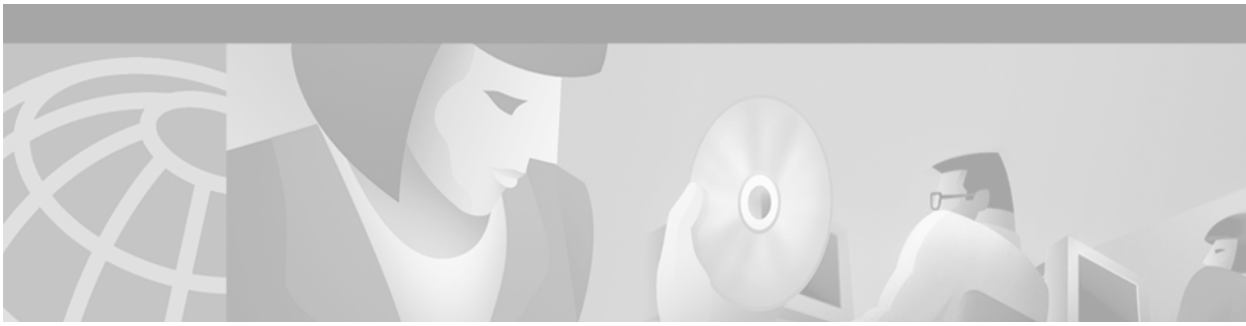

Release Notes for Cisco 7000 Family for Cisco IOS Release 12.2 T

June 7, 2001

Note You can find the most current Cisco IOS documentation on Cisco.com. This set of electronic documents may contain updates and modifications made after the hard-copy documents were printed.

These release notes for the Cisco 7000 family describe the enhancements provided in Cisco IOS Release 12.2(2)T. These release notes are updated as needed.

For a list of the software caveats that apply to Cisco IOS Release 12.2 T, see *Caveats for Cisco IOS Release12.2T*, which accompanies these release notes. The caveats document is updated for every maintenance release and is located on Cisco.com and the Documentation CD-ROM.

Use these release notes with *Cross-Platform Release Notes for Cisco IOS Release 12.2 T* on Cisco.com and theDocumentation CD-ROM.

Contents

These release notes contain the following sections:

Cisco Systems

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

78-12946-01

System Requirements

This section describes the system requirements for Cisco IOS Release 12.2 T and includes the following sections:

Memory Recommendations

Table 1 Memory Requirements for Cisco IOS Release 12.2(2)T

Platforms	Feature Sets	Image Name	Software Image	Flash Memory Recommended	DRAM Memory Recommended	Runs From
Cisco 7100 Series	IP Standard Feature Set	IP	c7100-is-mz	16 MB Flash	64 MB DRAM	RAM
		IP IPSec 56	c7100-ik8s-mz	16 MB Flash	64 MB DRAM	RAM
		IP IPSec 3DES	c7100-ik9s-mz	16 MB Flash	64 MB DRAM	RAM
	IP Firewall Standard Feature Set	IP/FW/IDS	c7100-io3s-mz	16 MB Flash	64 MB DRAM	RAM
		IP/FW/IDS IPSec 56	c7100-ik8o3s-mz	16 MB Flash	64 MB DRAM	RAM
		IP/FW/IDS IPSec 3DES	c7100-ik9o3s-mz	16 MB Flash	64 MB DRAM	RAM
	Enterprise Standard Feature Set	Enterprise	c7100-js-mz	16 MB Flash	64 MB DRAM	RAM
		Enterprise IPSec 56	c7100-jk8s-mz	16 MB Flash	64 MB DRAM	RAM
		Enterprise IPSec 3DES	c7100-jk9s-mz	16 MB Flash	64 MB DRAM	RAM
	Enterprise Firewall Standard Feature Set	Enterprise/FW/IDS	c7100-jo3s-mz	16 MB Flash	64 MB DRAM	RAM
		Enterprise/FW/IDS IPSec 56	c7100-jk8o3s-mz	16 MB Flash	64 MB DRAM	RAM
		Enterprise/FW/IDS IPSec 3DES	c7100-jk9o3s-mz	16 MB Flash	64 MB DRAM	RAM

Table 1 Memory Requirements for Cisco IOS Release 12.2(2)T (continued)

Platforms	Feature Sets	Image Name	Software Image	Flash Memory Recommended	DRAM Memory Recommended	Runs From
Cisco 7200 Series	IP Standard Feature Set	IP	c7200-is-mz	16 MB Flash	128 MB DRAM	RAM
		IP IPSec 56	c7200-ik8s-mz	16 MB Flash	128 MB DRAM	RAM
		IP IPSec 3DES	c7200-ik9s-mz	16 MB Flash	128 MB DRAM	RAM
	IP Firewall Standard Feature Set	IP/FW/IDS	c7200-io3s-mz	16 MB Flash	128 MB DRAM	RAM
		IP/FW/IDS IPSec 56	c7200-ik8o3s-mz	16 MB Flash	128 MB DRAM	RAM
		IP/FW/IDS IPSec 3DES	c7200-ik9o3s-mz	16 MB Flash	128 MB DRAM	RAM
	Enterprise Standard Feature Set	Enterprise	c7200-js-mz	16 MB Flash	128 MB DRAM	RAM
		Enterprise IPSec 56	c7200-jk8s-mz	16 MB Flash	128 MB DRAM	RAM
		Enterprise IPSec 3DES	c7200-jk9s-mz	16 MB Flash	128 MB DRAM	RAM
	Enterprise MCM Feature Set	Enterprise MCM	c7200-jx2-mz	16 MB Flash	128 MB DRAM	RAM
	Enterprise Wireless Feature Set	Enterprise Wireless	c7200-g5js-mz	16 MB Flash	128 MB DRAM	RAM
		Enterprise Wireless IPSec 56	c7200-g5jk8s-mz	16 MB Flash	128 MB DRAM	RAM
	Enterprise Firewall Standard Feature Set	Enterprise/FW/IDS	c7200-jo3s-mz	16 MB Flash	128 MB DRAM	RAM
		Enterprise/FW/IDS IPSec 56	c7200-jk8o3s-mz	16 MB Flash	128 MB DRAM	RAM
		Enterprise/FW/IDS IPSec 3DES	c7200-jk9o3s-mz	16 MB Flash	128 MB DRAM	RAM
	Enterprise/SNASW Feature Set	Enterprise/SNASW	c7200-a3js-mz	16 MB Flash	128 MB DRAM	RAM
		Enterprise/SNASW IPSec 56	c7200-a3jk8s-mz	16 MB Flash	128 MB DRAM	RAM
		Enterprise/SNASW IPSec 3DES	c7200-a3jk9s-mz	16 MB Flash	128 MB DRAM	RAM
	Desktop/IBM Standard Feature Set	Desktop/IBM	c7200-ds-mz	16 MB Flash	128 MB DRAM	RAM
		Desktop/IBM IPSec 56	c7200-dk8s-mz	16 MB Flash	128 MB DRAM	RAM

Table 1 Memory Requirements for Cisco IOS Release 12.2(2)T (continued)

Platforms	Feature Sets	Image Name	Software Image	Flash Memory Recommended	DRAM Memory Recommended	Runs From
	Desktop/IBM Firewall Standard Feature Set	Desktop/IBM/FW/IDS	c7200-do3s-mz	16 MB Flash	128 MB DRAM	RAM
		Desktop/IBM/FW/IDS IPSec 56	c7200-dk8o3s-mz	16 MB Flash	128 MB DRAM	RAM
		Desktop/IBM/FW/IDS IPSec 3DES	c7200-dk9o3s-mz	16 MB Flash	128 MB DRAM	RAM
Cisco 7500 Series	IP Standard Feature Set	IP	rsp-isv-mz	20 MB Flash	128 MB DRAM	RAM
		IP IPSec 56	rsp-ik8sv-mz	20 MB Flash	128 MB DRAM	RAM
		IP IPSec 3DES	rsp-ik9sv-mz	20 MB Flash	128 MB DRAM	RAM
	IP Firewall Standard Feature Set	IP/FW/IDS	rsp-io3sv-mz	20 MB Flash	128 MB DRAM	RAM
		IP/FW/IDS IPSec 56	rsp-ik8o3sv-mz	20 MB Flash	128 MB DRAM	RAM
		IP/FW/IDS IPSec 3DES	rsp-ik9o3sv-mz	20 MB Flash	128 MB DRAM	RAM
	Enterprise Standard Feature Set	Enterprise	rsp-jsv-mz	20 MB Flash	128 MB DRAM	RAM
		Enterprise IPSec 56	rsp-jk8sv-mz	20 MB Flash	128 MB DRAM	RAM
		Enterprise IPSec 3DES	rsp-jk9sv-mz	20 MB Flash	128 MB DRAM	RAM
	Enterprise Firewall Standard Feature Set	Enterprise/FW/IDS	rsp-jo3sv-mz	20 MB Flash	128 MB DRAM	RAM
		Enterprise/FW/IDS IPSec 56	rsp-jk8o3sv-mz	20 MB Flash	128 MB DRAM	RAM
		Enterprise/FW/IDS IPSec 3DES	rsp-jk9o3sv-mz	20 MB Flash	128 MB DRAM	RAM
	Enterprise/SNASW Feature Set	Enterprise/SNASW	rsp-a3jsv-mz	20 MB Flash	128 MB DRAM	RAM
		Enterprise/SNASW IPSec 56	rsp-a3jk8sv-mz	20 MB Flash	128 MB DRAM	RAM
		Enterprise/SNASW IPSec 3DES	rsp-a3jk9sv-mz	20 MB Flash	128 MB DRAM	RAM
	Desktop/IBM Standard Feature Set	Desktop/IBM	rsp-dsv-mz	20 MB Flash	128 MB DRAM	RAM
		Desktop/IBM IPSec 56	rsp-dk8sv-mz	20 MB Flash	128 MB DRAM	RAM

Table 1 Memory Requirements for Cisco IOS Release 12.2(2)T (continued)

Platforms	Feature Sets	Image Name	Software Image	Flash Memory Recommended	DRAM Memory Recommended	Runs From
	Desktop/IBM Firewall Standard Feature Set	Desktop/IBM/FW/IDS	rsp-do3sv-mz	20 MB Flash	128 MB DRAM	RAM
		Desktop/IBM/FW/IDS IPSec 56	rsp-dk8o3sv-mz	20 MB Flash	128 MB DRAM	RAM
		Desktop/IBM/FW/IDS IPSec 3DES	rsp-dk9o3sv-mz	20 MB Flash	128 MB DRAM	RAM

Supported Hardware

Cisco IOS Release 12.2(2)T supports the Cisco 7000 family:

- Cisco 7000 series routers (Cisco 7000 and Cisco 7010) upgraded with the 7000 Series Route Switch Processor (RSP7000) and 7000 Series Chassis Interface (RSP7000CI)
- Cisco 7100 series routers (Cisco 7120 and Cisco 7140)
- Cisco 7200 series routers (Cisco 7202, Cisco 7204, and Cisco 7206)
- Cisco 7500 series routers (Cisco 7505, Cisco 7507, Cisco 7513, and Cisco 7576)

For detailed descriptions of the new hardware features, see the "New and Changed Information" section on page 27.

Determining the Software Version

To determine the version of Cisco IOS software running on your Cisco 7000 family router, log in to the router and enter the **show version** EXEC command:

```
Router> show version
Cisco Internetwork Operating System Software
IOS (tm) 12.2 T Software (C7200-JS-MZ), Version 12.2(2)T, RELEASE SOFTWARE
```

Upgrading to a New Software Release

For general information about upgrading to a new software release, refer to S*oftware Installation and Upgrade Procedures* located at the following URL:

http://www.cisco.com/warp/public/130/upgrade_index.shtml

Microcode and Modem Code Software

Microcode software images are bundled with the system software image—with the exception of the Channel Interface Processor (CIP) microcode (all system software images). Bundling eliminates the need to store separate microcode images. When the router starts, the system software unpacks the microcode software bundle and loads the proper software on all the interface processor boards. Table 2 lists the current microcode versions for the Cisco 7000 family.

You could have received a later version of modem code than the one bundled with the Cisco IOS software. The modem code in Flash memory is mapped to the modems. Unless you fully understand how Cisco IOS software uses modem code, it is important to keep the factory configuration.

The modem code release notes are on Cisco.com and the Documentation CD-ROM.

On Cisco.com at:

Technical Documents: **Documentation Home Page**: **Access Servers and Access Routers**: **Firmware and Portware Information**

On the Documentation CD-ROM at:

Cisco Product Documentation: **Access Servers and Access Routers**: **Firmware and Portware Information**

Table 2 Current Microcode Versions for the Cisco 7000 Family

Processor or Module	Current Bundled Route Switch Processor (RSP) Microcode Version	Minimum Version Required
AIP (ATM Interface Processor)	20.18	20.13
EIP (Ethernet Interface Processor)	20.6	20.3
FEIP (Fast Ethernet Interface Processor)	20.8	20.7
FIP (FDDI Interface Processor)	20.4	20.4
FSIP (Fast Serial Interface Processor)	20.9	20.9
HIP (HIIS Interface Processor)	20.2	20.2
MIP (MultiChannel Interface Processor)	22.3	22.3
TRIP (Token Ring Interface Processor)	20.2	20.2
VIP2 (second-generation Versatile Interface Processor)	22.20	22.20

Feature Set Tables

The Cisco IOS software is packaged in feature sets consisting of software images—depending on the platform. Each feature set contains a specific set of Cisco IOS features.

Cisco IOS Release 12.2 T supports the same feature sets as Cisco IOS Release 12.2, but Cisco IOS Release 12.2 T can include new features supported by the Cisco 7000 family.

Caution Cisco IOS images with strong encryption (including, but not limited to, 168-bit Triple Data Encryption Standard (3DES) data encryption feature sets) are subject to United States government export controls and have limited distribution. Strong encryption images to be installed outside the United States are likely to require an export license. Customer orders may be denied or subject to delay because of United States government regulations. When applicable, purchaser and user must obtain local import and use authorizations for all encryption strengths. Please contact your sales representative or distributor for more information, or send an e-mail to export@cisco.com.

Table 3 through Table 16 list the features and feature sets supported by the Cisco 7000 family in Cisco IOS Release 12.2 T and use the following conventions:

- Yes—The feature is supported in the software image.
- No—The feature is not supported in the software image.
- In—The number in the "In" column indicates the Cisco IOS release in which the feature was introduced. For example, (5) means a feature was introduced in 12.2(5)T. If a cell in this column is empty, the feature was included in the initial base release.

Note This table might not be cumulative or list all the features in each image. You can find the most current Cisco IOS documentation on Cisco.com. These electronic documents may contain updates and modifications made after the hard-copy documents were printed. If you have a Cisco.com login account, you can find image and release information regarding features prior to Cisco IOS Release 12.2(2)T by using the Feature Navigator tool at http://www.cisco.com/go/fn.

Table 3 Feature List by Feature Set for the Cisco 7100 Series

Features	In	Software Images by Feature Sets			
		IP	IP IPSec 56	IP IPSec 3DES	IP/FW/IDS
Broadband					
Distinguished Name-Based Crypto Maps	(2)	No	Yes	Yes	No
IP Routing					
BGP Link Bandwidth	(2)	Yes	Yes	Yes	Yes
IPv6 for Cisco IOS Software	(2)	Yes	Yes	Yes	Yes
Mobile IP MIB Support for SNMP	(2)	Yes	Yes	Yes	Yes
NAT Support of H.323 RAS	(2)	No	No	No	Yes
iBGP Multipath Load Sharing	(2)	Yes	Yes	Yes	Yes
Management					
SNMP Support for VPN	(2)	Yes	Yes	Yes	Yes

Table 3 Feature List by Feature Set for the Cisco 7100 Series (continued)

Features	In	Software Images by Feature Sets			
		IP	IP IPSec 56	IP IPSec 3DES	IP/FW/IDS
Miscellaneous					
CNS Configuration Agent	(2)	Yes	Yes	Yes	Yes
CNS Event Agent	(2)	Yes	Yes	Yes	Yes
Interface Alias Long Name Support for SNMP	(2)	Yes	Yes	Yes	Yes
Interface Index Display	(2)	Yes	Yes	Yes	Yes
Quality of Service					
Low Latency Queueing Enhancement-Priority Percentage Support	(2)	Yes	Yes	Yes	Yes
Security					
DF Bit Override Functionality with IPSec Tunnels	(2)	No	Yes	Yes	No

Table 4 Feature List by Feature Set for the Cisco 7100 Series, Part 2

Features	In	Software Images by Feature Sets			
		IP/FW/IDS IPSec 56	IP/FW/IDS IPSec 3DES	Enterprise	Enterprise IPSec 56
Broadband					
Distinguished Name-Based Crypto Maps	(2)	Yes	Yes	No	Yes
IP Routing					
BGP Link Bandwidth	(2)	Yes	Yes	Yes	Yes
IPv6 for Cisco IOS Software	(2)	Yes	Yes	Yes	Yes
Mobile IP MIB Support for SNMP	(2)	Yes	Yes	Yes	Yes
NAT Support of H.323 RAS	(2)	Yes	Yes	Yes	Yes
iBGP Multipath Load Sharing	(2)	Yes	Yes	Yes	Yes
Management					
SNMP Support for VPN	(2)	Yes	Yes	Yes	Yes
Miscellaneous					
CNS Configuration Agent	(2)	Yes	Yes	Yes	Yes
CNS Event Agent	(2)	Yes	Yes	Yes	Yes
Interface Alias Long Name Support for SNMP	(2)	Yes	Yes	Yes	Yes
Interface Index Display	(2)	Yes	Yes	Yes	Yes
Quality of Service					
Low Latency Queueing Enhancement-Priority Percentage Support	(2)	Yes	Yes	Yes	Yes
Security					
DF Bit Override Functionality with IPSec Tunnels	(2)	Yes	Yes	No	Yes

Table 5 Feature List by Feature Set for the Cisco 7100 Series, Part 3

Features	In	Software Images by Feature Sets			
		Enterprise IPSec 3DES	Enterprise FW/IDS	Enterprise/ FW/IDS IPSec 56	Enterprise/ FW/IDS IPSec 3DES
Broadband					
Distinguished Name-Based Crypto Maps	(2)	Yes	No	Yes	Yes
IP Routing					
BGP Link Bandwidth	(2)	Yes	Yes	Yes	Yes
IPv6 for Cisco IOS Software	(2)	Yes	Yes	Yes	Yes
Mobile IP MIB Support for SNMP	(2)	Yes	Yes	Yes	Yes
NAT Support of H.323 RAS	(2)	Yes	Yes	Yes	Yes
iBGP Multipath Load Sharing	(2)	Yes	Yes	Yes	Yes
Management					
SNMP Support for VPN	(2)	Yes	Yes	Yes	Yes
Miscellaneous					
CNS Configuration Agent	(2)	Yes	Yes	Yes	Yes
CNS Event Agent	(2)	Yes	Yes	Yes	Yes
Interface Alias Long Name Support for SNMP	(2)	Yes	Yes	Yes	Yes
Interface Index Display	(2)	Yes	Yes	Yes	Yes
Quality of Service					
Low Latency Queueing Enhancement-Priority Percentage Support	(2)	Yes	Yes	Yes	Yes
Security					
DF Bit Override Functionality with IPSec Tunnels	(2)	Yes	No	Yes	Yes

Table 6 Feature List by Feature Set for the Cisco 7200 Series

Features	In	Software Images by Feature Sets			
		IP	IP IPSec 56	IP IPSec 3DES	IP/FW/IDS
Broadband					
DHCP Option 82 Support for Routed Bridge Encapsulation	(2)	Yes	Yes	Yes	Yes
Distinguished Name-Based Crypto Maps	(2)	No	Yes	Yes	No
Dial Services					
Modem Script and System Script Support in LSDO	(2)	Yes	Yes	Yes	Yes
Shell-Based Authentication of VPDN Users	(2)	Yes	Yes	Yes	Yes
IP Routing					
BGP Link Bandwidth	(2)	Yes	Yes	Yes	Yes

Table 6 Feature List by Feature Set for the Cisco 7200 Series (continued)

Features	In	Software Images by Feature Sets			
		IP	IP IPSec 56	IP IPSec 3DES	IP/FW/IDS
IPv6 for Cisco IOS Software	(2)	Yes	Yes	Yes	Yes
Mobile IP MIB Support for SNMP	(2)	Yes	Yes	Yes	Yes
NAT Support of H.323 RAS	(2)	No	No	No	Yes
iBGP Multipath Load Sharing	(2)	Yes	Yes	Yes	Yes
Management					
MPLS Label Distribution Protocol MIB	(2)	No	No	No	No
MPLS Label Switching Router MIB	(2)	No	No	No	No
MPLS Traffic Engineering MIB	(2)	No	No	No	No
SA Agent Support for Application Monitoring, Frame Relay, VoIP, and MPLS VPN	(2)	Yes	Yes	Yes	Yes
SNMP Support for VPN	(2)	Yes	Yes	Yes	Yes
SNMP Trap Support for VSI Master MIB	(2)	No	No	No	No
Trimble Palisade NTP Synchronization Driver for the Cisco 7200 Series	(2)	Yes	Yes	Yes	Yes
Miscellaneous					
CNS Configuration Agent	(2)	Yes	Yes	Yes	Yes
CNS Event Agent	(2)	Yes	Yes	Yes	Yes
Enhancements to H.323 Call Statistics	(2)	Yes	Yes	Yes	Yes
Interface Alias Long Name Support for SNMP	(2)	Yes	Yes	Yes	Yes
Interface Index Display	(2)	Yes	Yes	Yes	Yes
PPP over Ethernet Client	(2)	Yes	Yes	Yes	Yes
Protocols					
MPLS Label Distribution Protocol	(2)	No	No	No	No
Quality of Service					
Class-Based Frame-Relay DE-Bit Matching and Marking	(2)	Yes	Yes	Yes	Yes
Control Plane DSCP Support for RSVP	(2)	Yes	Yes	Yes	Yes
Low Latency Queueing Enhancement-Priority Percentage Support	(2)	Yes	Yes	Yes	Yes
MPLS QoS Multi-VC Mode for PA-A3	(2)	No	No	No	No
RSVP Support for ATM/PVCs	(2)	Yes	Yes	Yes	Yes
Scalability					
RSVP Scalability Enhancements	(2)	Yes	Yes	Yes	Yes
Security					
DF Bit Override Functionality with IPSec Tunnels	(2)	No	Yes	Yes	No
Secure Copy	(2)	No	Yes	Yes	No

Table 6 Feature List by Feature Set for the Cisco 7200 Series (continued)

Features	In	Software Images by Feature Sets			
		IP	IP IPSec 56	IP IPSec 3DES	IP/FW/IDS
Switching					
IOS Server Load Balancing	(2)	Yes	Yes	Yes	Yes
Netflow Multiple Export Destinations	(2)	Yes	Yes	Yes	Yes
Voice Services					
H.323 Call Redirection Enhancements	(2)	Yes	Yes	Yes	Yes
H.323 Version 2 Phase 2	(2)	Yes	No	No	No
High Performance Gatekeeper	(2)	Yes	Yes	Yes	Yes
MGCP CAS PBX and PRI Backhaul on Cisco 7200 Routers	(2)	Yes	Yes	Yes	Yes
SS7 Gateway Support	(2)	Yes	Yes	Yes	Yes
TCL IVR disconnect cause-code manipulation	(2)	Yes	Yes	Yes	Yes
Voice over ATM with AAL2 Trunking on Cisco 7200 Series Routers	(2)	Yes	Yes	Yes	Yes
WAN Services					
X.25 Annex G Session Status Change Reporting	(2)	Yes	Yes	Yes	Yes

Table 7 Feature List by Feature Set for the Cisco 7200 Series, Part 2

Features	In	Software Images by Feature Sets			
		IP/FW/IDS IPSec 56	IP/FW/IDS IPSec 3DES	Enterprise	Enterprise IPSec 56
Broadband					
DHCP Option 82 Support for Routed Bridge Encapsulation	(2)	Yes	Yes	Yes	Yes
Distinguished Name-Based Crypto Maps	(2)	Yes	Yes	No	Yes
Dial Services					
Modem Script and System Script Support in LSDO	(2)	Yes	Yes	Yes	Yes
Shell-Based Authentication of VPDN Users	(2)	Yes	Yes	Yes	Yes
IP Routing					
BGP Link Bandwidth	(2)	Yes	Yes	Yes	Yes
IPv6 for Cisco IOS Software	(2)	Yes	Yes	Yes	Yes
Mobile IP MIB Support for SNMP	(2)	Yes	Yes	Yes	Yes
NAT Support of H.323 RAS	(2)	Yes	Yes	Yes	Yes
iBGP Multipath Load Sharing	(2)	Yes	Yes	Yes	Yes
Management					
MPLS Label Distribution Protocol MIB	(2)	No	No	Yes	Yes

Table 7 Feature List by Feature Set for the Cisco 7200 Series, Part 2 (continued)

Features	In	Software Images by Feature Sets			
		IP/FW/IDS IPSec 56	IP/FW/IDS IPSec 3DES	Enterprise	Enterprise IPSec 56
MPLS Label Switching Router MIB	(2)	No	No	Yes	Yes
MPLS Traffic Engineering MIB	(2)	No	No	Yes	Yes
SA Agent Support for Application Monitoring, Frame Relay, VoIP, and MPLS VPN	(2)	Yes	Yes	Yes	Yes
SNMP Support for VPN	(2)	Yes	Yes	Yes	Yes
SNMP Trap Support for VSI Master MIB	(2)	No	No	Yes	Yes
Trimble Palisade NTP Synchronization Driver for the Cisco 7200 Series	(2)	Yes	Yes	Yes	Yes
Miscellaneous					
CNS Configuration Agent	(2)	Yes	Yes	Yes	Yes
CNS Event Agent	(2)	Yes	Yes	Yes	Yes
Enhancements to H.323 Call Statistics	(2)	Yes	Yes	Yes	Yes
Interface Alias Long Name Support for SNMP	(2)	Yes	Yes	Yes	Yes
Interface Index Display	(2)	Yes	Yes	Yes	Yes
PPP over Ethernet Client	(2)	Yes	Yes	Yes	Yes
Protocols					
MPLS Label Distribution Protocol	(2)	No	No	Yes	Yes
Quality of Service					
Class-Based Frame-Relay DE-Bit Matching and Marking	(2)	Yes	Yes	Yes	Yes
Control Plane DSCP Support for RSVP	(2)	Yes	Yes	Yes	Yes
Low Latency Queueing Enhancement-Priority Percentage Support	(2)	Yes	Yes	Yes	Yes
MPLS QoS Multi-VC Mode for PA-A3	(2)	No	No	Yes	Yes
RSVP Support for ATM/PVCs	(2)	Yes	Yes	Yes	Yes
Scalability					
RSVP Scalability Enhancements	(2)	Yes	Yes	Yes	Yes
Security					
DF Bit Override Functionality with IPSec Tunnels	(2)	Yes	Yes	No	Yes
Secure Copy	(2)	Yes	Yes	No	Yes
Switching					
IOS Server Load Balancing	(2)	Yes	Yes	Yes	Yes
Netflow Multiple Export Destinations	(2)	Yes	Yes	Yes	Yes
Voice Services					
H.323 Call Redirection Enhancements	(2)	Yes	Yes	Yes	Yes
H.323 Version 2 Phase 2	(2)	No	No	Yes	No

Table 7 Feature List by Feature Set for the Cisco 7200 Series, Part 2 (continued)

Features	In	Software Images by Feature Sets			
		IP/FW/IDS IPSec 56	IP/FW/IDS IPSec 3DES	Enterprise	Enterprise IPSec 56
High Performance Gatekeeper	(2)	Yes	Yes	Yes	Yes
MGCP CAS PBX and PRI Backhaul on Cisco 7200 Routers	(2)	Yes	Yes	Yes	Yes
SS7 Gateway Support	(2)	Yes	Yes	Yes	Yes
TCL IVR disconnect cause-code manipulation	(2)	Yes	Yes	Yes	Yes
Voice over ATM with AAL2 Trunking on Cisco 7200 Series Routers	(2)	Yes	Yes	Yes	Yes
WAN Services					
X.25 Annex G Session Status Change Reporting	(2)	Yes	Yes	Yes	Yes

Table 8 Feature List by Feature Set for the Cisco 7200 Series, Part 3

Features	In	Software Images by Feature Sets			
		Enterprise IPSec 3DES	Enterprise MCM	Enterprise Wireless	Enterprise Wireless IPSec 56
Broadband					
DHCP Option 82 Support for Routed Bridge Encapsulation	(2)	Yes	Yes	Yes	Yes
Distinguished Name-Based Crypto Maps	(2)	Yes	No	Yes	Yes
Dial Services					
Modem Script and System Script Support in LSDO	(2)	Yes	Yes	Yes	Yes
Shell-Based Authentication of VPDN Users	(2)	Yes	Yes	Yes	Yes
IP Routing					
BGP Link Bandwidth	(2)	Yes	Yes	Yes	Yes
IPv6 for Cisco IOS Software	(2)	Yes	Yes	Yes	Yes
Mobile IP MIB Support for SNMP	(2)	Yes	Yes	Yes	Yes
NAT Support of H.323 RAS	(2)	Yes	Yes	Yes	Yes
iBGP Multipath Load Sharing	(2)	Yes	Yes	Yes	Yes
Management					
MPLS Label Distribution Protocol MIB	(2)	Yes	Yes	Yes	Yes
MPLS Label Switching Router MIB	(2)	Yes	Yes	Yes	Yes
MPLS Traffic Engineering MIB	(2)	Yes	Yes	Yes	Yes
SA Agent Support for Application Monitoring, Frame Relay, VoIP, and MPLS VPN	(2)	Yes	No	Yes	Yes
SNMP Support for VPN	(2)	Yes	Yes	Yes	Yes
SNMP Trap Support for VSI Master MIB	(2)	Yes	Yes	Yes	Yes

Table 8 Feature List by Feature Set for the Cisco 7200 Series, Part 3 (continued)

Features	In	Software Images by Feature Sets			
		Enterprise IPSec 3DES	Enterprise MCM	Enterprise Wireless	Enterprise Wireless IPSec 56
Trimble Palisade NTP Synchronization Driver for the Cisco 7200 Series	(2)	Yes	Yes	Yes	Yes
Miscellaneous					
CNS Configuration Agent	(2)	Yes	Yes	Yes	Yes
CNS Event Agent	(2)	Yes	Yes	Yes	Yes
Enhancements to H.323 Call Statistics	(2)	Yes	Yes	Yes	Yes
Interface Alias Long Name Support for SNMP	(2)	Yes	Yes	Yes	Yes
Interface Index Display	(2)	Yes	Yes	Yes	Yes
PPP over Ethernet Client	(2)	Yes	Yes	Yes	Yes
Protocols					
MPLS Label Distribution Protocol	(2)	Yes	Yes	Yes	Yes
Quality of Service					
Class-Based Frame-Relay DE-Bit Matching and Marking	(2)	Yes	Yes	Yes	Yes
Control Plane DSCP Support for RSVP	(2)	Yes	Yes	Yes	Yes
Low Latency Queueing Enhancement-Priority Percentage Support	(2)	Yes	Yes	Yes	Yes
MPLS QoS Multi-VC Mode for PA-A3	(2)	Yes	Yes	Yes	Yes
RSVP Support for ATM/PVCs	(2)	Yes	Yes	Yes	Yes
Scalability					
RSVP Scalability Enhancements	(2)	Yes	Yes	Yes	Yes
Security					
DF Bit Override Functionality with IPSec Tunnels	(2)	Yes	No	No	Yes
Secure Copy	(2)	Yes	No	No	Yes
Switching					
IOS Server Load Balancing	(2)	Yes	Yes	Yes	Yes
Netflow Multiple Export Destinations	(2)	Yes	Yes	Yes	Yes
Voice Services					
H.323 Call Redirection Enhancements	(2)	Yes	No	Yes	Yes
H.323 Version 2 Phase 2	(2)	No	No	No	No
High Performance Gatekeeper	(2)	Yes	Yes	Yes	Yes
MGCP CAS PBX and PRI Backhaul on Cisco 7200 Routers	(2)	Yes	No	Yes	Yes
SS7 Gateway Support	(2)	Yes	No	Yes	Yes
TCL IVR disconnect cause-code manipulation	(2)	Yes	No	Yes	Yes

Table 8 Feature List by Feature Set for the Cisco 7200 Series, Part 3 (continued)

Features	In	Software Images by Feature Sets			
		Enterprise IPSec 3DES	Enterprise MCM	Enterprise Wireless	Enterprise Wireless IPSec 56
Voice over ATM with AAL2 Trunking on Cisco 7200 Series Routers	(2)	Yes	No	Yes	Yes
WAN Services					
X.25 Annex G Session Status Change Reporting	(2)	Yes	Yes	Yes	Yes

Table 9 Feature List by Feature Set for the Cisco 7200 Series, Part 4

Features	In	Software Images by Feature Sets			
		Enterprise/ FW/IDS	Enterprise/ FW/IDS IPSec 56	Enterprise/ FW/IDS IPSec 3DES	Enterprise/ SNASW
Broadband					
DHCP Option 82 Support for Routed Bridge Encapsulation	(2)	Yes	Yes	Yes	Yes
Distinguished Name-Based Crypto Maps	(2)	No	Yes	Yes	No
Dial Services					
Modem Script and System Script Support in LSDO	(2)	Yes	Yes	Yes	Yes
Shell-Based Authentication of VPDN Users	(2)	Yes	Yes	Yes	Yes
IP Routing					
BGP Link Bandwidth	(2)	Yes	Yes	Yes	Yes
IPv6 for Cisco IOS Software	(2)	Yes	Yes	Yes	Yes
Mobile IP MIB Support for SNMP	(2)	Yes	Yes	Yes	Yes
NAT Support of H.323 RAS	(2)	Yes	Yes	Yes	Yes
iBGP Multipath Load Sharing	(2)	Yes	Yes	Yes	Yes
Management					
MPLS Label Distribution Protocol MIB	(2)	Yes	Yes	Yes	Yes
MPLS Label Switching Router MIB	(2)	Yes	Yes	Yes	Yes
MPLS Traffic Engineering MIB	(2)	Yes	Yes	Yes	Yes
SA Agent Support for Application Monitoring, Frame Relay, VoIP, and MPLS VPN	(2)	Yes	Yes	Yes	Yes
SNMP Support for VPN	(2)	Yes	Yes	Yes	Yes
SNMP Trap Support for VSI Master MIB	(2)	Yes	Yes	Yes	Yes
Trimble Palisade NTP Synchronization Driver for the Cisco 7200 Series	(2)	Yes	Yes	Yes	Yes
Miscellaneous					
CNS Configuration Agent	(2)	Yes	Yes	Yes	Yes

Table 9 Feature List by Feature Set for the Cisco 7200 Series, Part 4 (continued)

Features	In	Software Images by Feature Sets			
		Enterprise/ FW/IDS	Enterprise/ FW/IDS IPSec 56	Enterprise/ FW/IDS IPSec 3DES	Enterprise/ SNASW
CNS Event Agent	(2)	Yes	Yes	Yes	Yes
Enhancements to H.323 Call Statistics	(2)	Yes	Yes	Yes	Yes
Interface Alias Long Name Support for SNMP	(2)	Yes	Yes	Yes	Yes
Interface Index Display	(2)	Yes	Yes	Yes	Yes
PPP over Ethernet Client	(2)	Yes	Yes	Yes	Yes
Protocols					
MPLS Label Distribution Protocol	(2)	Yes	Yes	Yes	Yes
Quality of Service					
Class-Based Frame-Relay DE-Bit Matching and Marking	(2)	Yes	Yes	Yes	Yes
Control Plane DSCP Support for RSVP	(2)	Yes	Yes	Yes	Yes
Low Latency Queueing Enhancement-Priority Percentage Support	(2)	Yes	Yes	Yes	Yes
MPLS QoS Multi-VC Mode for PA-A3	(2)	Yes	Yes	Yes	Yes
RSVP Support for ATM/PVCs	(2)	Yes	Yes	Yes	Yes
Scalability					
RSVP Scalability Enhancements	(2)	Yes	Yes	Yes	Yes
Security					
DF Bit Override Functionality with IPSec Tunnels	(2)	No	Yes	Yes	No
Secure Copy	(2)	No	Yes	Yes	No
Switching					
IOS Server Load Balancing	(2)	Yes	Yes	Yes	Yes
Netflow Multiple Export Destinations	(2)	Yes	Yes	Yes	Yes
Voice Services					
H.323 Call Redirection Enhancements	(2)	Yes	Yes	Yes	Yes
H.323 Version 2 Phase 2	(2)	No	No	No	No
High Performance Gatekeeper	(2)	Yes	Yes	Yes	Yes
MGCP CAS PBX and PRI Backhaul on Cisco 7200 Routers	(2)	Yes	Yes	Yes	Yes
SS7 Gateway Support	(2)	Yes	Yes	Yes	Yes
TCL IVR disconnect cause-code manipulation	(2)	Yes	Yes	Yes	Yes
Voice over ATM with AAL2 Trunking on Cisco 7200 Series Routers	(2)	Yes	Yes	Yes	Yes
WAN Services					
X.25 Annex G Session Status Change Reporting	(2)	Yes	Yes	Yes	Yes

Table 10 Feature List by Feature Set for the Cisco 7200 Series, Part 5

Features	In	Software Images by Feature Sets			
		Enterprise/ SNASW IPSec 56	Enterprise/ SNASW IPSec 3DES	Desktop/IBM	Desktop/ IBM IPSec 56
Broadband					
DHCP Option 82 Support for Routed Bridge Encapsulation	(2)	Yes	Yes	Yes	Yes
Distinguished Name-Based Crypto Maps	(2)	Yes	Yes	No	Yes
Dial Services					
Modem Script and System Script Support in LSDO	(2)	Yes	Yes	Yes	Yes
Shell-Based Authentication of VPDN Users	(2)	Yes	Yes	Yes	Yes
IP Routing					
BGP Link Bandwidth	(2)	Yes	Yes	Yes	Yes
IPv6 for Cisco IOS Software	(2)	Yes	Yes	Yes	Yes
Mobile IP MIB Support for SNMP	(2)	Yes	Yes	Yes	Yes
NAT Support of H.323 RAS	(2)	Yes	Yes	No	No
iBGP Multipath Load Sharing	(2)	Yes	Yes	Yes	Yes
Management					
MPLS Label Distribution Protocol MIB	(2)	Yes	Yes	No	No
MPLS Label Switching Router MIB	(2)	Yes	Yes	No	No
MPLS Traffic Engineering MIB	(2)	Yes	Yes	No	No
SA Agent Support for Application Monitoring, Frame Relay, VoIP, and MPLS VPN	(2)	Yes	Yes	No	No
SNMP Support for VPN	(2)	Yes	Yes	Yes	Yes
SNMP Trap Support for VSI Master MIB	(2)	Yes	Yes	No	No
Trimble Palisade NTP Synchronization Driver for the Cisco 7200 Series	(2)	Yes	Yes	Yes	Yes
Miscellaneous					
CNS Configuration Agent	(2)	Yes	Yes	Yes	Yes
CNS Event Agent	(2)	Yes	Yes	Yes	Yes
Enhancements to H.323 Call Statistics	(2)	Yes	Yes	Yes	Yes
Interface Alias Long Name Support for SNMP	(2)	Yes	Yes	Yes	Yes
Interface Index Display	(2)	Yes	Yes	Yes	Yes
PPP over Ethernet Client	(2)	Yes	Yes	Yes	Yes
Protocols					
MPLS Label Distribution Protocol	(2)	Yes	Yes	No	No
Quality of Service					
Class-Based Frame-Relay DE-Bit Matching and Marking	(2)	Yes	Yes	Yes	Yes

Table 10 Feature List by Feature Set for the Cisco 7200 Series, Part 5 (continued)

Features	In	Software Images by Feature Sets			
		Enterprise/ SNASW IPSec 56	Enterprise/ SNASW IPSec 3DES	Desktop/IBM	Desktop/ IBM IPSec 56
Control Plane DSCP Support for RSVP	(2)	Yes	Yes	Yes	Yes
Low Latency Queueing Enhancement-Priority Percentage Support	(2)	Yes	Yes	Yes	Yes
MPLS QoS Multi-VC Mode for PA-A3	(2)	Yes	Yes	No	No
RSVP Support for ATM/PVCs	(2)	Yes	Yes	Yes	Yes
Scalability					
RSVP Scalability Enhancements	(2)	Yes	Yes	Yes	Yes
Security					
DF Bit Override Functionality with IPSec Tunnels	(2)	Yes	Yes	No	Yes
Secure Copy	(2)	Yes	Yes	No	Yes
Switching					
IOS Server Load Balancing	(2)	Yes	Yes	Yes	Yes
Netflow Multiple Export Destinations	(2)	Yes	Yes	Yes	Yes
Voice Services					
H.323 Call Redirection Enhancements	(2)	Yes	Yes	Yes	Yes
H.323 Version 2 Phase 2	(2)	No	No	No	No
High Performance Gatekeeper	(2)	Yes	Yes	Yes	Yes
MGCP CAS PBX and PRI Backhaul on Cisco 7200 Routers	(2)	Yes	Yes	No	No
SS7 Gateway Support	(2)	Yes	Yes	No	No
TCL IVR disconnect cause-code manipulation	(2)	Yes	Yes	Yes	Yes
Voice over ATM with AAL2 Trunking on Cisco 7200 Series Routers	(2)	Yes	Yes	Yes	Yes
WAN Services					
X.25 Annex G Session Status Change Reporting	(2)	Yes	Yes	Yes	Yes

Table 11 Feature List by Feature Set for the Cisco 7200 Series, Part 6

Features	In	Software Images by Feature Sets		
		Desktop/ IBM/FW/IDS	Desktop/ IBM/FW/IDS IPSec 56	Desktop/ IBM/FW/IDS IPSec 3DES
Broadband				
DHCP Option 82 Support for Routed Bridge Encapsulation	(2)	Yes	Yes	Yes
Distinguished Name-Based Crypto Maps	(2)	No	Yes	Yes

Table 11 Feature List by Feature Set for the Cisco 7200 Series, Part 6 (continued)

Features	In	Software Images by Feature Sets		
		Desktop/ IBM/FW/IDS	Desktop/ IBM/FW/IDS IPSec 56	Desktop/ IBM/FW/IDS IPSec 3DES
Dial Services				
Modem Script and System Script Support in LSDO	(2)	Yes	Yes	Yes
Shell-Based Authentication of VPDN Users	(2)	Yes	Yes	Yes
IP Routing				
BGP Link Bandwidth	(2)	Yes	Yes	Yes
IPv6 for Cisco IOS Software	(2)	Yes	Yes	Yes
Mobile IP MIB Support for SNMP	(2)	Yes	Yes	Yes
NAT Support of H.323 RAS	(2)	Yes	Yes	Yes
iBGP Multipath Load Sharing	(2)	Yes	Yes	Yes
Management				
MPLS Label Distribution Protocol MIB	(2)	No	No	No
MPLS Label Switching Router MIB	(2)	No	No	No
MPLS Traffic Engineering MIB	(2)	No	No	No
SA Agent Support for Application Monitoring, Frame Relay, VoIP, and MPLS VPN	(2)	No	No	No
SNMP Support for VPN	(2)	Yes	Yes	Yes
SNMP Trap Support for VSI Master MIB	(2)	No	No	No
Trimble Palisade NTP Synchronization Driver for the Cisco 7200 Series	(2)	Yes	Yes	Yes
Miscellaneous				
CNS Configuration Agent	(2)	Yes	Yes	Yes
CNS Event Agent	(2)	Yes	Yes	Yes
Enhancements to H.323 Call Statistics	(2)	Yes	Yes	Yes
Interface Alias Long Name Support for SNMP	(2)	Yes	Yes	Yes
Interface Index Display	(2)	Yes	Yes	Yes
PPP over Ethernet Client	(2)	Yes	Yes	Yes
Protocols				
MPLS Label Distribution Protocol	(2)	No	No	No
Quality of Service				
Class-Based Frame-Relay DE-Bit Matching and Marking	(2)	Yes	Yes	Yes
Control Plane DSCP Support for RSVP	(2)	Yes	Yes	Yes
Low Latency Queueing Enhancement-Priority Percentage Support	(2)	Yes	Yes	Yes
MPLS QoS Multi-VC Mode for PA-A3	(2)	No	No	No

Table 11 Feature List by Feature Set for the Cisco 7200 Series, Part 6 (continued)

Features	In	Software Images by Feature Sets		
		Desktop/ IBM/FW/IDS	Desktop/ IBM/FW/IDS IPSec 56	Desktop/ IBM/FW/IDS IPSec 3DES
RSVP Support for ATM/PVCs	(2)	Yes	Yes	Yes
Scalability				
RSVP Scalability Enhancements	(2)	Yes	Yes	Yes
Security				
DF Bit Override Functionality with IPSec Tunnels	(2)	No	Yes	Yes
Secure Copy	(2)	No	Yes	Yes
Switching				
IOS Server Load Balancing	(2)	Yes	Yes	Yes
Netflow Multiple Export Destinations	(2)	Yes	Yes	Yes
Voice Services				
H.323 Call Redirection Enhancements	(2)	Yes	Yes	Yes
H.323 Version 2 Phase 2	(2)	No	No	No
High Performance Gatekeeper	(2)	Yes	Yes	Yes
MGCP CAS PBX and PRI Backhaul on Cisco 7200 Routers	(2)	No	No	No
SS7 Gateway Support	(2)	No	No	No
TCL IVR disconnect cause-code manipulation	(2)	Yes	Yes	Yes
Voice over ATM with AAL2 Trunking on Cisco 7200 Series Routers	(2)	Yes	Yes	Yes
WAN Services				
X.25 Annex G Session Status Change Reporting	(2)	Yes	Yes	Yes

Table 12 Feature List by Feature Set for the Cisco 7500 Series

Features	In	Software Images by Feature Sets			
		IP	IP IPSec 56	IP IPSec 3DES	IP/FW/IDS
Broadband					
DHCP Option 82 Support for Routed Bridge Encapsulation	(2)	Yes	Yes	Yes	Yes
IP Routing					
BGP Link Bandwidth	(2)	Yes	Yes	Yes	Yes
Distributed Time-Based Access Lists	(2)	Yes	Yes	Yes	Yes
IPv6 for Cisco IOS Software	(2)	Yes	Yes	Yes	Yes
Mobile IP MIB Support for SNMP	(2)	Yes	Yes	Yes	Yes

Table 12 Feature List by Feature Set for the Cisco 7500 Series (continued)

Features	In	Software Images by Feature Sets			
		IP	IP IPSec 56	IP IPSec 3DES	IP/FW/IDS
NAT Support of H.323 RAS	(2)	No	No	No	Yes
iBGP Multipath Load Sharing	(2)	Yes	Yes	Yes	Yes
Management					
MPLS Label Distribution Protocol MIB	(2)	No	No	No	No
MPLS Label Switching Router MIB	(2)	No	No	No	No
MPLS Traffic Engineering MIB	(2)	No	No	No	No
SA Agent Support for Application Monitoring, Frame Relay, VoIP, and MPLS VPN	(2)	Yes	Yes	Yes	Yes
SNMP Trap Support for VSI Master MIB	(2)	No	No	No	No
Miscellaneous					
Circuit Interface Identification Persistence for SNMP	(2)	Yes	Yes	Yes	Yes
CNS Configuration Agent	(2)	Yes	Yes	Yes	Yes
CNS Event Agent	(2)	Yes	Yes	Yes	Yes
Interface Alias Long Name Support for SNMP	(2)	Yes	Yes	Yes	Yes
Interface Index Display	(2)	Yes	Yes	Yes	Yes
Protocols					
MPLS Label Distribution Protocol	(2)	No	No	No	No
Quality of Service					
Class-Based Frame-Relay DE-Bit Matching and Marking	(2)	Yes	Yes	Yes	Yes
MPLS QoS Multi-VC Mode for PA-A3	(2)	Yes	Yes	Yes	Yes
Security					
DF Bit Override Functionality with IPSec Tunnels	(2)	No	Yes	Yes	No
Switching					
Netflow Multiple Export Destinations	(2)	Yes	Yes	Yes	Yes
Voice Services					
H.323 Version 2 Phase 2	(2)	Yes	No	No	No
SS7 Gateway Support	(2)	Yes	Yes	Yes	Yes

Table 13 Feature List by Feature Set for the Cisco 7500 Series, Part 2

Features	In	Software Images by Feature Sets			
		IP/FW/IDS IPSec 56	IP/FW/IDS IPSec 3DES	Enterprise	Enterprise IPSec 56
Broadband					
DHCP Option 82 Support for Routed Bridge Encapsulation	(2)	Yes	Yes	Yes	Yes
IP Routing					
BGP Link Bandwidth	(2)	Yes	Yes	Yes	Yes
Distributed Time-Based Access Lists	(2)	Yes	Yes	Yes	Yes
IPv6 for Cisco IOS Software	(2)	Yes	Yes	Yes	Yes
Mobile IP MIB Support for SNMP	(2)	Yes	Yes	Yes	Yes
NAT Support of H.323 RAS	(2)	Yes	Yes	Yes	Yes
iBGP Multipath Load Sharing	(2)	Yes	Yes	Yes	Yes
Management					
MPLS Label Distribution Protocol MIB	(2)	No	No	Yes	Yes
MPLS Label Switching Router MIB	(2)	No	No	Yes	Yes
MPLS Traffic Engineering MIB	(2)	No	No	Yes	Yes
SA Agent Support for Application Monitoring, Frame Relay, VoIP, and MPLS VPN	(2)	Yes	Yes	Yes	Yes
SNMP Trap Support for VSI Master MIB	(2)	No	No	Yes	Yes
Miscellaneous					
Circuit Interface Identification Persistence for SNMP	(2)	Yes	Yes	Yes	Yes
CNS Configuration Agent	(2)	Yes	Yes	Yes	Yes
CNS Event Agent	(2)	Yes	Yes	Yes	Yes
Interface Alias Long Name Support for SNMP	(2)	Yes	Yes	Yes	Yes
Interface Index Display	(2)	Yes	Yes	Yes	Yes
Protocols					
MPLS Label Distribution Protocol	(2)	No	No	Yes	Yes
Quality of Service					
Class-Based Frame-Relay DE-Bit Matching and Marking	(2)	Yes	Yes	Yes	Yes
MPLS QoS Multi-VC Mode for PA-A3	(2)	Yes	Yes	Yes	Yes
Security					
DF Bit Override Functionality with IPSec Tunnels	(2)	Yes	Yes	No	Yes
Switching					
Netflow Multiple Export Destinations	(2)	Yes	Yes	Yes	Yes

Table 13 Feature List by Feature Set for the Cisco 7500 Series, Part 2 (continued)

Features	In	Software Images by Feature Sets			
		IP/FW/IDS IPSec 56	IP/FW/IDS IPSec 3DES	Enterprise	Enterprise IPSec 56
Voice Services					
H.323 Version 2 Phase 2	(2)	No	No	Yes	No
SS7 Gateway Support	(2)	Yes	Yes	Yes	Yes

Table 14 Feature List by Feature Set for the Cisco 7500 Series, Part 3

Features	In	Software Images by Feature Sets			
		Enterprise IPSec 3DES	Enterprise/ FW/IDS	Enterprise/ FW/IDS IPSec 56	Enterprise/ FW/IDS IPSec 3DES
Broadband					
DHCP Option 82 Support for Routed Bridge Encapsulation	(2)	Yes	Yes	Yes	Yes
IP Routing					
BGP Link Bandwidth	(2)	Yes	Yes	Yes	Yes
Distributed Time-Based Access Lists	(2)	Yes	Yes	Yes	Yes
IPv6 for Cisco IOS Software	(2)	Yes	Yes	Yes	Yes
Mobile IP MIB Support for SNMP	(2)	Yes	Yes	Yes	Yes
NAT Support of H.323 RAS	(2)	Yes	Yes	Yes	Yes
iBGP Multipath Load Sharing	(2)	Yes	Yes	Yes	Yes
Management					
MPLS Label Distribution Protocol MIB	(2)	Yes	Yes	Yes	Yes
MPLS Label Switching Router MIB	(2)	Yes	Yes	Yes	Yes
MPLS Traffic Engineering MIB	(2)	Yes	Yes	Yes	Yes
SA Agent Support for Application Monitoring, Frame Relay, VoIP, and MPLS VPN	(2)	Yes	Yes	Yes	Yes
SNMP Trap Support for VSI Master MIB	(2)	Yes	Yes	Yes	Yes
Miscellaneous					
Circuit Interface Identification Persistence for SNMP	(2)	Yes	Yes	Yes	Yes
CNS Configuration Agent	(2)	Yes	Yes	Yes	Yes
CNS Event Agent	(2)	Yes	Yes	Yes	Yes
Interface Alias Long Name Support for SNMP	(2)	Yes	Yes	Yes	Yes
Interface Index Display	(2)	Yes	Yes	Yes	Yes
Protocols					
MPLS Label Distribution Protocol	(2)	Yes	Yes	Yes	Yes

Table 14 Feature List by Feature Set for the Cisco 7500 Series, Part 3 (continued)

Features	In	Software Images by Feature Sets			
		Enterprise IPSec 3DES	Enterprise/ FW/IDS	Enterprise/ FW/IDS IPSec 56	Enterprise/ FW/IDS IPSec 3DES
Quality of Service					
Class-Based Frame-Relay DE-Bit Matching and Marking	(2)	Yes	Yes	Yes	Yes
MPLS QoS Multi-VC Mode for PA-A3	(2)	Yes	Yes	Yes	Yes
Security					
DF Bit Override Functionality with IPSec Tunnels	(2)	Yes	No	Yes	Yes
Switching					
Netflow Multiple Export Destinations	(2)	Yes	Yes	Yes	Yes
Voice Services					
H.323 Version 2 Phase 2	(2)	No	No	No	No
SS7 Gateway Support	(2)	Yes	Yes	Yes	Yes

Table 15 Feature List by Feature Set for the Cisco 7500 Series, Part 4

Features	In	Software Images by Feature Sets			
		Enterprise/ SNASW	Enterprise/ SNASW IPSec 56	Enterprise/ SNASW IPSec 3DES	Desktop/IBM
Broadband					
DHCP Option 82 Support for Routed Bridge Encapsulation	(2)	Yes	Yes	Yes	Yes
IP Routing					
BGP Link Bandwidth	(2)	Yes	Yes	Yes	Yes
Distributed Time-Based Access Lists	(2)	Yes	Yes	Yes	Yes
IPv6 for Cisco IOS Software	(2)	Yes	Yes	Yes	Yes
Mobile IP MIB Support for SNMP	(2)	Yes	Yes	Yes	Yes
NAT Support of H.323 RAS	(2)	Yes	Yes	Yes	No
iBGP Multipath Load Sharing	(2)	Yes	Yes	Yes	Yes
Management					
MPLS Label Distribution Protocol MIB	(2)	Yes	Yes	Yes	No
MPLS Label Switching Router MIB	(2)	Yes	Yes	Yes	No
MPLS Traffic Engineering MIB	(2)	Yes	Yes	Yes	No
SA Agent Support for Application Monitoring, Frame Relay, VoIP, and MPLS VPN	(2)	Yes	Yes	Yes	No
SNMP Trap Support for VSI Master MIB	(2)	Yes	Yes	Yes	No

Table 15 Feature List by Feature Set for the Cisco 7500 Series, Part 4 (continued)

Features	In	Software Images by Feature Sets			
		Enterprise/ SNASW	Enterprise/ SNASW IPSec 56	Enterprise/ SNASW IPSec 3DES	Desktop/IBM
Miscellaneous					
Circuit Interface Identification Persistence for SNMP	(2)	Yes	Yes	Yes	Yes
CNS Configuration Agent	(2)	Yes	Yes	Yes	Yes
CNS Event Agent	(2)	Yes	Yes	Yes	Yes
Interface Alias Long Name Support for SNMP	(2)	Yes	Yes	Yes	Yes
Interface Index Display	(2)	Yes	Yes	Yes	Yes
Protocols					
MPLS Label Distribution Protocol	(2)	Yes	Yes	Yes	No
Quality of Service					
Class-Based Frame-Relay DE-Bit Matching and Marking	(2)	Yes	Yes	Yes	Yes
MPLS QoS Multi-VC Mode for PA-A3	(2)	Yes	Yes	Yes	Yes
Security					
DF Bit Override Functionality with IPSec Tunnels	(2)	No	Yes	Yes	No
Switching					
Netflow Multiple Export Destinations	(2)	Yes	Yes	Yes	Yes
Voice Services					
H.323 Version 2 Phase 2	(2)	No	No	No	No
SS7 Gateway Support	(2)	Yes	Yes	Yes	No

Table 16 Feature List by Feature Set for the Cisco 7500 Series, Part 5

Features	In	Software Images by Feature Sets			
		Desktop/IBM IPSec 56	Desktop/ IBM/FW/IDS	Desktop/ IBM/FW/IDS IPSec 56	Desktop/ IBM/FW/IDS IPSec 3DES
Broadband					
DHCP Option 82 Support for Routed Bridge Encapsulation	(2)	Yes	Yes	Yes	Yes
IP Routing					
BGP Link Bandwidth	(2)	Yes	Yes	Yes	Yes
Distributed Time-Based Access Lists	(2)	Yes	Yes	Yes	Yes
IPv6 for Cisco IOS Software	(2)	Yes	Yes	Yes	Yes
Mobile IP MIB Support for SNMP	(2)	Yes	Yes	Yes	Yes
NAT Support of H.323 RAS	(2)	No	Yes	Yes	Yes
iBGP Multipath Load Sharing	(2)	Yes	Yes	Yes	Yes

Table 16 Feature List by Feature Set for the Cisco 7500 Series, Part 5 (continued)

Features	In	Software Images by Feature Sets			
		Desktop/IBM IPSec 56	Desktop/ IBM/FW/IDS	Desktop/ IBM/FW/IDS IPSec 56	Desktop/ IBM/FW/IDS IPSec 3DES
Management					
MPLS Label Distribution Protocol MIB	(2)	No	No	No	No
MPLS Label Switching Router MIB	(2)	No	No	No	No
MPLS Traffic Engineering MIB	(2)	No	No	No	No
SA Agent Support for Application Monitoring, Frame Relay, VoIP, and MPLS VPN	(2)	No	No	No	No
SNMP Trap Support for VSI Master MIB	(2)	No	No	No	No
Miscellaneous					
Circuit Interface Identification Persistence for SNMP	(2)	Yes	Yes	Yes	Yes
CNS Configuration Agent	(2)	Yes	Yes	Yes	Yes
CNS Event Agent	(2)	Yes	Yes	Yes	Yes
Interface Alias Long Name Support for SNMP	(2)	Yes	Yes	Yes	Yes
Interface Index Display	(2)	Yes	Yes	Yes	Yes
Protocols					
MPLS Label Distribution Protocol	(2)	No	No	No	No
Quality of Service					
Class-Based Frame-Relay DE-Bit Matching and Marking	(2)	Yes	Yes	Yes	Yes
MPLS QoS Multi-VC Mode for PA-A3	(2)	Yes	Yes	Yes	Yes
Security					
DF Bit Override Functionality with IPSec Tunnels	(2)	Yes	No	Yes	Yes
Switching					
Netflow Multiple Export Destinations	(2)	Yes	Yes	Yes	Yes
Voice Services					
H.323 Version 2 Phase 2	(2)	No	No	No	No
SS7 Gateway Support	(2)	No	No	No	No

New and Changed Information

The following sections list the new hardware and software features supported by the Cisco 7000 family for Cisco IOS Release 12.2 T.

New Hardware Features in Cisco IOS Release 12.2(2)T

There are no new hardware features supported in Cisco IOS Release 12.2(2)T.

New Software Features in Cisco IOS Release 12.2(2)T

The following new software features are supported by the Cisco 7000 family for Cisco IOS Release 12.2(2)T:

BGP Link Bandwidth

Platforms: Cisco 7100 series, Cisco 7200 series, and Cisco 7500 series routers

The Border Gateway Protocol (BGP) Link Bandwidth feature is used to advertise the bandwidth of an autonomous system exit link as an extended community. The BGP Link Bandwidth feature is supported by the internal BGP (iBGP) and external BGP (eBGP) multipath features. The link bandwidth extended community indicates the preference of an autonomous system exit link in terms of bandwidth. The link bandwidth extended community attribute may be propagated to all iBGP peers and used with the BGP multipath features to configure unequal cost load balancing. When a router receives a route from a directly connected external neighbor and advertises this route to iBGP neighbors, the router may advertise the bandwidth of that link.

Circuit Interface Identification Persistence for SNMP

Platforms: Cisco 7500 series routers

The Circuit Interface MIB (CISCO-CIRCUIT-INTERFACE-MIB) provides a MIB object (cciDescr) that can be used to identify individual circuit-based interfaces for SNMP monitoring. The Circuit Interface Identification Persistence for SNMP feature maintains this user-defined name of the circuit across reboots, allowing the consistent identification of circuit interfaces. Circuit Interface Identification Persistence is enabled using the **snmp mib persist circuit** global configuration command.

Class-Based Frame-Relay DE-Bit Matching and Marking

Platforms: Cisco 7200 series and Cisco 7500 series routers

The Modular QoS CLI in Cisco IOS Release 12.2(2)T has been enhanced to include matching and marking based on the Frame Relay discard eligibility (DE) bit. Frame Relay DE-Bit Matching and Marking is documented as part of the Class-Based Marking feature module.

The discard eligibility (DE) bit in the address field of a Frame Relay frame is used as a method for prioritizing the discarding of frames in congested Frame Relay networks. The Frame Relay DE bit has only one bit and can therefore only have two settings, 0 or 1. If congestion occurs in a Frame Relay network, frames with the DE bit set at 1 are discarded before frames with the DE bit set at 0. Therefore, important traffic should have the DE bit set at 0 while less important traffic should be forwarded with the DE bit set at 1.

The default DE bit setting is 0. The Class-Based Packet Marking feature allows users to change the DE bit setting to 1 for various traffic, giving users the option of keeping the default value of 0 or changing the value to 1. Users can therefore use the Frame Relay DE-Bit marking to prioritize frames in a Frame Relay network.

CNS Configuration Agent

Platforms: Cisco 7100 series, Cisco 7200 series, and Cisco 7500 series routers

The CNS Configuration Agent supports Cisco IOS devices (routers) by providing:

- Initial configurations
- Incremental (partial) configurations
- Synchronized configuration updates

Initial Configuration

When a Cisco IOS device first comes up, it connects to the configuration server component of CNS 1.5 Configuration Agent by establishing a TCP connection. This is done by using a standard CLI command: **cns config initial**. The device issues a request and identifies itself by providing a unique device ID to the configuration server.

When the CNS web server receives a request for a configuration file, it invokes the Java Servlet and executes the corresponding embedded code. This directs the CNS web server to access the directory server and file system to read the configuration reference for this device (device ID) and template. The configuration agent prepares an instantiated configuration file by substituting all the parameter values specified in the template with valid values for this device. The configuration server forwards the configuration file to the CNS web server for transmission to the Cisco IOS device.

The CNS Configuration Agent accepts the configuration file from the CNS web server, performs XML parsing, syntax checking (optional), and loads the configuration file. The Cisco IOS device reports the status of the configuration load as an event that can be subscribed to by a network monitoring or workflow application.

Incremental Configuration

Once the network is up and running, new services can be added using the CNS Configuration Agent. Incremental (partial) configurations can be sent to IOS devices. The actual configuration can be sent as an event payload by way of the event gateway (push operation) or as a signal event that triggers the device to initiate a pull operation.

The IOS device can check the syntax of the configuration before applying it. If successful, the IOS device applies the incremental configuration and publishes an event that signals success to the configuration server. If the device fails to apply the incremental configuration, it publishes an event that indicates an error status.

Once the IOS device has applied the incremental configuration, it can write it to NVRAM, or wait until signaled to do so.

Synchronized Configurations

When an IOS device receives a configuration, it has the option to defer the application of the configuration upon receipt of a write-signal event. This feature allows the device configuration to be synchronized with other dependent network activities.

Benefits

- Provides an automatic mechanism for delivering configuration files to IOS devices.
- Enables dynamic creation of configuration files using information from a directory repository.

- Employs an open scalable architecture.
- Supports event-based provisioning interface for partial configurations.

CNS Event Agent

Platforms: Cisco 7100 series, Cisco 7200 series, and Cisco 7500 series routers

Cisco Networking Services (CNS) is a foundation technology for linking users to network services. CNS Software Developers Kit (SDK) accomplishes this linking by making applications network-aware and increasing the intelligence of the network elements. CNS SDK provides building blocks to a range of customers in market segments such as enterprise, service provider, independent software vendors, and system integrators.

The CNS Event Agent is part of the Cisco IOS infrastructure that allows Cisco IOS applications to publish and subscribe to events on a CNS Event Bus. CNS Event Agent works in conjunction with the CNS Configuration Agent feature.

Control Plane DSCP Support for RSVP

Platforms: Cisco 7200 series routers

The Control Plane DSCP Support for RSVP feature allows you to set the priority value in the type of service (ToS) byte/differentiated services (DiffServ) field in the Internet Protocol (IP) header for RSVP signaling messages. The IP header functions with resource providers such as Weighted Fair Queueing (WFQ), so that voice frames have priority over data fragments and data frames. When packets arrive in a router's output queue, the voice packets are placed ahead of the data frames.

There is one new command:

ip rsvp signalling dscp [value]—Specifies the DSCP to be used on all RSVP messages transmitted on an interface.

There is one modified command:

show ip rsvp interface detail—The keyword, **detail**, was added to display information about RSVP interface parameters.

DF Bit Override Functionality with IPSec Tunnels

Platforms: Cisco 7100 series, Cisco 7200 series, and Cisco 7500 series routers

The DF Bit Override Functionality with IPSec Tunnels feature allows customers to configure the setting of the DF bit when encapsulating tunnel mode IPSec traffic on a global or per-interface level. Thus, if the DF bit is set to clear, routers can fragment packets regardless of the original DF bit setting.

DHCP Option 82 Support for Routed Bridge Encapsulation

Platforms: Cisco 7200 series and Cisco 7500 series routers

The DHCP Option 82 Support for Routed Bridge Encapsulation feature provides support for the DHCP relay agent information option when ATM routed bridge encapsulation (RBE) is used.

This feature enables the DHCP relay agent to communicate information to the DHCP server using a suboption of the DHCP relay agent information option called agent remote ID. The information sent in agent remote ID includes an IP address identifying the relay agent and information about the ATM interface and the PVC over which the DHCP request came in. The DHCP server can use this information to make IP address assignments and security policy decisions.

Distinguished Name-Based Crypto Maps

Platforms: Cisco 7100 series and Cisco 7200 series routers

The Distinguished Name-Based Crypto Maps feature allows you to restrict access to selected encrypted interfaces to peers with specific certificates, especially certificates with particular Distinguished Names (DNs).

Initially, if the router accepted a certificate or a shared secret from the encrypting peer, Cisco IOS did not have a method of preventing the peer from communicating with any encrypted interface other than the restrictions on the IP address of the encrypting peer. This feature allows you to configure which crypto maps are usable to a peer based on the DN that a peer used to authenticate itself; thus enabling you to control which encrypted interfaces a peer with a specified DN can access.

Distributed Time-Based Access Lists

Platforms: Cisco 7500 series routers

Cisco IOS allows implementation of access lists based on the time of day. To do so, you create a time range that defines specific times of the day and week. The time range is identified by a name and then referenced by a function, so that those time restrictions are imposed on the function itself.

Currently, IP and IPX extended access lists are the only functions that can use time ranges. The time range allows the network administrator to define when the permit or deny statements in the access list are in effect.

Before the introduction of the Distributed Time-Based Access Lists feature, time-based access lists were not supported on line cards for the Cisco 7500 series routers. If time-based access lists were configured, they behaved as normal access lists. If an interface on a line card was configured with access lists, the packets switched into the interface were not distributed switched through the line card but forwarded to the route processor for processing.

The Distributed Time-Based Access Lists feature allows packets destined for an interface configured with time-based access lists to be distributed switched through the line card.

For this functionality to work, the software clock must remain synchronized between the route processor and the line card. This synchronization occurs through an exchange of ipc (interprocess communications) messages from the route processor to the line card. When a time range or a time-range entry is changed, added, or deleted, an ipc message is sent by the route processor to the line card.

Benefits

The Distributed Time-Based Access Lists feature gives network administrators more control over permitting or denying a user access to resources. Customers can now take advantage of the performance benefits of distributed switching and the flexibility given by time-based access lists.

Enhancements to H.323 Call Statistics

Platforms: Cisco 7200 series routers

Beginning with Cisco IOS Release 12.2(4)T, enhancements to H.323 call statistics allow you to clear the gateway counters, display H.323 messages that have been sent and received, obtain statistics on the reasons calls are disconnected, and display debug output for various components within the H.323 subsystem. To enable these enhancements, the following commands have been added or modified: clear h323 gateway, show h323 gateway, and debug cch323.

The following subsection provides a brief description of the H.323 standard, H.323 gateways, and their roles in the communications process. The "Command Reference" section provides a description of the commands that have been added or modified. The command enhancements do not affect configuration in any way; therefore, there are no configuration sections in this document.

H.323 Standard and H.323 Gateways

The International Telecommunication Union (ITU) H.323 standard provides for sending and receiving audio, video, and data on an IP-based internetwork.

An H.323 gateway is an endpoint on a LAN that provides real-time, two-way communication between H.323 terminals on the LAN and other ITU terminals on the WAN. An H.323 gateway can also communicate with another H.323 gateway. Gateways allow H.323 terminals to communicate with non-H.323 terminals by converting protocols. The gateway is the point at which a circuit-switched call is encoded and repackaged into IP packets. In an environment in which both gatekeepers and gateways are used, only gateways are configured to send Voice over IP (VoIP) data.

Gateways communicate with gatekeepers using the Registration, Admission, and Status (RAS) protocol. The gatekeeper maintains resource availability information, which it uses to select the appropriate gateway during the admission of a call.

Two important phases of H.323 call signaling are call setup and call termination. Either gateway may terminate a call.

High Performance Gatekeeper

Platforms: Cisco 7200 series routers

The Cisco High Performance Gatekeeper feature introduces new gatekeeper functionality and modifications for facilitating carrier-class reliability, security, and performance into the Cisco Voice Network solution portfolio. These H.323 standard-based features have carrier-grade reliability and performance characteristics with a robust open application protocol interface to enable development of enhanced applications like voice VPNs and wholesale voice solutions.

The new gatekeeper is characterized by the following:

- Increased support for back end applications
- Increased performance on a single gatekeeper
- Alternate gatekeeper support to the gatekeeper. Each alternate gatekeeper, or GK node, shares its local zone information so that the cluster can effectively manage all local zones within the cluster. Each alternate gatekeeper has a unique local zone. Clusters provide a mechanism for distributing call processing seamlessly across a converged IP network infrastructure to support IP telephony, facilitate redundancy, and provide feature transparency and scalability.

This feature addresses the scalability, redundancy, and performance aspects of the gatekeeper as part of the Cisco Multimedia Conference Manager (MCM) to present a complete Cisco solution. The Cisco H.323 MCM provides the network administrator with the ability to identify H.323 traffic and to apply appropriate policies. The Cisco H.323 Multimedia Conference Manager is implemented on Cisco IOS software and enables a network manager to do the following:

- Limit the H.323 traffic on the LAN and WAN.
- Provide user accounting for records based on the service utilization.
- Inject quality of service (QoS) parameters for the H.323 traffic generated by applications such as VoIP, data conferencing, and video conferencing.
- Provide the mechanism to implement security for H.323 communications.

H.323 Call Redirection Enhancements

Platforms: Cisco 7200 series routers

The H.323 call redirection enhancements feature includes support for two facilityReason fields in the user-to-user information element (UUIE) of the H.323 Facility message: routeCallToGatekeeper and callForwarded. These enhancements also provide a non-standard method for using the Facility message to effect call transfer.

The user-to-user information element (UUIE) of the Facility message is used primarily for call redirection. The UUIE contains a field, facilityReason, that indicates the nature of the redirection. The H.323 Call Redirection Enhancements feature adds support for two of the reasons: routeCallToGatekeeper and callForwarded. It also provides a non-standard method for using the Facility message to effect call transfer.

H.323 Version 2 Phase 2

Platforms: Cisco 7200 series and Cisco 7500 series routers

Cisco H.323 Version 2 Phase 2 upgrades Cisco IOS software by adding several optional features of the H.323 Version 2 specification and facilitates customized extensions to the Cisco Gatekeeper.

H.323v2 Fast Connect

The Fast Connect feature allows endpoints to establish media channels without waiting for a separate H.245 connection to be opened. This streamlines the number of messages that are exchanged and the amount of processing that must be done before endpoint connections can be established.

H.245 Tunneling

Through H.245 tunneling, H.245 messages are encapsulated within Q.931 messages without using a separate H.245 TCP connection. When tunneling is enabled, one or more H.245 messages can be encapsulated in any Q.931 message. H.245 tunneling is not supported as a standalone feature; initiation of H.245 tunneling procedures can be initiated only by using the **dtmf-relay** command, and only from an active Fast Connect call. Furthermore, if dtmf-relay is configured on a Version 2 VoIP dial peer and the active call has been established by using Fast Connect, tunneling procedures initiated by the opposite endpoint are accepted and supported. H.245 tunneling is backward-compatible with H.323 Version 1 configurations.

H.450.2 Call Transfer

Call Transfer allows an H.323 endpoint to redirect an answered call to another H.323 endpoint. Cisco gateways support H.450.2 Call Transfer as the transferred and transferred-to party. The transferring endpoint must be an H.450-capable terminal; the Cisco gateway cannot act as the transferring endpoint. Gatekeeper-controlled or Gatekeeper-initiated Call Transfer is not supported.

H.450.3 Call Deflection

Call Deflection is a feature under H.450.3 Call Diversion (Call Forwarding) that allows a called H.323 endpoint to redirect the unanswered call to another H.323 endpoint. Cisco gateways support H.450.3 Call Deflection as the originating, deflecting, and deflected-to gateway. The Cisco gateway as the deflecting gateway will support invocation of Call Deflection only by using an incoming PRI QSIG message (a Call Deflection cannot be invoked by using any other trunk type).

H.323 Version 2 Phase 2 does not support Gatekeeper-controlled or Gatekeeper initiated Call Deflection.

Hookflash Relay

A hookflash indication is a brief on-hook condition during a call. The indication is not long enough in duration to be interpreted as a signal to disconnect the call. You can create a hookflash indication by quickly depressing and releasing the hook on your telephone.

PBXs and telephone switches are frequently programmed to intercept hookflash indications and use them as a way to allow a user to invoke supplemental services. For example, your local service provider might allow you to enter a hookflash as a means of switching between calls if you subscribe to a call-waiting service. In the traditional telephone network, a hookflash results in a voltage change on the telephone line. Because there is no equivalent of this voltage change in an IP network, the ITU H.245 standard defines a message representing a hookflash. To send a hookflash indication using this message, an H.323 endpoint sends an H.245 user input indication message containing an “H.245-signal” or “H.245-alpha” structure with a value of “!”. This value represents a hookflash indication.

H.235 Security

Security for Registration, Admission, and Status protocol (RAS) signaling between H.323 endpoints and Gatekeepers is enhanced in H.323 Version 2 Phase 2 by including secure endpoint registration of the Cisco gateway to the Cisco Gatekeeper and secure per-call authentication. The authentication type is “password with hashing” as described in ITU H.235. Specifically, the encryption method is MD5 with password hashing. This functionality is provided by the security token required-for CLI on the Gatekeeper and the security password CLI on the gateway.

GKTMP

The Gatekeeper Transaction Message Protocol (GKTMP) for the Cisco Gatekeeper provides a transaction-oriented application protocol that allows an external application to modify Gatekeeper behavior by processing specified RAS messages.

You can specify a set of triggers that use RAS messages that the Gatekeeper recognizes. Triggers are specified filter conditions that must match each type of RAS message. These triggers can be registered dynamically by using the external application, or you can configure this information by using the CLI on the Gatekeeper.

Gateway Support for Alternate Endpoints

The Alternate Endpoint feature allows a Gatekeeper to specify alternative destinations for a call when queried with an Admission Request (ARQ) by an originating gateway. If the first destination gateway fails to connect, the Gatekeeper tries all the alternate destinations before going to the next dial peer rotary (if a rotary is configured).

This feature is not supported by the Cisco Gatekeeper; it is intended for use with third-party Gatekeepers that implement the Alternate Endpoint field in the ACF message. No support is provided for the gateway to send a list of alternate endpoints in RRQ messages.

Gateway Support for a Network-Based Billing Number

This feature informs the Gatekeeper of the specific voice port or T1/E1 span from which an incoming call entered the ingress gateway. This is done using a Cisco proprietary, nonstandard field that has been added to the Admission Request (ARQ) message sent by the ingress gateway. No configuration is necessary for this feature.

Gateway Support for Voice-Port Description

This feature provides the Gatekeeper with a configurable string that identifies the voice port or T1/E1 span from which an incoming call entered the ingress gateway.

This is done using a Cisco proprietary, nonstandard field that has been added to the ARQ message sent by the ingress gateway. The string in the ARQ corresponds to the setting of the **voice-port description** command. This feature is similar to the Network-Based Billing Number feature, but differs in two important respects:

- The voice-port description field is only included in the ARQ if the voice-port description is configured through the CLI for the applicable voice port.
- Because the voice-port description is configurable, the user can provide customer-specific information to the Gatekeeper. For example, the voice-port description can be configured to correspond to the Carrier Identification Code (CIC) for calls received on a particular T1/E1 Span.

iBGP Multipath Load Sharing

Platforms: Cisco 7100 series, Cisco 7200 series, and Cisco 7500 series routers

The iBGP Multipath Load Sharing feature allows the user to configure multiple internal BGP best paths. This enables a router to evenly share the traffic destined for a particular site.

When a Border Gateway Protocol (BGP) speaker router with no local policy configured receives multiple network layer reachability information (NLRI) from the internal BGP for the same destination, the router will choose one internal BGP path as the best path. The best path is then installed in the IP routing table of the router.

The Internal BGP Multipath Load Sharing feature enables the BGP speaker router to select multiple internal BGP paths as the best paths to a destination. The best paths or multipaths are then installed in the IP routing table of the router.

For multiple paths to the same destination to be considered as multipaths, the following criteria must be met:

- All attributes must be the same. The attributes include weight, local preference, autonomous system path (entire attribute and not just length), origin code, Multiple Exit Discriminator (MED), and Interior Gateway Protocol (IGP) distance.
- The next hop router for each multipath must be different.

Even if the criteria are met and multiple paths are considered multipaths, the BGP speaker router will still designate one of the multipaths as the best path and advertise this best path to its neighbors.

IPv6 for Cisco IOS Software

Platforms: Cisco 7100 series, Cisco 7200 series, and Cisco 7500 series routers

The Internet Protocol (IP) is a packet-based protocol used to exchange data, voice, and video traffic over digital networks. IP handles addressing, fragmentation, reassembly, and protocol demultiplexing. It is the foundation on which all other IP protocols (collectively referred to as the IP Protocol suite) are built. A network-layer protocol, IP contains addressing and control information that allows data packets to be routed. IPv6, formerly called IPng (next generation), is a replacement for the current version of IP (version 4).

Interface Alias Long Name Support for SNMP

Platforms: Cisco 7100 series, Cisco 7200 series, and Cisco 7500 series routers

The Interface Alias (IfAlias) is a user-specified description of an interface used for SNMP network management. The IfAlias is an object in the Interfaces Group MIB (IF-MIB) that can be set by a network manager to "name" an interface. The IfAlias value for an interface or subinterface can be set using the **description** command in interface configuration mode, or by using a Set operation from a Network Management System.

Prior to this release, IfAlias descriptions for subinterfaces were limited to 64 characters. A new Cisco IOS software command, **snmp ifmib ifalias long**, configures the system to handle IfAlias descriptions of up to 256 characters. IfAlias descriptions appear in the output of the **show interfaces** CLI command.

Interface Index Display

Platforms: Cisco 7100 series, Cisco 7200 series, and Cisco 7500 series routers

The Interface Index (IfIndex) is a user-specified identification number for an interface used in SNMP network management. The IfIndex is an object in the Interfaces Group MIB (IF-MIB) that can be set by a network manager to consistently identify an interface. A new Cisco IOS software command, **show snmp mib ifmib ifindex**, allows the user to view the IfIndex identification numbers assigned to interfaces and subinterfaces using the CLI. This provides a way to view these values without the need for a Network Management Station.

IOS Server Load Balancing

Platforms: Cisco 7200 series routers

The IOS Server Load Balancing (SLB) feature is an IOS-based solution that provides IP server load balancing. Using the IOS Sever Load Balancing (SLB) feature, you can define a *virtual server* that represents a group of *real servers* in a cluster of network servers known as a *server farm*. In this environment, the clients connect to the IP address of the virtual server. When a client initiates a connection to the virtual server, the IOS SLB function chooses a real server for the connection based on a configured load-balancing algorithm.

IOS SLB also provides firewall load balancing, which balances flows across a group of firewalls called a *firewall farm*.

Low Latency Queueing Enhancement-Priority Percentage Support

Platforms: Cisco 7100 series and Cisco 7200 series

The Low Latency Queueing Enhancement-Priority Percentage Support feature allows you to configure bandwidth as a percentage within low latency queueing (LLQ). Specifically, you can designate a percentage of the bandwidth to be allocated to an entity (such as a physical interface, a shaped ATM permanent virtual circuit (PVC), or a shaped Frame Relay PVC) to which a policy map is attached. Traffic associated with the policy map will then be given priority treatment. This feature also allows you to specify the percentage of bandwidth to be allocated to nonpriority traffic classes.

This feature modifies two existing commands—**bandwidth** and **priority**. This feature adds a new keyword to the **bandwidth** command—**remaining percent**. The feature also changes the functionality of the existing **percent** keyword. These changes result in the following commands for bandwidth: **bandwidth percent** and **bandwidth remaining percent**. The **bandwidth percent** command configures bandwidth as an absolute percentage of the total bandwidth on the interface. The **bandwidth remaining**

percent command allows you to allocate bandwidth as a relative percentage of the total bandwidth available on the interface. This command allows you to specify the relative percentage of the bandwidth to be allocated to the classes of traffic.

This feature also adds the **percent** keyword to the **priority** command. The **priority percent** command indicates that the bandwidth will be allocated as a percentage of the total bandwidth of the interface. You can then specify the percentage (that is, a number from 1 to 100) to be allocated by using the *percentage* argument with the **priority percent** command.

Unlike the **bandwidth** command, the **priority** command provides a strict priority to the traffic class, which ensures low latency to high priority traffic classes.

MGCP CAS PBX and PRI Backhaul on Cisco 7200 Routers

Platforms: Cisco 7200 series and Cisco 7500 series routers

The MGCP CAS PBX feature extends the earlier Simple Gateway Control Protocol (SGCP) channel-associated signaling (CAS) onto the merged SGCP/MGCP software base to enable various service provider solutions. MGCP CAS PBX provides the following benefits:

- CAS termination and translation to MGCP on Business Gateways (BGWs) and Trunking Gateways (TGWs)
- Digital CAS (E&M) interfaces are supported in addition to the analog (FXO, FXS, and E&M) interfaces.
- Support for CAS PBX and Feature Group D CAS functions
- MGCP 0.1 has been expanded to support CAS packages that handle CAS PBX and Feature Group D CAS functions, including Barge-In/Busy Line Verify, and 911 capabilities on the TGW.

The essential difference for current SGCP users is that support for the SGCP application has been replaced with the MGCP application. The MGCP application supports both SGCP commands and MGCP commands, permitting access to a larger feature set than with the SGCP application alone. The MGCP CAS PBX software assumes the MGCP mode as the default environment. This allows the gateway to recognize MGCP messages sent by the call agent.

The PRI/Q.931 Signaling Backhaul feature enables you to reliably transport the signaling (Q.931 and above layers) from a PRI trunk that is physically connected to a media gateway (for example, a Cisco 7200 series router) to a media gateway controller (Cisco VSC3000) for processing. Additionally, the Cisco VSC3000 can respond through the same interface.

Signaling backhaul takes place between a media gateway and a VSC. Gateways provide an interface between the Public Switched Telephone Network (PSTN) and the packet network world (IP or ATM). The VSC provides call processing and gateway control. Signaling backhaul is the ability to reliably pass as many layers of a protocol stack as possible through a gateway directly to a VSC.

Signaling backhaul occurs at a common boundary for all protocols. For ISDN, the signaling backhaul takes place at the Layer 2 (Q.921) and Layer 3 (Q.931) boundary. The lower layers of the protocol are terminated and processed on the gateway, while the upper layers are backhauled to the VSC. The upper layers of the protocol are backhauled, or transported, to the VSC using Reliable User Datagram Protocol (RUDP) over IP. RUDP provides autonomous notification of connected and failed sessions, and in-sequence, guaranteed delivery of signaling protocols across an IP network. Backhaul session manager is a software function on the VSC and gateway that manages RUDP sessions. The session manager groups sessions between endpoints, establishes a selection priority, and collects these groups together to form a set.

Signaling backhaul provides the additional advantage of distributed protocol processing, enabling greater expandability and scalability while offloading lower layer protocol processing from the VSC.

Mobile IP MIB Support for SNMP

Platforms: Cisco 7100 series, Cisco 7200 series, and Cisco 7500 series routers

The Mobile IP MIB Support for SNMP feature adds a MIB module that expands network monitoring capabilities of Foreign Agent (FA) and Home Agent (HA) Mobile IP Entities. Mobile IP management using SNMP is defined in two MIBs: the RFC2006-MIB and the CISCO-MOBILE-IP-MIB. The Cisco Mobile IP MIB is a Cisco enterprise-specific extension to IETF RFC 2006 MIB module that allows you to monitor the total number of HA Mobile bindings and the total number of FA visitor bindings. This release also adds support for RFC 2006 Set operations and a SNMP notification. Set operations (performed from a Network Management System) are supported for starting and stopping the mobile IP service, configuring security associations, modifying advertisement parameters, and configuring "care-of addresses" for foreign agents. An SNMP notification (trap or inform) for security violations can be enabled on supported routing devices using the **snmp-server enable traps ipmobile** and **snmp-server host** global configuration CLI commands. As this feature affects security, use of SNMPv3 is strongly recommended.

For further details, see the *Mobile IP MIB Support for SNMP* feature guide at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t1/ft1mip.htm

Modem Script and System Script Support in LSDO

Platforms: Cisco 7200 series routers

The Modem and System Chat Script Support in Large-Scale Dial-Out Networks feature allows users to use modem and system chat scripts by linking them to AAA service outbound attributes for use by Cisco network access servers in large-scale dial-out networks. Currently, the large-scale dial-out network architecture does not allow chat scripts for a particular session to be passed through the network.

The Modem and System Chat Script Support in Large-Scale Dial-Out Networks feature allows modem and system chat scripts to pass through large-scale dialout networks by allocating two new authentication, authorization, and accounting (AAA) attributes for outbound service. The Modem and System Chat Script Support in Large-Scale Dial-Out Networks feature provides two new outbound service attributes for passing chat scripts, modem-script and system-script. Large-scale dial-out supports Cisco attribute-value (AV) pairs and TACACS+ attributes.

MPLS QoS Multi-VC Mode for PA-A3

Platforms: Cisco 7200 series and Cisco 7500 series routers

MPLS quality of service (QoS) functionality enables network administrators to satisfy a wide range of requirements in transmitting IP packets through an MPLS-enabled network.

In general, MPLS QoS enables the duplication of Cisco IOS IP QoS (Layer 3) functions on MPLS devices, including label edge routers (LERs), label switching routers (LSRs), and Asynchronous Transfer Mode LSRs (ATM-LSRs). MPLS QoS functions map nearly one-for-one to IP QoS functions on all types of interfaces.

The MPLS QoS Multi-VC Mode feature provides the following significant benefits:

- Ensures effective deployment of differentiated service classes in an MPLS-enabled ATM network.
- Leverages the use of existing ATM infrastructures.

MPLS Label Distribution Protocol

Platforms: Cisco 7200 series and Cisco 7500 series routers

The Cisco MPLS Label Distribution Protocol (LDP) allows the construction of highly scalable and flexible IP Virtual Private Networks (VPNs) that support multiple levels of services.

LDP provides a standard methodology for hop-by-hop distribution of labels in an MPLS network by assigning labels to routes that have been chosen by the underlying Interior Gateway Protocol (IGP) routing protocols. The resulting label switch paths (LSPs) forward label traffic across an MPLS backbone to particular destinations. These capabilities enable service providers to implement Cisco MPLS-based IP VPNs and IP+ATM services across multivendor MPLS networks.

LDP enables label switching routers (LSRs) to request, distribute, and release label prefix binding information to peer routers in a network. Thus, LSRs can discover potential peers and establish LDP sessions with those peers to exchange label binding information.

LDP is a superset of the Cisco prestandard Tag Distribution Protocol (TDP), which also supports MPLS forwarding along normally routed paths. For the features that LDP and TDP share in common, the pattern of protocol exchange between network routing platforms is identical. The differences between LDP and TDP for those features supported by both protocols are largely embedded in their respective implementation details, such as the encoding of protocol messages.

This release of LDP supports both the LDP and TDP protocols and provides the means for transitioning an existing network from a TDP environment to an LDP environment. Thus, you can run LDP and TDP simultaneously on any router platform. The routing protocol that you select can be configured on a per-interface basis for directly connected neighbors and on a per-session basis for nondirectly connected (targeted) neighbors. In addition, an LSP across an MPLS network can be supported by LDP on some hops and by TDP on other hops.

MPLS Label Distribution Protocol MIB

Platforms: Cisco 7200 series and Cisco 7500 series routers

The MPLS Label Distribution Protocol (LDP) MIB is an idealized label switching database that provides an effective management infrastructure for using LDP in an MPLS network.

The notation used in the MPLS LDP MIB adheres to the conventions defined in the Abstract System Notation One (ASN.1) standard, which defines an Open System Interconnection (OSI) language used in describing data types independently from particular computer structures and presentation techniques.

Each object in the MPLS LDP MIB incorporates a DESCRIPTION field that describes the object's meaning and usage, which, together with other object characteristics, provides information that enables network administrators to monitor and control network devices, measure network performance, and collect network statistics.

MPLS Label Switching Router MIB

Platforms: Cisco 7200 series and Cisco 7500 series routers

The MPLS Label Switching Router MIB allows you to use the Simple Network Management Protocol (SNMP) to remotely monitor a label switching router (LSR) that is using the Multiprotocol Label Switching (MPLS) technology. The MPLS-LSR-MIB mirrors the Cisco Label Switching subsystem, specifically, the LSR management information that is provided by the label forwarding information base (LFIB).

The MPLS-LSR-MIB contains managed objects that support the retrieval of label switching information from a router and is based on Revision 05 of the IEFT MPLS-LSR-MIB. This implementation enables a network administrator to get information on the status, character, and performance of the following:

- MPLS-capable interfaces on the LSR
- Incoming MPLS segments (labels) to an LSR and their associated parameters
- Outgoing segments (labels) at an LSR and their associated parameters

In addition, the network manager can retrieve the status of cross-connect entries that associate MPLS segments together.

MPLS Traffic Engineering MIB

Platforms: Cisco 7200 series and Cisco 7500 series routers

The MPLS Traffic Engineering (TE) MIB enables a standardized, SNMP-based approach to managing the MPLS traffic engineering features in Cisco IOS. Providing this capability requires SNMP agent code implementation of the MPLS TE MIB.

The MPLS TE MIB is based on an IETF draft MIB that includes objects describing features that support MPLS traffic engineering. The implementation of the MPLS TE MIB within Cisco IOS closely corresponds to the features described in the IETF draft MIB.

Some slight differences between the IETF draft MIB and the actual implementation of the traffic engineering capabilities within Cisco IOS require some minor translations between the MPLS TE MIB and the internal data structures of Cisco IOS. These translations are accomplished by means of the SNMP agent code. Also, while running as a low priority process, the SNMP agent provides a management interface to Cisco IOS.

The Cisco MPLS TE MIB implementation tracks the following version of the IETF draft MIB: *draft-ietf-mpls-te-mib-05.txt*. This IETF draft document is continually being evolved toward the status of a standard and will undergo revisions from time to time. Accordingly, the Cisco implementation of the MPLS TE MIB is expected to track the evolution of the IETF draft MIB.

The SNMP objects defined in the MPLS TE MIB can be viewed by any standard SNMP management utility. All MPLS TE MIB objects are based on the IETF draft MIB; accordingly, no specific Cisco-developed applications are required to support the MPLS TE MIB.

Benefits of the MPLS Traffic Engineering MIB

The MPLS Traffic Engineering MIB provides the following benefits:

- Provides a standards-based SNMP interface for retrieving information about MPLS traffic engineering.
- Provides information about the traffic flows on MPLS traffic engineering tunnels.
- Presents MPLS traffic engineering tunnel routes, including the configured route, the IGP calculated route, and the actual route traversed.
- Provides information, in conjunction with the Interface MIB, about how a tunnel was rerouted in the event of a link failure.
- Provides information about the configured resources used for an MPLS traffic engineering tunnel.

Functional Structure of the MPLS TE MIB

The SNMP agent code supporting the MPLS TE MIB follows the existing model for such code in Cisco IOS and is, in part, generated by the IOS tool set, based on the MIB source code.

The SNMP agent code, which has a layered structure that is common to MIB support code in Cisco IOS, consists of four layers:

- Platform independent layer—This layer is generated primarily by the MIB development IOS tool set and incorporates platform and implementation independent functions. The IOS MIB development tool set creates a standard set of files associated with a MIB.
- Application interface layer—The functions, names, and template code for MIB objects in this layer are also generated by the MIB development IOS tool set.
- Application specific layer—This layer provides an interface between the application interface layer and the API and data structures layer below and performs tasks needed to retrieve required information from IOS, such as searching through data structures.
- API and data structures layer—This layer contains the data structures or APIs within IOS that are retrieved or called in order to set or retrieve SNMP management information.

Restrictions

The following restrictions apply to the MPLS TE MIB for Cisco IOS Release 12.0(14)ST:

- Supports read-only (RO) permission for MIB objects.
- Contains no configuration support for SET functions; only SNMP GET, GETNEXT, and GETBULK retrieval functions are supported in this release.
- Contains no support for TE MIB traps; interface MIB (ifMIB) traps are sent when tunnel interfaces go up or down.
- Contains no support for Guaranteed Bandwidth Traffic Engineering (GBTE) or Auto Bandwidth features.

Related Features and Technologies

The MPLS TE MIB requires the following features and technologies:

- Standards-based SNMP network management utility
- IOS Multiprotocol Label Switching (MPLS) feature
- IOS MPLS Traffic Engineering feature
- IOS MPLS Label Switching Router MIB feature

Related Documents

For descriptions of other MPLS-based functionality associated with Cisco IOS Release 12.0(14)ST, consult the following documentation:

- *MPLS Label Distribution Protocol Enhancements*
- *MPLS Label Switching Router MIB*
- *MPLS Scalability Enhancements for LSC and ATM LSR*
- *Automatic Bandwidth Adjustment for MPLS Traffic Engineering Tunnels*
- *Scalability Enhancements for MPLS Traffic Engineering*
- *MPLS Quality of Service Enhancements*
- *MPLS Traffic Engineering Access List Node Exclusion*
- *RFC 2233 Interfaces MIB*

NAT Support of H.323 RAS

Platforms: Cisco 7100 series, Cisco 7200 series, and Cisco 7500 series routers

Cisco IOS NAT supports all H.225 and H.245 message types, including those sent in the RAS protocol. RAS provides a number of messages that are used by software clients and Voice over IP (VoIP) devices to register their location, request assistance in call setup, and control bandwidth. The RAS messages are directed toward an H.323 gatekeeper.

Some RAS messages include IP addressing information in the payload, typically meant to register a user with the gatekeeper or learn about another user already registered. If these messages are not known to NAT, they cannot be translated to an IP address that will be visible to the public.

Previously, NAT did not support H.323 RAS messages. With this enhancement, embedded IP addresses can be inspected for potential address translation.

NetFlow Multiple Export Destinations

Platforms: Cisco 7200 series and Cisco 7500 series routers

The NetFlow Multiple Export Destinations feature enables configuration of multiple destinations of the NetFlow data. With this feature enabled, two identical streams of NetFlow data are sent to the destination host. Currently, the maximum number of export destinations allowed is two.

The NetFlow Multiple Export Destinations feature improves the chances of receiving complete NetFlow data by providing redundant streams of data. By sending the exact same export data to more than one NetFlow collector, fewer packets will be lost.

PPP over Ethernet Client

Platforms: Cisco 7200 series routers

The PPP over Ethernet Client feature provides PPP over Ethernet (PPPoE) client support on routers or digital subscriber line (DSL) modems on customer premises.

PPPoE client is supported on ATM permanent virtual circuits (PVCs) using a dialer interface for cloning virtual access. One PVC will support one PPPoE client.

Multiple PPPoE clients can run concurrently on different PVCs, but each PPPoE client must use a separate dialer interface and a separate dialer pool. Refer to the

following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/ftpppoec.htm

RSVP Scalability Enhancements

Platforms: Cisco 7200 series routers

RSVP typically performs admission control, classification, policing, and scheduling of data packets on a per-flow basis and keeps a database of information for each flow.

In a network in which the number of flows that RSVP maintains is relatively small, this model functions well. However, to facilitate integration with service provider (differentiated services DiffServ) networks and to enable scalability across enterprise networks, RSVP can now be configured to perform admission control only. You can use class-based weighted fair queueing (CBWFQ) to provide the classification,

policing, and scheduling functions. CBWFQ puts packets into classes based on the differentiated services code point (DSCP) value in the packet's IP header, thereby eliminating the need for per-flow state and per-flow processing.

There are two new commands:

ip rsvp data-packet classification none—Disables data packet classification.

ip rsvp resource-provider {*none* | *wfq interface* | *wfq pvc*}—Configures a resource provider for an aggregate flow.

There is one modified command:

show ip rsvp interface detail—The keyword, **detail**, was added to display information about RSVP interface parameters.

RSVP Support for ATM/PVCs

Platforms: Cisco 7200 series routers

The RSVP support for ATM/PVCs feature allows RSVP to function with per-PVC queueing for voice-like flows. Specifically, RSVP can install reservations on PVCs defined at the interface and subinterface levels. There is no limit to the number of PVCs that can be configured per interface or subinterface.

There are two new commands:

ip rsvp layer2 overhead [*h c n*]—Controls the overhead accounting performed by RSVP/WFQ when a flow is admitted onto an ATM PVC.

ip rsvp resource-provider {*none* | *wfq interface* | *wfq pvc*}—Configures a resource provider for an aggregate flow.

There is one modified command:

show ip rsvp interface detail—The keyword, **detail**, was added to display information about RSVP interface parameters.

SA Agent Support for Application Monitoring, Frame Relay, VoIP, and MPLS VPN

Platforms: Cisco 7200 series and Cisco 7500 series routers

The Cisco Service Assurance Agent (SA Agent) is a Cisco IOS software network monitoring solution. This enhancement to the Cisco SA Agent provides the following features: Application Performance Monitoring, Frame Relay Monitoring, Path Jitter, and MPLS VPN awareness.

SA Agent Application Performance Monitor (APM) operations allow the user to monitor performance of applications over a network. Monitoring the performance of network-hosted applications gives service providers and IT departments the ability to verify that applications are performing as needed and to implement improvements as necessary.

SA Agent Frame Relay Monitor (FRM) operations allow the user to monitor key performance metrics (round-trip latency, packet loss, and data integrity) over Frame Relay PVCs. Proactively monitoring the performance of Frame Relay networks is essential for service providers who offer Frame Relay services.

SA Agent path echo operations have been enhanced to provide hop-by-hop jitter measurement using ICMP packets for VoIP monitoring. The Cisco SA Agent has also been enhanced to allow monitoring within MPLS Virtual Private Networks (VPNs).

Secure Copy

Platforms: Cisco 7200 series routers

The Secure Copy (SCP) feature provides a secure and authenticated method for copying router configuration or router image files. SCP relies on Secure Shell (SSH), an application and a protocol that provides a secure replacement for the Berkeley r-tools.

The behavior of SCP is similar to that of remote copy (rcp), which comes from the Berkeley r-tools suite, except that it is reliant upon SSH for security. In addition, SCP requires that AAA authorization be configured so the router can determine whether the user has the correct privilege level.

SCP allows a user who is logged into Cisco IOS software to copy anything that exists in the Cisco IOS File System (IFS) to and from a router by using the **copy** command. Whereas someone using a remote workstation cannot perform this task.

Shell-Based Authentication of VPDN Users

Platforms: Cisco 7200 series routers

The Shell-Based Authentication of VPDN Users feature provides terminal services for VPDN users to support rollout of wholesale dial networks. Terminal services (shell login or exec login) on the network access server (NAS) provide the following capabilities:

- Enabling a dial-in user session to be terminated at the access server.
- Authenticating the user with a character-mode login dialog such as username/password or username/challenge/password, Secure ID, Safeword, and so on.
- Initiating PPP and tunneling it to a home gateway (HGW).

With the terminal services, user authentication methods other than PAP and CHAP can be applied to PPP users. With the Shell-Based Authentication of VPDN Users feature, PPP authentication data is preconfigured or entered before PPP starts. Authentication is completed without any further input from the user.

Terminal services provided by Exec-VPDN add an enhancement to an existing AAA configuration command that enables a user to be authenticated at a remote network determined by the DNIS number. This enhancement supports **login** in addition to **ppp**:

aaa dnis map *dnis-number* **authentication** { **ppp** | **login** } **group** *name*

If a proxy AAA server is used by the NAS to authenticate an exec login, this command is not needed. Shell-based authentication then uses the DNIS or domain name to decide which AAA server should authenticate the user.

The new feature supports L2F and L2TP without PPP user authentication.

SNMP Support for VPN

Platforms: Cisco 7100 series and Cisco 7200 series routers

The Support Simple Network Management Protocol (SNMP) over Virtual Private Network (VPN) feature allows the sending and receiving of SNMP notifications using VPN routing/forwarding (VRFs) table.

SNMP is an application-layer protocol that provides a message format for communication between SNMP managers and agents.

A VPN is a network that provides high-connectivity transfers on a shared system with the same usage guidelines as a private network. A VPN can be built on the Internet over IP, Frame Relay, or ATM networks.

A VRF stores per-VPN routing data. It defines the VPN membership of a customer site attached to the network access server (NAS). A VRF consists of an IP routing table, a derived Cisco Express Forwarding (CEF) table, and guidelines and routing protocol parameters that control the information that is included in the routing table.

The Support SNMP over VPN feature provides configuration commands that allow users to associate SNMP agents and managers with specific VRFs. The specified VRF is used for the sending of SNMP notifications (traps and informs) and responses between agents and managers. If a VRF is not specified, the default routing table for the VPN is used.

SNMP Trap Support for VSI Master MIB

Platforms: Cisco 7200 series and Cisco 7500 series routers

The virtual switch interface (VSI) Master MIB monitors and manages ATM switches that are connected to routers through the virtual switch interface. The VSI master is a software module that resides on a router. The VSI master enables an application to control an ATM switch that is connected to the router. The VSI protocol runs between the VSI master and a VSI slave. The VSI master can communicate with more than one slave across a control interface that connects the router to the switch. Each master/slave connection is called a VSI session.

The VSI Master MIB allows you to manage and monitor the activities of the VSI components, including controllers, sessions, logical interfaces, and cross-connects. The MIB provides notifications in the form of traps when any of the VSI components change operational state, violate configured thresholds, or are added or removed. The MIB allows you to specify which VSI components can send traps. To enable the traps for certain VSI components, you can use the MIB objects or Cisco IOS commands.

SS7 Gateway Support

Platforms: Cisco7200 series and Cisco 7500 series routers

Using the SS7 Gateway Support feature, you can connect Cisco VoIP or H.323 voice-enabled media gateways to a circuit-switched time-division multiplexing (TDM) network using Signaling System 7 (SS7). The Cisco SC2200 Signalling Controller is used as a protocol translator to control the gateway via the N12+(Q.931) protocol.

The SS7 Gateway Support feature provides the following benefits:

- SDN User Part (ISUP) signaling links to SS7 network with a Cisco SC2200 Signalling Controller
- T1 or E1 links with 24 or 30 bearer channels to a Media Gateway controlled by a Cisco SC2200 Signalling Controller with Cisco Redundant Link Manager (RLM) protocol conversion
- Continuity testing on outgoing calls with tone generation and detection capability

- Continuity testing on incoming calls with loopback and transponder capability
- Caller ID (ANI) presentation support
- Caller ID screening
- Dial-peer destination wildcards
- Dial-peer numbering type support
- Bearer capability mapping

TCL IVR disconnect cause-code Manipulation

Platforms: Cisco 7200 series routers

The **leg disconnect** command disconnects one or more call legs that are not part of any connection. The *cause_code* argument, which has been added in Cisco IOS Release 12.2(2)T, is an integer ISDN cause code for the disconnect. It is of the form di-*xxx* or just *xxx*, where *xxx* is the ISDN cause code. Refer to the following document for further information:
http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/vapp_dev/tclivrv2.htm

Trimble Palisade NTP Synchronization Driver for the Cisco 7200 Series

Platforms: Cisco 7200 series routers

Cisco IOS Release 12.1(1) and Cisco IOS Release 12.1(1)T introduce a driver that supports the use of the Trimble Palisade NTP Synchronization Kit with the Cisco 7200 series routers. The Trimble GPS product can provide a signal that can by used for NTP time-synchronization of a network. The Trimble Palisade NTP Synchronization Kit can be connected to the auxiliary port of a Cisco 7200 router. The refclock (reference clock) driver provided by this feature provides the ability to receive an RTS timestamp signal on the auxiliary port of the router. The addition of a driver for the Trimble Palisade product in no way implies a recommendation or warranty by Cisco for the Trimble product. To enable the driver, use the **ntp refclock trimble pps none** command in line configuration mode for the aux 0 line.

For more information, see
http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t1/dtrimble.htm

Voice over ATM with AAL2 Trunking on Cisco 7200 Series Routers

Platforms: Cisco 7200 series routers

Voice over ATM (VoATM)

This feature enables Cisco 7200 series routers to carry voice traffic (for example, telephone calls and faxes) over ATM networks using AAL2. AAL2 is the most bandwidth-efficient standards-based trunking method for transporting compressed voice, voice-band data, circuit-mode data, and frame-mode data over ATM infrastructures.

Transparent Common Channel Signaling (T-CCS)

The Transparent Common Channel Signaling (T-CCS) feature provides a way to interconnect private branch exchanges (PBXs), key systems (KTs), and central office switches (COs) when the private integrated services network exchange (PINX) does not support Q (point of the ISDN model) Signaling (QSIG), or when the PINX uses a proprietary solution. T-CCS allows the connection of two PBXs with PRI interfaces that use one CCS protocol without the need for interpretation of CCS signaling for call processing. A PBX PRI group is transported transparently through the data network and the feature

preserves proprietary signaling. From the PBX standpoint, this is accomplished through a point-to-point connection. Calls from the PINXs are not routed, but follow a preconfigured route to the destination. Frame forwarding, used with T-CCS, forwards High-Level Data Link Control (HDLC) frames over a preconfigured interface running HDLC, Frame Relay, or ATM encapsulation.

X.25 Annex G Session Status Change Reporting

Platforms: Cisco 7200 series routers

The X.25 Annex G Session Status Change Reporting feature introduces the **logging event frame-relay x25** interface configuration command, which provides console or system log notification of X.25 Annex G session status changes when an X.25 Annex G session carried over Frame Relay changes state. Before this feature was introduced, there was no notification.

This feature detects changes in session status using an X.25 Link Access Procedure, Balanced (LAPB) N2 counter. The LAPB N2 counter is the number of unsuccessful transmit attempts that are made before the link is declared down. After the N2 consecutive polled commands have not been answered, a notification is generated, indicating that the X.25 profile or context associated with the data-link connection identifier (DLCI), that is running across the failed radio link, has gone down. A message is generated to the console or system log when the link goes down. A message is also generated to the console or system log when the link comes back up. The notification response time is contingent on the values assigned to the LAPB N1 counter and the LAPB T1 timer.

MIBs

Current MIBs

To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml.

Deprecated and Replacement MIBs

Old Cisco MIBs will be replaced in a future release. Currently, OLD-CISCO-* MIBs are being converted into more scalable MIBs without affecting existing Cisco IOS products or network management system (NMS) applications. You can update from deprecated MIBs to the replacement MIBs as shown in Table 17.

Table 17 Deprecated and Replacement MIBs

Deprecated MIB	Replacement
OLD-CISCO-APPLETALK-MIB	RFC1243-MIB
OLD-CISCO-CHASSIS-MIB	ENTITY-MIB
OLD-CISCO-CPUK-MIB	To be determined
OLD-CISCO-DECNET-MIB	To be determined
OLD-CISCO-ENV-MIB	CISCO-ENVMON-MIB
OLD-CISCO-FLASH-MIB	CISCO-FLASH-MIB

Table 17 Deprecated and Replacement MIBs (continued)

Deprecated MIB	Replacement
OLD-CISCO-INTERFACES-MIB	IF-MIB CISCO-QUEUE-MIB
OLD-CISCO-IP-MIB	To be determined
OLD-CISCO-MEMORY-MIB	CISCO-MEMORY-POOL-MIB
OLD-CISCO-NOVELL-MIB	NOVELL-IPX-MIB
OLD-CISCO-SYS-MIB	(Compilation of other OLD* MIBs)
OLD-CISCO-SYSTEM-MIB	CISCO-CONFIG-COPY-MIB
OLD-CISCO-TCP-MIB	CISCO-TCP-MIB
OLD-CISCO-TS-MIB	To be determined
OLD-CISCO-VINES-MIB	CISCO-VINES-MIB
OLD-CISCO-XNS-MIB	To be determined

Important Notes

The following sections contain important notes about Cisco IOS Release 12.2 T that can apply to the Cisco 7000 family routers.

Caveats

Caveats describe unexpected behavior in Cisco IOS software releases. Severity 1 caveats are the most serious caveats; severity 2 caveats are less serious. Severity 3 caveats are moderate caveats, and only select severity 3 caveats are included in the caveats document.

For information on caveats in Cisco IOS Release 12.2 T, see *Caveats for Cisco IOS Release 12.2 T.*

All caveats in Cisco IOS Release 12.2 are also in Cisco IOS Release 12.2 T.

For information on caveats in Cisco IOS Release 12.2, see *Caveats for Cisco IOS Release 12.2*, which lists severity 1 and 2 caveats and select severity 3 caveats and is located on Cisco.com and the Documentation CD-ROM.

Because Cisco IOS Release 12.2(2)T is the initial base release, there are no resolved caveats. For a list of the resolved caveats, see the next mainline caveats document.

Related Documentation

The following sections describe the documentation available for the Cisco 7000 family routers. These documents consist of hardware and software installation guides, Cisco IOS configuration guides and command references, system error messages, feature modules, and other documents.

Documentation is available as printed manuals or electronic documents, except for feature modules, which are available online on Cisco.com and the Documentation CD-ROM.

Use these release notes with these documents:

- Release-Specific Documents, page 48
- Platform-Specific Documents, page 49
- Feature Modules, page 49
- Cisco IOS Software Documentation Set, page 50

Release-Specific Documents

The following documents are specific to Cisco IOS Release 12.2 and are located on Cisco.com and the Documentation CD-ROM:

- *Cross-Platform Release Notes for Cisco IOS Release 12.2.*

  On Cisco.com at:

  Technical Documents: **Cisco IOS Software Configuration**: **Cisco IOS Release 12.2**: **Release Notes**: **Cross-Platform Release Notes**

  On the Documentation CD-ROM at:

  Cisco Product Documentation: **Cisco IOS Software Configuration**: **Cisco IOS Release 12.2**: **Release Notes**: **Cross-Platform Release Notes**

- Product bulletins, field notices, and other release-specific documents on Cisco.com at:

  Technical Documents

- *Caveats for Cisco IOS Release 12.2 T*

  On Cisco.com at:

  Technical Documents: **Cisco IOS Software Configuration**: **Cisco IOS Release 12.2**: **Release Notes**: **Caveats**

  On the Documentation CD-ROM at:

  Cisco Product Documentation: **Cisco IOS Software Configuration**: **Cisco IOS Release 12.2**: **Caveats**

Note If you have an account with Cisco.com, you can use Bug Navigator II to find caveats of any severity for any release. To reach Bug Navigator II, log in to Cisco.com and click **Software Center**: **Cisco IOS Software**: **Bug Toolkit**: **Bug Navigator II**. Another option is to go to http://www.cisco.com/support/bugtools/bugtool.shtml.

Platform-Specific Documents

These documents are available for the Cisco 7000 family on Cisco.com and the Documentation CD-ROM:

- *Cisco 7500 Series Installation and Configuration Guide*
- *Cisco 7200 VXR Installation and Configuration Guide*
- *Cisco 7206 Installation and Configuration Guide*
- *Cisco 7204 Installation and Configuration Guide*
- *Cisco 7202 Installation and Configuration Guide*
- *Cisco 7100 Series VPN Router Installation and Configuration Guide*
- *Cisco 7010 Users Guide*

  On Cisco.com at:

  Technical Documents: **Cisco Product Documentation**: **Core/High-End Routers**

  On the Documentation CD-ROM at:

  Cisco Product Documentation: **Core/High-End Routers**

Feature Modules

Feature modules describe new features supported by Cisco IOS Release 12.2 T and are updates to the Cisco IOS documentation set. A feature module consists of a brief overview of the feature, benefits, configuration tasks, and a command reference. As updates, the feature modules are available online only. Feature module information is incorporated in the next printing of the Cisco IOS documentation set.

On Cisco.com at:

Technical Documents: **Cisco IOS Software Configuration**: **Cisco IOS Release 12.2**: **New Feature Documentation**

On the Documentation CD-ROM at:

Cisco Product Documentation: **Cisco IOS Software Configuration**: **Cisco IOS Release 12.2**: **New Feature Documentation**

Feature Navigator

Feature Navigator is a web-based tool that enables you to quickly determine which Cisco IOS software images support a particular set of features and which features are supported in a particular Cisco IOS image.

Feature Navigator is available 24 hours a day, 7 days a week. To access Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, e-mail the Contact Database Administration group at cdbadmin@cisco.com. If you do not have an account on Cisco.com, go to http://www.cisco.com/register and follow the directions to establish an account.

To use Feature Navigator, you must have a JavaScript-enabled web browser such as Netscape 3.0 or later, or Internet Explorer 4.0 or later. Internet Explorer 4.0 always has JavaScript enabled. To enable JavaScript for Netscape 3.x or Netscape 4.x, follow the instructions provided with the web browser. For Java Script support and enabling instructions for other browsers, check with the browser vendor.

Feature Navigator is updated when major Cisco IOS software releases and technology releases occur. You can access Feature Navigator at the following URL:

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

Cisco IOS Software Documentation Set

The Cisco IOS software documentation set consists of the Cisco IOS configuration guides, Cisco IOS command references, and several other supporting documents. The Cisco IOS software documentation set is shipped with your order in electronic form on the Documentation CD-ROM—unless you specifically ordered the printed versions.

Documentation Modules

Each module in the Cisco IOS documentation set consists of one or more configuration guides and one or more corresponding command references. Chapters in a configuration guide describe protocols, configuration tasks, and Cisco IOS software functionality, and contain comprehensive configuration examples. Chapters in a command reference provide complete command syntax information. Use each configuration guide with its corresponding command reference.

On Cisco.com at:

Technical Documents: **Documentation Home Page**: **Cisco IOS Software Configuration**: **Cisco IOS Release 12.2**: **Configuration Guides and Command References**

On the Documentation CD-ROM at:

Cisco Product Documentation: **Cisco IOS Software Configuration**: **Cisco IOS Release 12.2**: **Configuration Guides and Command References**

Cisco IOS Release 12.2 Documentation Set Contents

Table 18 lists the contents of the Cisco IOS Release 12.2 software documentation set, which is available in electronic form and in printed form if ordered.

Note You can find the most current Cisco IOS documentation on Cisco.com and the Documentation CD-ROM. These electronic documents may contain updates and modifications made after the hard-copy documents were printed.

On Cisco.com at:

Technical Documents: **Documentation Home Page**: **Cisco IOS Software Configuration**: **Cisco IOS Release 12.2**

On the Documentation CD-ROM at:

Cisco Product Documentation: **Cisco IOS Software Configuration**: **Cisco IOS Release 12.2**

Table 18 Cisco IOS Release 12.2 Documentation Set

Books	Major Topics
• *Cisco IOS Configuration Fundamentals Configuration Guide* • *Cisco IOS Configuration Fundamentals Command Reference*	Cisco IOS User Interfaces File Management System Management
• *Cisco IOS Bridging and IBM Networking Configuration Guide* • *Cisco IOS Bridging and IBM Networking Command Reference, Volume 1 of 2* • *Cisco IOS Bridging and IBM Networking Command Reference, Volume 2 of 2*	Transparent Bridging SRB Token Ring Inter-Switch Link Token Ring Route Switch Module RSRB DLSW+ Serial Tunnel and Block Serial Tunnel LLC2 and SDLC IBM Network Media Translation SNA Frame Relay Access NCIA Client/Server Airline Product Set DSPU and SNA Service Point SNA Switching Services Cisco Transaction Connection Cisco Mainframe Channel Connection CLAW and TCP/IP Offload CSNA, CMPC, and CMPC+ TN3270 Server
• *Cisco IOS Dial Technologies Configuration Guide: Dial Access* • *Cisco IOS Dial Technologies Configuration Guide: Large-Scale Dial Applications* • *Cisco IOS Dial Technologies Command Reference, Volume 1 of 2* • *Cisco IOS Dial Technologies Command Reference, Volume 2 of 2*	Dial Access Modem and Dial Shelf Configuration and Management ISDN Configuration Signaling Configuration Point-to-Point Protocols Dial-on-Demand Routing Dial Backup Dial Related Addressing Service Network Access Solutions Large-Scale Dial Solutions Cost-Control Solutions Internetworking Dial Access Scenarios
• *Cisco IOS Interface Configuration Guide* • *Cisco IOS Interface Command Reference*	LAN Interfaces Serial Interfaces Logical Interfaces
• *Cisco IOS IP Configuration Guide* • *Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services* • *Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols* • *Cisco IOS IP Command Reference, Volume 3 of 3: Multicast*	IP Addressing IP Services IP Routing Protocols IP Multicast
• *Cisco IOS AppleTalk and Novell IPX Configuration Guide* • *Cisco IOS AppleTalk and Novell IPX Command Reference*	AppleTalk Novell IPX

Table 18 Cisco IOS Release 12.2 Documentation Set (continued)

Books	Major Topics
• *Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS, and XNS Configuration Guide* • *Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS, and XNS Command Reference*	Apollo Domain Banyan VINES DECnet ISO CLNS XNS
• *Cisco IOS Voice, Video, and Fax Configuration Guide* • *Cisco IOS Voice, Video, and Fax Command Reference*	Voice over IP Call Control Signaling Voice over Frame Relay Voice over ATM Telephony Applications Trunk Management Fax, Video, and Modem Support
• *Cisco IOS Quality of Service Solutions Configuration Guide* • *Cisco IOS Quality of Service Solutions Command Reference*	Packet Classification Congestion Management Congestion Avoidance Policing and Shaping Signaling Link Efficiency Mechanisms
• *Cisco IOS Security Configuration Guide* • *Cisco IOS Security Command Reference*	AAA Security Services Security Server Protocols Traffic Filtering and Firewalls IP Security and Encryption Passwords and Privileges Neighbor Router Authentication IP Security Options Supported AV Pairs
• *Cisco IOS Switching Services Configuration Guide* • *Cisco IOS Switching Services Command Reference*	Cisco IOS Switching Paths NetFlow Switching Multiprotocol Label Switching Multilayer Switching Multicast Distributed Switching Virtual LANs LAN Emulation
• *Cisco IOS Wide-Area Networking Configuration Guide* • *Cisco IOS Wide-Area Networking Command Reference*	ATM Frame Relay SMDS X.25 and LAPB
• *Cisco IOS Mobile Wireless Configuration Guide* • *Cisco IOS Mobile Wireless Command Reference*	General Packet Radio Service

Table 18 Cisco IOS Release 12.2 Documentation Set (continued)

Books	Major Topics
• *Cisco IOS Terminal Services Configuration Guide* • *Cisco IOS Terminal Services Command Reference*	ARA LAT NASI Telnet TN3270 XRemote X.28 PAD Protocol Translation
• *Cisco IOS Configuration Guide Master Index* • *Cisco IOS Command Reference Master Index* • *Cisco IOS Debug Command Reference* • *Cisco IOS Software System Error Messages* • New Features in 12.2-Based Limited Lifetime Releases • New Features in Release 12.2 T • Release Notes (Release note and caveat documentation for 12.2-based releases and various platforms)	

Obtaining Documentation

The following sections provide sources for obtaining documentation from Cisco Systems.

World Wide Web

The most current Cisco documentation is available on the World Wide Web at http://www.cisco.com. Translated documentation can be accessed at http://www.cisco.com/public/countries_languages.shtml.

Documentation CD-ROM

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

Ordering Documentation

Cisco documentation is available in the following ways:

- Registered Cisco Direct Customers can order Cisco product documentation from the Networking Products MarketPlace:

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

- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:

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

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, in North America, by calling 800 553-NETS (6387).

Documentation Feedback

If you are reading Cisco products documentation on the World Wide Web, you can submit technical comments electronically. Click **Feedback** in the toolbar and select **Documentation**. After you complete the form, click **Submit** to send it to Cisco.

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

For your convenience, many documents contain a response card behind the front cover for submitting your comments by mail. Otherwise, you can mail your comments to the following address:

Cisco Systems, Inc.
Document Resource Connection
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

The following sections provide sources for obtaining technical assistance from Cisco Systems.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information and resources at anytime, from anywhere in the world. This highly integrated Internet application is a powerful, easy-to-use tool for doing business with Cisco.

Cisco.com provides a broad range of features and services to help customers and partners streamline business processes and improve productivity. Through Cisco.com, you can find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online technical support, download and test software packages, and order Cisco learning materials and merchandise. Valuable online skill assessment, training, and certification programs are also available.

Customers and partners can self-register on Cisco.com to obtain additional personalized information and services. Registered users can order products, check on the status of an order, access technical support, and view benefits specific to their relationships with Cisco.

To access Cisco.com, go to the following website:

http://www.cisco.com

Technical Assistance Center

The Cisco TAC website is available to all customers who need technical assistance with a Cisco product or technology that is under warranty or covered by a maintenance contract.

Contacting TAC by Using the Cisco TAC Website

If you have a priority level 3 (P3) or priority level 4 (P4) problem, contact TAC by going to the TAC website:

http://www.cisco.com/tac

P3 and P4 level problems are defined as follows:

- P3—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- P4—You need information or assistance on Cisco product capabilities, product installation, or basic product configuration.

In each of the above cases, use the Cisco TAC website to quickly find answers to your questions.

To register for Cisco.com, go to the following website:

http://www.cisco.com/register/

Cisco.com registered users who cannot resolve a technical issue by using the TAC online resource can open a case online by using the TAC Case Open tool at the following website:

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

Contacting TAC by Telephone

If you have a priority level 1(P1) or priority level 2 (P2) problem, contact TAC by telephone and immediately open a case. To obtain a directory of toll-free numbers for your country, go to the following website:

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

P1 and P2 level problems are defined as follows:

- P1—Your production network is down, causing a critical impact to business operations if service is not restored quickly. No workaround is available.
- P2—Your production network is severely degraded, affecting significant aspects of your business operations. No workaround is available.