **Lightweight footprint** - with an average of < 1% CPU utilization and ~3MB memory, SystemEDGE has negligible system impact
- **Multi-platform support** - SystemEDGE works seamlessly across a wide range of operating systems and platforms
- **Distributed self-management** - push work out to self-managing SystemEDGE agents throughout your distributed client-server environment
- **Scaleable** -automated management enables you to scale to managing thousands of clients workstations and servers using existing IT staff
- **Extensible** - extend with *e*Health application insight modules, or add your own custom MIB variables to add SNMP management capabilities for homegrown applications
- **Out of the box value** - SystemEDGE installs quickly with minimal administrative footprint to deliver immediate value
- **Complement existing tools** - SystemEDGE provides information and can send industry standard SNMP traps to any SNMP-compliant network management station (NMS), enabling you to preserve your existing operational workflow and investment in other management software
- **Standalone or integrated with eHealth** - SystemEDGE is available as a standalone solution or as part of a comprehensive *e*Health solution

Questions/Comments:info@concord.com or call (800) 851-8725

eHealth® Application Insight Module for Microsoft® IIS

Product Quick List

eHealth application insight module (AIM) for Microsoft IIS is a plugin module that extends the functionality of eHealth SystemEDGE by adding the capability to monitor and manage the Microsoft IIS application. AIM for IIS delivers maximum availability and performance of Microsoft IIS by detecting problems in real-time, tracking usage statistics, and monitoring the impact on system resources.



The eHealth application insight module for Microsoft IIS provides real-time performance and fault management for Microsoft IIS, 24x7, from a web browser.

Contact

I'm interested - Call me!

Resources

- Product Demo
- Download Data Sheet
- Request an Evaluation
- Current Evaluation Accounts
- Content Guide (pdf)

Don't have Acrobat Reader?

Download it for free now!

Get Acrobat Reader

Certified

Microsoft CERTIFIED Partner

Features

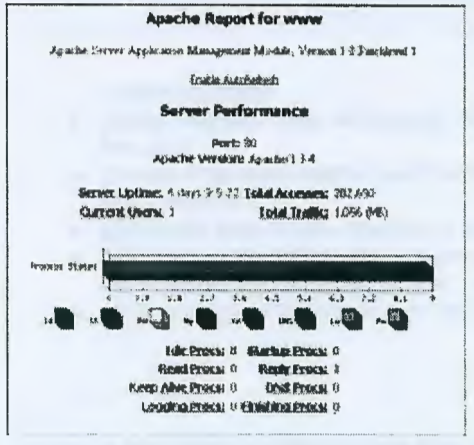
- Proactive self-management frees up IT personnel, keeps IIS up and running
- Ensure sufficient system resources with proactive capacity planning
- Meet and exceed SLA's for hosted and managed sites
- Reduce the overall cost to manage your IIS environment
- Real-time fault detection and self-healing corrective action through scalable, distributed self management

Questions/Comments:info@concord.com or call (800) 851-8725

eHealth® Application Insight Module for Apache

Product Quick List

Despite the pervasive use and reliance on Apache software by today's biggest Internet movers and shakers, minimal attention is spent addressing performance and availability issues. Small periods of downtime and subtle brownouts quickly result in financial penalties and failure to comply with service level agreements. With this in mind, Concord offers a self-managing solution for ensuring the health and availability of distributed Apache web server environments.



Distributed, self-managing agents automatically manage Apache performance, availability, and configuration. Apache server performance is shown here monitoring for sudden changes in traffic activity.

Management functions are distributed out to the host system, helping you to free up Web administrators to focus on more strategic activities. Leveraging management-by-exception technology, eHealth AIM for Apache continuously monitors Apache

Contact

I'm interested - Call me!

Resources

- Product Demo
- Download Data Sheet
- Request an Evaluation
- Current Evaluation Accounts
- Content Guide (pdf)

Don't have Acrobat Reader?

Download it for free now! Get Acrobat Reader

technology, eHealth AIM for Apache continuously monitors Apache services and system resources, alerting you only when something requires your attention. Whether you alert a staff member or have eHealth SystemEDGE initiate automatic, local corrective action, you can now fix problems before users and your business are affected.

Features

- Real-time fault detection and self-healing corrective action for mission-critical Apache Web servers
- Scalable, distributed, self management frees up IT resources
- Eliminate web server downtime and optimize Apache performance
- Ensure sufficient system resources with proactive capacity planning
- Lower support costs associated with managing your Apache implementation

Questions/Comments: info@concord.com or call (800) 851-8725

concord | applications systems networks

contact us | site index | login

solution fast finder | solutions & services | support | partners | news & events | about us | careers | search

Home > Solutions > eHealth application insight module for Oracle

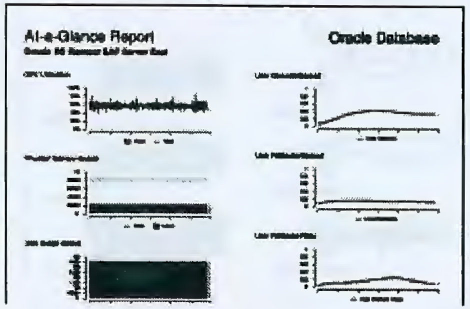
eHealth® Application Insight Module for Oracle®

Product Quick List

Database Administrators and Systems Managers need a reliable solution to ensure that databases are available and delivering strong performance - eHealth Aim for Oracle delivers on that need. eHealth AIM for Oracle extends the functionality of eHealth SystemEDGE by adding the capability to monitor and manage Oracle RDBMSs. Employing management-by-exception technology, eHealth AIM for Oracle only alerts IT staff when a problem requires their attention, and takes automated corrective actions to resolve problems.

eHealth AIM for Oracle also integrates with Concord's eHealth Live Health for detection of faults, potential outages, and brownouts across the entire IT infrastructure. With eHealth Live Health, database staff can

- Identify peculiar behavior patterns
- Improve SQL efficiency
- Identify transaction bottlenecks
- Eliminate brownouts before they lead to database failures



Oracle faults and potential outages are detected in real-time and historical reports ease troubleshooting and increase IT staff efficiency. The At-a-Glance report, shown here, correlates key database metrics on a single page over time to isolate database

Contact

I'm interested - Call me!

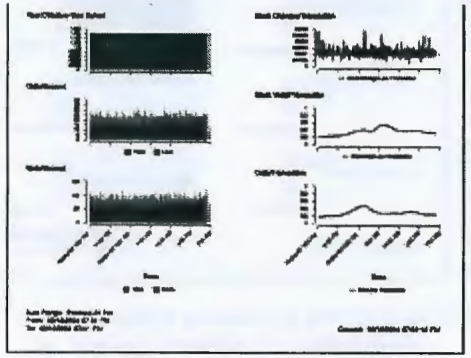
Resources

- Download Data Sheet
- Request an Evaluation
- Current Evaluation Accounts
- Content Guide (pdf)

Don't have Acrobat Reader?

Download it for free now!

Get Acrobat Reader



hotspots.

Features

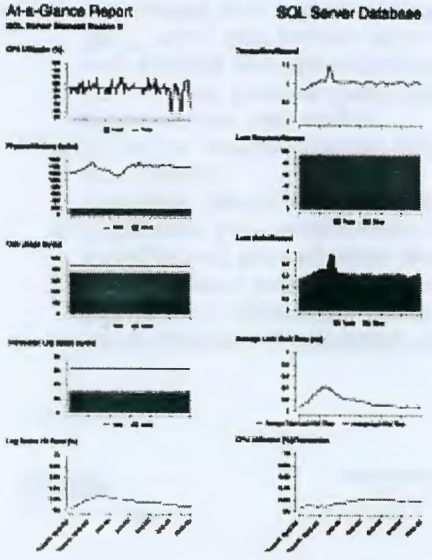
- Distributed self-management for a truly scalable applications management
- Ensure continuous scalability and automatically re-start Oracle database processes upon failure
- Establish automated monitoring for over 300 Oracle performance metrics spanning Oracle re-do logs, SQL statement efficiency, rollback segments, System Global Area (SGA), waits, tablespaces, and locks
- Extensible architecture can take unlimited corrective actions based on your own scripts
- Maintain your existing workflow with industry standard SNMP that integrates with your existing operational environment
- Fault, availability, and performance management across the entire IT infrastructure with *e*Health Suite's end-to-end integration

Benefits
Guarantee database uptime, performance, and reliability
Leverage limited IT resources by automating database management
Ensure that your database keeps up with changing business trends
Improve customer satisfaction and deliver the best possible user experience

eHealth® Application Insight Module for Microsoft® SQL Server

Product Quick List

SQL DBAs face the ongoing challenge of ensuring database uptime and optimal performance. Without the right set of tools, time will be spent reacting to fires instead of proactively ensuring a superior customer experience. eHealth application insight module (AIM) for Microsoft SQL Server offers fault and event management, proactive alarm notification, and the ability to fix problems automatically without the need for human intervention. And with seamless access to historical content, capacity planning and long term trend analysis are easier and more automated than ever before.



Automatically detect SQL Server faults and events, take corrective actions, and access integrated performance reports for rapid problem resolution.

Contact

► **I'm interested** - Call me!

Resources

- Product Demo
- Download Data Sheet
- Request an Evaluation
- Current Evaluation Accounts
- Content Guide (pdf)

Don't have Acrobat Reader?

Download it for free now! Get Adobe Acrobat Reader

Certified

Microsoft CERTIFIED Partner

Features

- SNMP Support—SystemEDGE is a pure standards-based SNMP agent, lightweight footprint, with an average of < 1% CPU utilization and 5MB memory, your SQL Server database management has negligible system impact
- Distributed Self-management—push work down to self-managing agents across your database and systems environment
- Extensible architecture can take unlimited corrective actions based on your own scripts
- Complement Existing Tools—integrate SystemEDGE with your existing operations tools by sending industry-standard SNMP traps. Add value to your current investment while maintaining your existing workflow
- Standalone or Integrated Solution—deploy a standalone SQL Server management solution or integrate with the eHealth Suite for complete end-to-end IT management

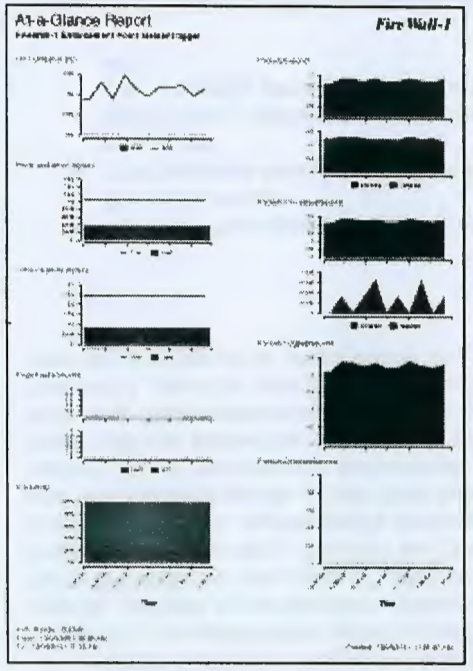
Benefits
Establish automated monitoring for SQL Server performance metrics including lock requests, access methods, transaction log activity, memory utilization, SQL efficiency, buffer efficiency, and user logon activity.
Access database configuration information in real-time, as well as track hardware and software assets for the underlying host system.
Monitor and restart failed SQL Server processes and services to ensure maximum uptime.
Watch SQL Server log files for regular text expressions that may indicate security or user violations, as well as application and system events.

Questions/Comments: info@concord.com or call (800) 851-8725

eHealth® Application Insight Module for Check Point® Firewall-1®

Product Quick List

Concord offers the only fully integrated solution for managing fault, performance, and availability across the entire internet infrastructure including applications, systems, networks, and now firewalls.



Concord's eHealth solution for FireWall-1 combines real-time fault and performance management with an integrated historical perspective. Using the At-A-Glance report (shown here), eHealth automatically correlates and isolates problem areas when faults of suspicious activities are encountered.

Contact

I'm interested - Call me!

Resources

- Download Data Sheet
- Request an Evaluation
- Current Evaluation Accounts
- Content Guide (pdf)

Don't have Acrobat Reader?

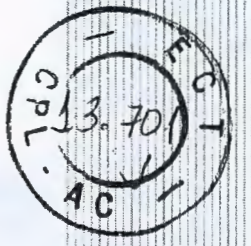
Download it for free now! Get Adobe Acrobat Reader

The eHealth application insight module (AIM) for Check Point FireWall-1, in combination with Concord's eHealth SystemEDGE agents, delivers comprehensive, proactive management of Check Point FireWall-1 to ensure availability and performance of mission critical firewall services. The AIM for Check Point FireWall-1 deploys quickly and easily, automatically discovering management servers and enforcement points. It can then automatically monitor firewall status, detect performance bottlenecks, identify suspicious traffic flows that can jeopardize the security of your organization, and automate fault notification. With the eHealth AIM for Check Point FireWall-1, you can identify security and performance issues before they have a chance to wreak havoc on your business.

Features

- Footprint Management ensures adequate system capacity for firewall services
- Configuration Management for troubleshooting and problem resolution
- Performance Management detects potential Denial of Service (DoS) attacks through industry-standard SNMP and OPSEC API's

Benefits
Ensure firewall availability with automated failure detection and correction
Automatic identification and notification of faults and suspicious firewall or network activity
Maximize firewall availability, performance, and security
Lower IT costs through consolidated management of security infrastructure with applications, systems, and networks

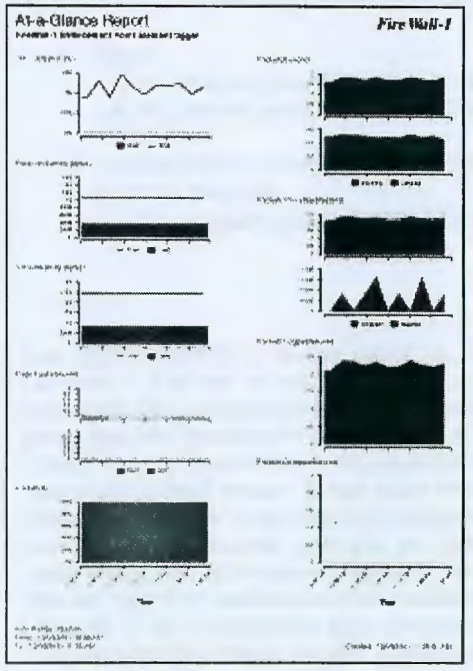


Questions/Comments:info@concord.com or call (800) 851-8725

eHealth® Application Insight Module for Check Point™ Firewall-1®

Product Quick List

Concord offers the only fully integrated solution for managing fault, performance, and availability across the entire internet infrastructure including applications, systems, networks, and now firewalls.



Concord's eHealth solution for FireWall-1 combines real-time fault and performance management with an integrated historical perspective. Using the At-A-Glance report (shown here), eHealth automatically correlates and isolates problem areas when faults of suspicious activities are encountered.

Contact

I'm interested - Call me!

Resources

- Download Data Sheet
- Request an Evaluation
- Current Evaluation Accounts
- Content Guide (pdf)

Don't have Acrobat Reader?

Download it for free now! Get Adobe Acrobat Reader

The eHealth application insight module (AIM) for Check Point FireWall-1, in combination with Concord's eHealth SystemEDGE agents, delivers comprehensive, proactive management of Check Point FireWall-1 to ensure availability and performance of mission critical firewall services. The AIM for Check Point FireWall-1 deploys quickly and easily, automatically discovering management servers and enforcement points. It can then automatically monitor firewall status, detect performance bottlenecks, identify suspicious traffic flows that can jeopardize the security of your organization, and automate fault notification. With the eHealth AIM for Check Point FireWall-1, you can identify security and performance issues before they have a chance to wreak havoc on your business.

Features

- Footprint Management ensures adequate system capacity for firewall services
- Configuration Management for troubleshooting and problem resolution
- Performance Management detects potential Denial of Service (DoS) attacks through industry-standard SNMP and OPSEC API's

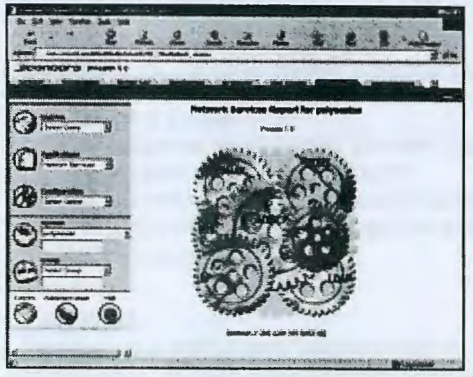
Benefits
Ensure firewall availability with automated failure detection and correction
Automatic identification and notification of faults and suspicious firewall or network activity
Maximize firewall availability, performance, and security
Lower IT costs through consolidated management of security infrastructure with applications, systems, and networks

Questions/Comments:info@concord.com or call (800) 851-8725

eHealth® Application Insight Module for Network Services (UNIX)

Product Quick List

Business applications and processes rely on underlying network services like Sendmail, LDAP, DHCP and DNS. When these mission critical services are unavailable or performing poorly, they can bring business activities to a halt, affecting end user productivity, revenue, and customer satisfaction. Concord's eHealth application insight module (AIM) for Network Services [UNIX] ensures the health and performance of your underlying infrastructure so your revenue-generating services go un-interrupted.



The eHealth AIM for Network Services [UNIX] provides users with automated management and reporting for a variety of mission critical applications.

The eHealth AIM for Network Services [UNIX] works with eHealth SystemEDGE agents to proactively detect, isolate, and correct service failures and bottlenecks before end users are affected.

The eHealth AIM for Network Services [UNIX] can be used alongside eHealth Service Availability to perform continuous, active tests for

Contact

I'm interested - Call me!

Resources

- Download Data Sheet
- Request an Evaluation
- Current Evaluation Accounts
- Content Guide (pdf)

Don't have Acrobat Reader?

Download it for free now! Get Acrobat Reader

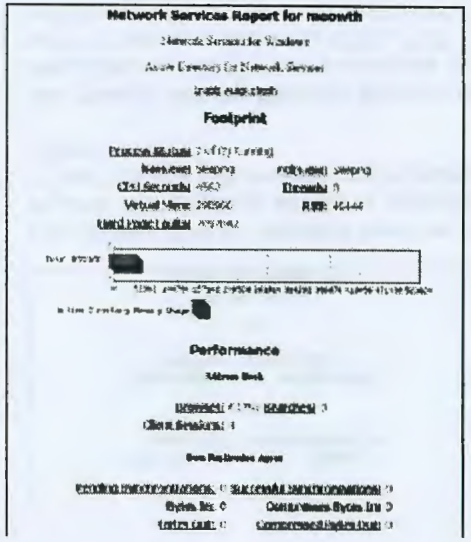
services like DNS, SMTP, POP3, PING, TCP Connect and more. This combined approach ensures availability from both the back-end servers, as well as the end-user perspective - minimizing impact on the business.

Benefits
Ensure availability and performance of critical network services including: • Sendmail • Lightweight Directory Access Protocol (LDAP) • Dynamic Host Configuration Protocol (DHCP) • Network File System (NFS) • Network Information Service (NIS) • Line Printer (LP)
Ensure availability of critical network services with automated failure detection and correction
Detect performance bottlenecks before service outages occur
Automate fault notification through integration with eHealth Fault Manager and 3rd party tools
Lower IT costs through consolidated management of applications, systems and networks

eHealth Application Insight Module for Network Services (Windows)

Product Quick List

Business applications and processes rely on underlying network services like Active Directory, WINS, DNS, and DHCP. When these mission critical services are unavailable or performing poorly, they can bring business activities to a halt, affecting end user productivity, revenue, and customer satisfaction. Concord's eHealth application insight module (AIM) for Network Services (Windows) ensures the health and performance of your underlying infrastructure so your revenue-generating services go un-interrupted.



The eHealth AIM for Network Services (Windows) provides users with automated management and reporting for a variety of mission critical applications.

Contact

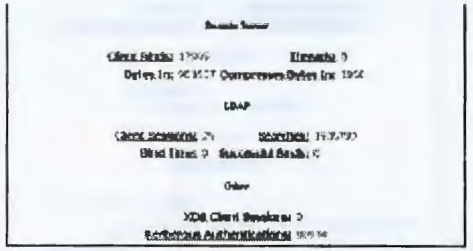
I'm interested - Call me!

Resources

- Download Data Sheet
- Request an Evaluation
- Current Evaluation Accounts
- Content Guide (pdf)

Don't have Acrobat Reader?

Download it for free now! Get Acrobat Reader



The *e*Health AIM for Network Services (Windows) works with *e*Health SystemEDGE agents to proactively detect, isolate, and correct service failures and bottlenecks before end users are affected.

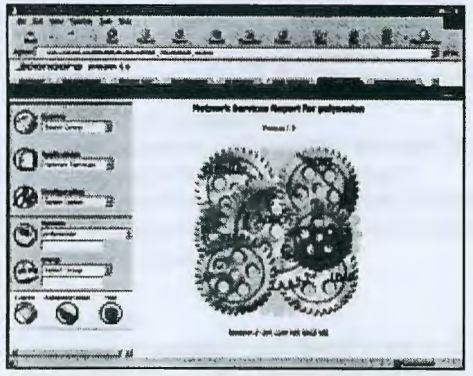
The *e*Health AIM for Network Services (Windows) can be used alongside *e*Health Service Availability to perform continuous, active tests for services like DNS, PING, TCP Connect and more. This combined approach ensures availability from both the back-end servers, as well as the end-user perspective - minimizing impact on the business.

Benefits
Ensure availability and performance of critical network services including: • Active Directory • Windows Internet Naming Service (WINS) • Dynamic Host Configuration Protocol (DHCP) • Domain Name Server (DNS)
Ensure availability of critical network services with automated failure detection and correction
Detect performance bottlenecks before service outages occur
Automate fault notification through integration with eHealth Fault Manager and 3rd party tools
Lower IT costs through consolidated management of applications, systems and networks

eHealth - Application Insight Module for Network Services (UNIX)

Product Quick List

Business applications and processes rely on underlying network services like Sendmail, LDAP, DHCP and DNS. When these mission critical services are unavailable or performing poorly, they can bring business activities to a halt, affecting end user productivity, revenue, and customer satisfaction. Concord's eHealth application insight module (AIM) for Network Services [UNIX] ensures the health and performance of your underlying infrastructure so your revenue-generating services go un-interrupted.



The eHealth AIM for Network Services [UNIX] provides users with automated management and reporting for a variety of mission critical applications.

The eHealth AIM for Network Services [UNIX] works with eHealth SystemEDGE agents to proactively detect, isolate, and correct service failures and bottlenecks before end users are affected.

The eHealth AIM for Network Services [UNIX] can be used alongside eHealth Service Availability to perform continuous, active tests for

Contact

I'm interested - Call me!

Resources

- Download Data Sheet
- Request an Evaluation
- Current Evaluation Accounts
- Content Guide (pdf)

Don't have Acrobat Reader?

Download it for free now! Get Adobe Acrobat Reader

services like DNS, SMTP, POP3, PING, TCP Connect and more. This combined approach ensures availability from both the back-end servers, as well as the end-user perspective - minimizing impact on the business.

Benefits
Ensure availability and performance of critical network services including: • Sendmail • Lightweight Directory Access Protocol (LDAP) • Dynamic Host Configuration Protocol (DHCP) • Network File System (NFS) • Network Information Service (NIS) • Line Printer (LP)
Ensure availability of critical network services with automated failure detection and correction
Detect performance bottlenecks before service outages occur
Automate fault notification through integration with eHealth Fault Manager and 3rd party tools
Lower IT costs through consolidated management of applications, systems and networks

Manual 36

IBM Tivoli Storage Manager for Windows - Quick Start

IBM Tivoli Storage Manager
for Windows

Quick Start

Version 5 Release 2

GC32-0784-01

Chapter 1. Introducing IBM Tivoli Storage Manager

IBM Tivoli Storage Manager provides automated, policy-based, distributed data and storage management for file servers and workstations in an enterprise network environment. The base functions provided by Tivoli Storage Manager include:

Backup and Restore:

The backup process creates a copy of the file or application data that can be recovered if the original data is lost or destroyed. Unlike other backup applications, Tivoli Storage Manager implements a *progressive backup methodology* to move data quickly and reliably. Using progressive backup, the number of file versions maintained by Tivoli Storage Manager and the length of time they are retained can be specified by the storage administrator. Refer to "Common Backup Methodologies" on page 6 for more information.

Backups can be scheduled, performed manually from the Tivoli Storage Manager client interface, or performed remotely using a Web-based interface.

The restore process transfers a backup data copy from Tivoli Storage Manager server-managed storage onto a designated machine.

Archive and Retrieval:

The archive process creates a copy of a file or a set of files and stores it as a unique object for a specified period of time. This function is useful for maintaining copies of vital records for historical purposes.

Like the backup process, the archive process can be scheduled, performed manually from the Tivoli Storage Manager client interface, or performed remotely using a Web-based interface.

The retrieval process transfers the archival data copy onto a designated machine.

Instant Archive and Rapid Recovery:

IBM Tivoli Storage Manager allows for the creation of a complete set of client files, called a *backup set*, on the Tivoli Storage Manager server system using the most recent backup versions stored by the server. In a process called *Instant Archive*, a backup set is used to retain a snapshot of a client file system for a designated period of time. The *Rapid Recovery* process allow you to copy backup sets onto portable media for LAN-free recovery of a client system.

IBM Tivoli Storage Manager also offers a number of separately licensed optional features. These include:

Space Manager Client:

This feature provides for the automatic and transparent movement of operational data from a client system to server-managed storage. This process, called *Hierarchical Space Management* (HSM), is implemented as a client installation and controlled by policy defined to the Tivoli Storage Manager server. HSM frees up space on a client machine by using distributed storage media as a virtual hard drive for that machine. Files are automatically moved and stored according to size, age, and usage. When a user accesses this data, it is dynamically and transparently restored to the client machine.

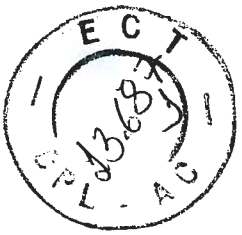
Manual 41

IBM Tivoli Storage Manager for AIX - Quick Start

IBM Tivoli Storage Manager
for AIX

Quick Start

Version 5 Release 2



GC32-0770-01

Chapter 1. Introducing IBM Tivoli Storage Manager

IBM Tivoli Storage Manager provides automated, policy-based, distributed data and storage management for file servers and workstations in an enterprise network environment. The base functions provided by Tivoli Storage Manager include:

Backup and Restore:

The backup process creates a copy of the file or application data that can be recovered if the original data is lost or destroyed. Unlike other backup applications, Tivoli Storage Manager implements a *progressive backup methodology* to move data quickly and reliably. Using progressive backup, the number of file versions maintained by Tivoli Storage Manager and the length of time they are retained can be specified by the storage administrator. Refer to "Common Backup Methodologies" on page 6 for more information.

Backups can be scheduled, performed manually from the Tivoli Storage Manager client interface, or performed remotely using a Web-based interface.

The restore process transfers a backup data copy from Tivoli Storage Manager server-managed storage onto a designated machine.

Archive and Retrieval:

The archive process creates a copy of a file or a set of files and stores it as a unique object for a specified period of time. This function is useful for maintaining copies of vital records for historical purposes.

Like the backup process, the archive process can be scheduled, performed manually from the Tivoli Storage Manager client interface, or performed remotely using a Web-based interface.

The retrieval process transfers the archival data copy onto a designated machine.

Instant Archive and Rapid Recovery:

IBM Tivoli Storage Manager allows for the creation of a complete set of client files, called a *backup set*, on the Tivoli Storage Manager server system using the most recent backup versions stored by the server. In a process called *Instant Archive*, a backup set is used to retain a snapshot of a client file system for a designated period of time. The *Rapid Recovery* process allow you to copy backup sets onto portable media for LAN-free recovery of a client system.

IBM Tivoli Storage Manager also offers a number of separately licensed optional features. These include:

Space Manager Client:

This feature provides for the automatic and transparent movement of operational data from a client system to server-managed storage. This process, called *Hierarchical Space Management* (HSM), is implemented as a client installation and controlled by policy defined to the Tivoli Storage Manager server. HSM frees up space on a client machine by using distributed storage media as a virtual hard drive for that machine. Files are automatically moved and stored according to size, age, and usage. When a user accesses this data, it is dynamically and transparently moved to the client machine.

Manual 42

IBM Tivoli Storage Manager for System Backup and Recovery Installation and User's Guide

IBM Tivoli Storage Manager for System Backup and Recovery

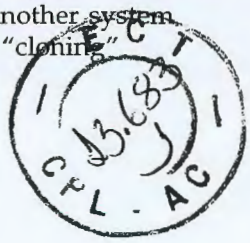
Installation and User's Guide

Version 5 Release 6

GC32-9076-01

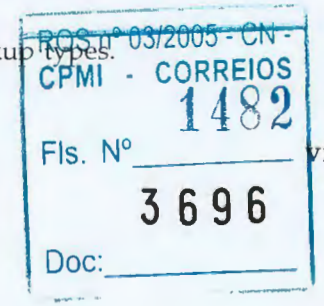
IBM Tivoli Storage Manager for System Backup and Recovery Overview

IBM Tivoli Storage Manager for System Backup and Recovery (also known as "SysBack") provides system administrators and other system users with a simple, efficient way to backup and recover data from a command line or a SMIT menu-driven interface. SysBack lets you recover all or part of the system. SysBack is also flexible; you can install one system installation image to another system with either identical or different hardware configurations, called "cloning."



SysBack features let you:

- Create various types of backups, including:
  - Full system (installation image)
  - Volume groups
  - Logical volumes (raw data)
  - Filesystems
  - Specific directories or files
- Incrementally backup and restore data.
- Perform "power" system backups that enable faster backup and restore times by backing up all data as raw logical volumes and heighten read/write performance while reducing CPU usage.
- Perform backups to locally attached tape drives or files on disk and remote hosts across the network.
- Selectively exclude specific files, directories, filesystems, or logical volumes from backups.
- Centrally manage backup clients using "pull" backups from a single server.
- Create backup scripts for easy automation.
- Define backup schedules for easy automation.
- Execute pre and post-backup scripts that enable environment-specific task automation, including halting database applications before beginning a backup.
- Perform backups to multiple sequential devices, automatically continuing the backup on the next device when the first is full and minimizing manual intervention when autoloading libraries are not available.
- Perform backups to multiple parallel devices, called "striping," which lets you complete a single backup in a fraction of the normal time.
- Create multiple copies of a single backup to different devices in approximately the same time it takes for a single copy.
- View progress status indicators that display estimated backup or restore sizes, times, performance estimates and a completion percentage estimate.
- Receive completion status logs on all backup, list and verification operations.
- Use SMIT menus to configure SysBack options, which let you backup and restore volume groups, logical volumes, filesystems, directories, or files and list and verifying backup images.
- Use sequential autoloading devices to minimize manual intervention and tape loading operations.
- "Stack" multiple backups on a single tape for all backup types.



Manual 43

IBM Tivoli Storage Manager for AIX
Storage Agent User's Guide

IBM Tivoli Storage Manager
for AIX

Storage Agent User's Guide

Version 5.2

GC32-0771-01

Chapter 1. Storage Agent Overview

IBM Tivoli Storage Manager for Storage Area Networks is a feature of Tivoli Storage Manager that enables LAN-free client-data movement.

This feature allows the client system to directly write data to, or read data from, storage devices attached to a storage area network (SAN), instead of passing or receiving the information over the network. Data movement is thereby off-loaded from the LAN and from the Tivoli Storage Manager server, making network bandwidth available for other uses. For instance, using the SAN for client data movement decreases the load on the Tivoli Storage Manager server and allows it to support a greater number of simultaneous client connections. See Figure 1. The storage agent, a component of the feature, makes LAN-free data movement possible.

You install the storage agent on the client machine where it shares storage resources with the Tivoli Storage Manager server. A Tivoli Storage Manager server, acting as a library manager, controls the storage devices. This server may be the server working in conjunction with the storage agent or another server in the enterprise. The Tivoli Storage Manager server keeps track of the metadata that the client has stored. The metadata, such as policy information and file name and size, is passed over the LAN connection between the storage agent and server.

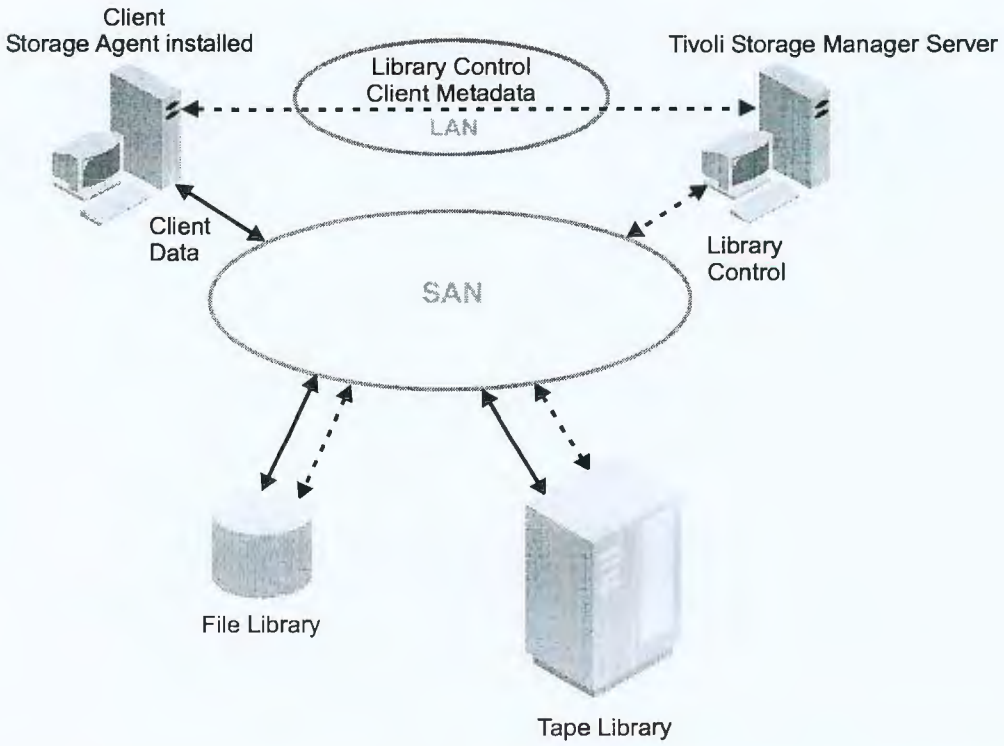


Figure 1. SAN Data Movement. Solid lines indicate data movement. Broken lines indicate movement of control information and metadata.

Manual 44

IBM Tivoli Storage Manager for Databases 5.1.5 - Data Protection for Microsoft SQL Server - Installation and User's Guide

IBM Tivoli Storage Manager for Databases 5.1.5

Data Protection for Microsoft SQL Server Installation and User's Guide

SC32-9059-00

Chapter 1. Introducing Data Protection for SQL

Data Protection for SQL allows you to perform online backups and restores of Microsoft SQL Server databases to Storage Manager Server storage using either command-line or graphical user interfaces (GUI) on Windows NT and Windows 2000. This chapter provides the following information about Data Protection for SQL:

- Version migration and coexistence
- Features
- Functions
- Security
- Performance
- Backup strategy considerations
- Online help
- Microsoft Cluster Server (MSCS) considerations

Version migration and coexistence considerations

IMPORTANT!

Data Protection for SQL Version 5.1.5 utilizes the same backup naming conventions, file space names and placement, and meta contents as Data Protection for SQL Version 2.2. Like Version 2.2, Data Protection for SQL Version 5.1.5 is completely incompatible with Data Protection for SQL Version 1. You cannot query or restore backup objects created by Version 1 with Version 2.2 or Version 5.1.5. As a result, if you are storing backup objects created by Version 1, **you must retain Version 1 for as long as you retain those backup objects**. Version 5.1.5 and Version 2.2 can coexist with Version 1. However, like Version 2.2, the Data Protection for SQL Version 5.1.5 interfaces are not compatible with the Version 1 interfaces. No migration tool is provided to help convert Version 1 command line scripts to Version 5.1.5 syntax. The Version 5.1.5 installation program will not replace any installed Version 1.

Data Protection for SQL Version 5.1.5 is compatible with Data Protection for SQL Version 2.2.

Data Protection for SQL features

Data Protection for SQL helps you protect and manage SQL Server data by making it easy to:

- Back up any SQL database to any Storage Manager Server.
- Perform full and transaction log backups and restores of SQL databases.
- Perform backups with an expanded range of options such as differential, file, and group operations. See " SQL Server database backup" on page 2 for more detail.
- Perform operations from multiple SQL Server instances on the same machine as Data Protection for SQL (for SQL Server 2000).

Note: You can access only one SQL Server per execution of Data Protection for SQL from either the command line or GUI.