



# Release Notes for Cisco 7000 Family for Cisco IOS Release 12.1 T

---

**December 06, 2000**



**Note**

---

You can find the most current Cisco IOS documentation on Cisco.com. These electronic documents may contain updates and modifications made after the hardcopy documents were printed.

---

These release notes for the Cisco 7000 family describe the enhancements provided in Cisco IOS Release 12.1(5)T1. These release notes are updated as needed.

For a list of the software caveats that apply to Release 12.1 T, see *Caveats for Cisco IOS Release 12.1 T* that accompanies these release notes. The caveats document is updated for every maintenance release and is located on Cisco.com and on the Documentation CD-ROM.

Use these release notes with *Cross-Platform Release Notes for Cisco IOS Release 12.1* on Cisco.com and on the Documentation CD-ROM.



**Note**

---

Cisco IOS Release 12.1(5)T1 contains 7200 series and 7500 series images only.

---



**Note**

---

Cisco IOS Release 12.1(5)T contains a fix for DDTs CSCdr91706. For more information, refer to the “ICaveat CSCdr91706 and IOS HTTP Vulnerability” section on page 90.

---



**Note**

---

Cisco IOS Release 12.1(5)T contains all features and products supported in Cisco IOS Release 12.1(1)E.

---



**Note**

---

Please see the “Important Notes” section on page 89 for information concerning Cisco IOS Release 12.1(3)T and 12.1(3a)T1.

---

# Contents

These release notes describe the following topics:

- System Requirements, page 2
- New and Changed Information, page 48
- MIBs, page 88
- Important Notes, page 89
- Caveats, page 93
- Related Documentation, page 93
- Obtaining Documentation, page 98
- Obtaining Technical Assistance, page 99

## System Requirements

This section describes the system requirements for Release 12.1 T:

- Memory Requirements, page 2
- Hardware Supported, page 7
- Determining the Software Version, page 8
- Upgrading to a New Software Release, page 8
- Microcode Software, page 8
- Feature Set Tables, page 9

## Memory Requirements

*Table 1 Images and Memory Requirements for Cisco IOS Release 12.1(5)T1*

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-is56i-mz	16 MB Flash	128 MB DRAM	RAM
		IP IPSec 3DES	c7200-ik2s-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-io3s56i-mz	16 MB Flash	128 MB DRAM	RAM
		IP/FW/IDS IPSec 3DES	c7200-ik2o3s-mz	16 MB Flash	128 MB DRAM	RAM

Table 1 Images and Memory Requirements for Cisco IOS Release 12.1(5)T1 (continued)

Platforms	Feature Sets	Image Name	Software Image	Flash Memory Recommended	DRAM Memory Recommended	Runs From
	Enterprise Standard Feature Set	Enterprise	c7200-js-mz	16 MB Flash	128 MB DRAM	RAM
		Enterprise IPsec 56	c7200-js56i-mz	16 MB Flash	128 MB DRAM	RAM
		Enterprise IPsec 3DES	c7200-jk2s-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-g5js56i-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-jo3s56i-mz	16 MB Flash	128 MB DRAM	RAM
		Enterprise/FW/IDS IPsec 3DES	c7200-jk2o3s-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-a3js56i-mz	16 MB Flash	128 MB DRAM	RAM
		Enterprise/SNASW IPsec 3DES	c7200-a3jk2s-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-ds56i-mz	16 MB Flash	128 MB DRAM	RAM
	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-do3s56i-mz	16 MB Flash	128 MB DRAM	RAM
		Desktop/IBM/FW/IDS IPsec 3DES	c7200-dk2o3s-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-isv56i-mz	20 MB Flash	128 MB DRAM	RAM
		IP IPsec 3DES	rsp-ik2sv-mz	20 MB Flash	128 MB DRAM	RAM

Table 1 Images and Memory Requirements for Cisco IOS Release 12.1(5)T1 (continued)

Platforms	Feature Sets	Image Name	Software Image	Flash Memory Recommended	DRAM Memory Recommended	Runs From
	IP Firewall Standard Feature Set	IP/FW/IDS	rsp-io3sv-mz	20 MB Flash	128 MB DRAM	RAM
		IP/FW/IDS IPSec 56	rsp-io3sv56i-mz	20 MB Flash	128 MB DRAM	RAM
		IP/FW/IDS IPSec 3DES	rsp-ik2o3sv-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-jsv56i-mz	20 MB Flash	128 MB DRAM	RAM
		Enterprise IPSec 3DES	rsp-jk2sv-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-jo3sv56i-mz	20 MB Flash	128 MB DRAM	RAM
		Enterprise/FW/IDS IPSec 3DES	rsp-jk2o3sv-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-a3jsv56i-mz	20 MB Flash	128 MB DRAM	RAM
		Enterprise/SNASW IPSec 3DES	rsp-a3jk2sv-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-dsv56i-mz	20 MB Flash	128 MB DRAM	RAM
	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-do3sv56i-mz	20 MB Flash	128 MB DRAM	RAM
		Desktop/IBM/FW/IDS/ IPSec 3DES	rsp-dk2o3sv-mz	20 MB Flash	128 MB DRAM	RAM

Table 2 Images and Memory Requirements for Cisco IOS Release 12.1(5)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-is56i-mz	16 MB Flash	64 MB DRAM	RAM
		IP IPSec 3DES	c7100-ik2s-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-io3s56i-mz	16 MB Flash	64 MB DRAM	RAM
		IP/FW/IDS IPSec 3DES	c7100-ik2o3s-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-js56i-mz	16 MB Flash	64 MB DRAM	RAM
		Enterprise IPSec 3DES	c7100-jk2s-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-jo3s56i-mz	16 MB Flash	64 MB DRAM	RAM
		Enterprise/FW/IDS IPSec 3DES	c7100-jk2o3s-mz	16 MB Flash	64 MB DRAM	RAM
Cisco 7200 Series	IP Standard Feature Set	IP	c7200-is-mz	16 MB Flash	128 MB DRAM	RAM
		IP IPSec 56	c7200-is56i-mz	16 MB Flash	128 MB DRAM	RAM
		IP IPSec 3DES	c7200-ik2s-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-io3s56i-mz	16 MB Flash	128 MB DRAM	RAM
		IP/FW/IDS IPSec 3DES	c7200-ik2o3s-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-js56i-mz	16 MB Flash	128 MB DRAM	RAM
		Enterprise IPSec 3DES	c7200-jk2s-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-g5js56i-mz	16 MB Flash	128 MB DRAM	RAM

Table 2 Images and Memory Requirements for Cisco IOS Release 12.1(5)T (continued)

Platforms	Feature Sets	Image Name	Software Image	Flash Memory Recommended	DRAM Memory Recommended	Runs From	
	Enterprise Firewall Standard Feature Set	Enterprise/FW/IDS	c7200-jo3s-mz	16 MB Flash	128 MB DRAM	RAM	
		Enterprise/FW/IDS IPSec 56	c7200-jo3s56i-mz	16 MB Flash	128 MB DRAM	RAM	
		Enterprise/FW/IDS IPSec 3DES	c7200-jk2o3s-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-a3js56i-mz	16 MB Flash	128 MB DRAM	RAM	
		Enterprise/SNASW IPSec 3DES	c7200-a3jk2s-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-ds56i-mz	16 MB Flash	128 MB DRAM	RAM	
	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-do3s56i-mz	16 MB Flash	128 MB DRAM	RAM	
		Desktop/IBM/FW/IDS IPSec 3DES	c7200-dk2o3s-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-isv56i-mz	20 MB Flash	128 MB DRAM	RAM
			IP IPSec 3DES	rsp-ik2sv-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-io3sv56i-mz	20 MB Flash	128 MB DRAM	RAM	
IP/FW/IDS IPSec 3DES			rsp-ik2o3sv-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-jsv56i-mz	20 MB Flash	128 MB DRAM	RAM	
		Enterprise IPSec 3DES	rsp-jk2sv-mz	20 MB Flash	128 MB DRAM	RAM	

Table 2 Images and Memory Requirements for Cisco IOS Release 12.1(5)T (continued)

Platforms	Feature Sets	Image Name	Software Image	Flash Memory Recommended	DRAM Memory Recommended	Runs From
	Enterprise Firewall Standard Feature Set	Enterprise/FW/IDS	rsp-jo3sv-mz	20 MB Flash	128 MB DRAM	RAM
		Enterprise/FW/IDS IPSec 56	rsp-jo3sv56i-mz	20 MB Flash	128 MB DRAM	RAM
		Enterprise/FW/IDS IPSec 3DES	rsp-jk2o3sv-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-a3jsv56i-mz	20 MB Flash	128 MB DRAM	RAM
		Enterprise/SNASW IPSec 3DES	rsp-a3jk2sv-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-dsv56i-mz	20 MB Flash	128 MB DRAM	RAM
	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-do3sv56i-mz	20 MB Flash	128 MB DRAM	RAM
		Desktop/IBM/FW/IDS/ IPSec 3DES	rsp-dk2o3sv-mz	20 MB Flash	128 MB DRAM	RAM

## Hardware Supported



**Note** Cisco IOS Release 12.1(5)T1 supports Cisco 7200 series and Cisco 7500 series routers.

Cisco IOS Release 12.1(5)T supports the Cisco 7000 family:

- 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)
- Cisco 7000 series routers (Cisco 7000 and Cisco 7010) upgraded with the 7000 Series Route Switch Processor (RSP7000) and 7000 Series Chassis Interface (RSP7000CI)



**Note** Cisco IOS Release 12.1(5)T does not support the VIP2-10, VIP2-15, VIP2-20, or VIP2-40.

For detailed descriptions of the new hardware features, see “New and Changed Information” section on page 48.

**Note**

A Hardware-Software Compatibility Matrix is available on Cisco.com for users with Cisco.com login accounts. Using this matrix, you can search for supported hardware components by entering a Cisco platform and IOS Release. The Hardware-Software Compatibility Matrix tool is also available at the following URL:

<http://www.cisco.com/cgi-bin/front.x/Support/HWSWmatrix/hwswmatrix.cgi>

## 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) 12.1 T Software (C7200-JS-MZ), Version 12.1(5) T, RELEASE SOFTWARE
```

## Upgrading to a New Software Release

For general information about upgrading to a new software release, see *Software Advisor* located at: <http://tools.cisco.com/Support/Fusion/FusionHome.do>

## Microcode 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 3 lists the current microcode versions for the Cisco 7000 family.

*Table 3 Current Microcode Versions for the Cisco 7000 Family*

Processor or Module	Current Bundled 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.

Release 12.1 T supports the same feature sets as Release 12.1, but Release 12.1 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 (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 due to United States government regulations. When applicable, purchaser/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](mailto:export@cisco.com).

Table 4 through Table 17 list the features and feature sets supported by the Cisco 7000 family in Cisco IOS Release 12.1 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 12.1(5)T.



### 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](http://Cisco.com). These electronic documents may contain updates and modifications made after the hardcopy documents were printed.

**Table 4** Feature List by Feature Set for the Cisco 7100 Series

Features	In	Software Images by Feature Sets			
		IP	IPSec 56	IPSec 3DES	IP/FW/IDS
<b>Bridging and IBM Networking</b>					
Bridging Between IEEE 802.1Q vLANs	(3)	No	No	No	No
SDLC SNRM Timer and Window Size Enhancements	(5)	Yes	Yes	Yes	Yes
<b>Configuration Fundamentals</b>					
AutoInstall Using DHCP for LAN Interfaces	(5)	Yes	Yes	Yes	Yes
Expression MIB Support of Delta, Wildcarding and Aggregation	(3)	Yes	No	No	Yes
Interface Index Persistence	(5)	Yes	No	No	Yes
NTP MIB	(5)	Yes	Yes	Yes	Yes
Parser Cache	(5)	Yes	Yes	Yes	Yes
<b>IP Addressing and Services</b>					
NAT—Enhanced H.225/H.245 Forwarding Engine	(5)	No	No	No	Yes

Table 4 Feature List by Feature Set for the Cisco 7100 Series (continued)

Features	In	Software Images by Feature Sets			
		IP	IPSec 56	IPSec 3DES	IP/FW/IDS
NAT—Support for NetMeeting Directory (Internet Locator Service—ILS)	(5)	Yes	Yes	Yes	Yes
NAT—Support of H.323 v2 Call Signalling (FastConnect)	(5)	No	No	No	Yes
<b>IP Multicast</b>					
IGMP, Version 3	(5)	Yes	Yes	Yes	Yes
Router-Port Group Management Protocol	(5)	Yes	Yes	Yes	Yes
<b>IP Routing</b>					
HSRP Support for ICMP Redirects	(3)	Yes	Yes	Yes	Yes
OSPF Flooding Reduction	(2)	Yes	Yes	Yes	Yes
<b>Miscellaneous</b>					
VPN Accelerator Card Enhancements	(5)	No	Yes	No	No
<b>Quality of Service</b>					
Set ATM CLP Bit	(5)	Yes	Yes	Yes	Yes
Class-Based Shaping	(3)	Yes	No	No	Yes
Class-Based QoS MIB	(5)	Yes	Yes	Yes	Yes
IP DSCP Marking for Frame-Relay PVC	(5)	Yes	Yes	Yes	Yes
Network-Based Application Recognition	(5)	Yes	Yes	Yes	Yes
Quality of Service Device Manager Command-Line Interface Commands	(5)	Yes	Yes	Yes	Yes
Quality of Service for Virtual Private Networks	(5)	Yes	Yes	Yes	Yes
<b>Security</b>					
IKE Extended Authentication	(1)	No	Yes	Yes	No
Wildcard Pre-Shared Key Enhancement	(1)	No	Yes	Yes	No
<b>Switching</b>					
Virtual Profile CEF Switched	(2)	Yes	Yes	Yes	Yes
<b>WAN</b>					
CUG Selection Facility Suppress Option	(5)	Yes	Yes	Yes	Yes

Table 5 Feature List by Feature Set for the Cisco 7100 Series, Part 2

Features	In	Software Images by Feature Sets			
		IP/FW IPSec 56	IP/FW/IDS IPSec 3DES	Enterprise	Enterprise IPSec 56
<b>Bridging and IBM Networking</b>					
Bridging Between IEEE 802.1Q vLANs	(3)	No	No	Yes	Yes
SDLC SNRM Timer and Window Size Enhancements	(5)	Yes	Yes	Yes	Yes

Table 5 Feature List by Feature Set for the Cisco 7100 Series, Part 2 (continued)

Features	In	Software Images by Feature Sets			
		IP/FW IPSec 56	IP/FW/IDS IPSec 3DES	Enterprise	Enterprise IPSec 56
<b>Configuration Fundamentals</b>					
AutoInstall Using DHCP for LAN Interfaces	(5)	Yes	Yes	Yes	Yes
Expression MIB Support of Delta, Wildcarding and Aggregation	(3)	No	No	Yes	No
Interface Index Persistence	(5)	No	No	Yes	No
NTP MIB	(5)	Yes	Yes	Yes	Yes
Parser Cache	(5)	Yes	Yes	Yes	Yes
<b>IP Addressing and Services</b>					
NAT—Enhanced H.225/H.245 Forwarding Engine	(5)	Yes	Yes	Yes	Yes
NAT—Support for NetMeeting Directory (Internet Locator Service—ILS)	(5)	Yes	Yes	Yes	Yes
NAT—Support of H.323 v2 Call Signalling (FastConnect)	(5)	Yes	Yes	Yes	Yes
<b>IP Multicast</b>					
IGMP, Version 3	(5)	Yes	Yes	Yes	Yes
Router-Port Group Management Protocol	(5)	Yes	Yes	Yes	Yes
<b>IP Routing</b>					
HSRP Support for ICMP Redirects	(3)	Yes	Yes	Yes	Yes
OSPF Flooding Reduction	(2)	Yes	Yes	Yes	Yes
<b>Miscellaneous</b>					
VPN Accelerator Card Enhancements	(5)	Yes	No	No	Yes
<b>Quality of Service</b>					
Set ATM CLP Bit	(5)	Yes	Yes	Yes	Yes
Class-Based Shaping	(3)	No	No	Yes	No
Class-Based QoS MIB	(5)	Yes	Yes	Yes	Yes
IP DSCP Marking for Frame-Relay PVC	(5)	Yes	Yes	Yes	Yes
Network-Based Application Recognition	(5)	Yes	Yes	Yes	Yes
Quality of Service Device Manager Command-Line Interface Commands	(5)	Yes	Yes	Yes	Yes
Quality of Service for Virtual Private Networks	(5)	Yes	Yes	Yes	Yes
<b>Security</b>					
IKE Extended Authentication	(1)	Yes	Yes	No	Yes
Wildcard Pre-Shared Key Enhancement	(1)	Yes	Yes	No	Yes
<b>Switching</b>					
Virtual Profile CEF Switched	(2)	Yes	Yes	Yes	Yes

Table 5 Feature List by Feature Set for the Cisco 7100 Series, Part 2 (continued)

Features	In	Software Images by Feature Sets			
		IP/FW IPSec 56	IP/FW/IDS IPSec 3DES	Enterprise	Enterprise IPSec 56
<b>WAN</b>					
CUG Selection Facility Suppress Option	(5)	Yes	Yes	Yes	Yes

Table 6 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
<b>Bridging and IBM Networking</b>					
Bridging Between IEEE 802.1Q vLANs	(3)	Yes	Yes	Yes	Yes
SDLC SNRM Timer and Window Size Enhancements	(5)	Yes	Yes	Yes	Yes
<b>Configuration Fundamentals</b>					
AutoInstall Using DHCP for LAN Interfaces	(5)	Yes	Yes	Yes	Yes
Expression MIB Support of Delta, Wildcarding and Aggregation	(3)	No	Yes	No	No
Interface Index Persistence	(5)	No	Yes	No	No
NTP MIB	(5)	Yes	Yes	Yes	Yes
Parser Cache	(5)	Yes	Yes	Yes	Yes
<b>IP Addressing and Services</b>					
NAT—Enhanced H.225/H.245 Forwarding Engine	(5)	Yes	Yes	Yes	Yes
NAT—Support for NetMeeting Directory (Internet Locator Service—ILS)	(5)	Yes	Yes	Yes	Yes
NAT—Support of H.323 v2 Call Signalling (FastConnect)	(5)	Yes	Yes	Yes	Yes
<b>IP Multicast</b>					
IGMP, Version 3	(5)	Yes	Yes	Yes	Yes
Router-Port Group Management Protocol	(5)	Yes	Yes	Yes	Yes
<b>IP Routing</b>					
HSRP Support for ICMP Redirects	(3)	Yes	Yes	Yes	Yes
OSPF Flooding Reduction	(2)	Yes	Yes	Yes	Yes
<b>Miscellaneous</b>					
VPN Accelerator Card Enhancements	(5)	Yes	No	Yes	Yes
<b>Quality of Service</b>					
Set ATM CLP Bit	(5)	Yes	Yes	Yes	Yes
Class-Based Shaping	(3)	No	Yes	No	No
Class-Based QoS MIB	(5)	Yes	Yes	Yes	Yes

Table 6 Feature List by Feature Set for the Cisco 7100 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
IP DSCP Marking for Frame-Relay PVC	(5)	Yes	Yes	Yes	Yes
Network-Based Application Recognition	(5)	Yes	Yes	Yes	Yes
Quality of Service Device Manager Command-Line Interface Commands	(5)	Yes	Yes	Yes	Yes
Quality of Service for Virtual Private Networks	(5)	Yes	Yes	Yes	Yes
<b>Security</b>					
IKE Extended Authentication	(1)	Yes	No	Yes	Yes
Wildcard Pre-Shared Key Enhancement	(1)	Yes	No	Yes	Yes
<b>Switching</b>					
Virtual Profile CEF Switched	(2)	Yes	Yes	Yes	Yes
<b>WAN</b>					
CUG Selection Facility Suppress Option	(5)	Yes	Yes	Yes	Yes

Table 7 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
<b>Bridging and IBM Networking</b>					
Bridging Between IEEE 802.1Q vLANs	(3)	No	No	No	No
SDLC SNRM Timer and Window Size Enhancements	(5)	Yes	Yes	Yes	Yes
SNMP Support for IOS vLAN Subinterfaces	(3)	Yes	Yes	Yes	Yes
TN3270 Server Connectivity Enhancements	(5)	Yes	Yes	Yes	Yes
<b>Configuration Fundamentals</b>					
AutoInstall Using DHCP for LAN Interfaces	(5)	Yes	Yes	Yes	Yes
Configuration through SNMP	(3)	Yes	No	No	Yes
Event MIB	(3)	Yes	Yes	Yes	Yes
Expression MIB Support of Delta, Wildcarding, and Aggregation	(3)	Yes	No	No	Yes
Individual SNMP Trap Support	(3)	Yes	Yes	Yes	Yes
Interface Index Persistence	(5)	Yes	Yes	Yes	Yes
Interface Range Specification	(5)	Yes	Yes	Yes	Yes
NTP MIB	(5)	Yes	Yes	Yes	Yes
Parser Cache	(5)	Yes	Yes	Yes	Yes
WCCP Redirection on Inbound Interfaces	(3)	Yes	No	No	Yes

Table 7 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
<b>Connectivity/Scalability</b>					
PPPoE on ATM	(1)	Yes	Yes	Yes	Yes
PPP Over Fast Ethernet 802.1Q	(5)	Yes	Yes	Yes	Yes
<b>Interfaces</b>					
FastEther Channel Enhancements on Cisco 7200 Series Routers	(5)	Yes	Yes	Yes	Yes
<b>IP Addressing and Services</b>					
HSRP support for MPLS VPNs	(3)	Yes	Yes	Yes	Yes
NAT—Enhanced H.225/H.245 Forwarding Engine	(5)	No	No	No	Yes
NAT—Support for NetMeeting Directory (Internet Locator Service—ILS)	(5)	Yes	Yes	Yes	Yes
NAT—Support of H.323 v2 Call Signalling (FastConnect)	(5)	No	No	No	Yes
NAT—Support of IP Phone to Cisco Call Manager	(5)	Yes	Yes	Yes	Yes
Turbo Access Control Lists	(5)	Yes	Yes	Yes	Yes
<b>IP Multicast</b>					
Bidirectional PIM	(2)	Yes	Yes	Yes	Yes
IGMP, Version 3	(5)	Yes	Yes	Yes	Yes
PIM Dense Mode State Refresh	(5)	Yes	Yes	Yes	Yes
Router-Port Group Management Protocol	(5)	Yes	Yes	Yes	Yes
Source Specific Multicast	(3)	Yes	Yes	Yes	Yes
<b>IP Routing</b>					
HSRP Support for ICMP Redirects	(3)	Yes	Yes	Yes	Yes
Minimum Masking Ability for NetFlow Router-Based Aggregation Schemes	(2)	Yes	Yes	Yes	Yes
OSPF Flooding Reduction	(2)	Yes	Yes	Yes	Yes
<b>Management</b>					
Service Assurance Agent Enhancement	(1)	Yes	Yes	Yes	Yes
<b>Miscellaneous</b>					
H.323 Version 2 Support	(1)	Yes	Yes	Yes	Yes
Inter-Autonomous Systems MPLS VPN Support	(5)	No	No	No	No
MPLS Traffic Engineering and Enhancements	(3)	No	No	No	No
Virtual Switch Interface Master MIB	(3)	No	No	No	No
VPN Accelerator Card Enhancements	(5)	No	Yes	No	No
<b>Mobile Wireless</b>					
General Packet Radio Service Release 1.4	(3)	No	No	No	No

Table 7 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
<b>Multiservice Applications—DSL</b>					
CEF Switching for Routed Bridge Encapsulation	(5)	Yes	Yes	Yes	Yes
PPPoE Radius Port Identification	(5)	Yes	Yes	Yes	Yes
<b>Multiservice Applications—Voice</b>					
Interworking Signaling Enhancements for H.323 and SIP VoIP	(5)	Yes	Yes	Yes	Yes
T.38 Fax Relay for Voice over IP H.323	(3)	Yes	Yes	Yes	Yes
<b>Quality of Service</b>					
Class-Based Marking	(3)	Yes	Yes	Yes	Yes
Class-Based Ethernet CoS Matching and Marking	(5)	Yes	Yes	Yes	Yes
Class-Based QoS MIB	(5)	Yes	Yes	Yes	Yes
Class-Based Policer for the DiffServ AF PHB	(5)	Yes	Yes	Yes	Yes
Class-Based Shaping	(3)	Yes	No	No	Yes
Configurable Per ATM-VC Hold Queue Size	(5)	Yes	Yes	Yes	Yes
COPS for RSVP	(1)	Yes	Yes	Yes	Yes
DiffServ Compliant WRED	(5)	Yes	Yes	Yes	Yes
IP DSCP marking for Frame-Relay PVC	(5)	Yes	Yes	Yes	Yes
Network-Based Application Recognition	(5)	Yes	Yes	Yes	Yes
Quality of Service Device Manager Command-Line Interface Commands	(5)	Yes	Yes	Yes	Yes
Quality of Service for Virtual Private Networks	(5)	Yes	Yes	Yes	Yes
RSVP Support for Frame Relay	(5)	Yes	Yes	Yes	Yes
RSVP Support for Low Latency Queuing	(3)	Yes	Yes	Yes	Yes
Set ATM CLP Bit	(5)	Yes	Yes	Yes	Yes
<b>Reliability</b>					
PGM Host	(1)	No	No	No	No
<b>Security</b>					
AAA Broadcast Accounting	(1)	Yes	Yes	Yes	Yes
AAA Server Group Deadtimer	(2)	Yes	Yes	Yes	Yes
Ecosystem Gatekeeper Interoperability Enhancements	(1)	Yes	Yes	No	No
Gateway-to-Gatekeeper Billing Redundancy	(1)	Yes	No	No	Yes
IKE Extended Authentication	(1)	No	Yes	Yes	No
Secure Shell, Version 1 Integrated Client	(3)	No	Yes	Yes	No
SSH, Version 1 Support for T Train	(1)	Yes	Yes	Yes	No
Wildcard Pre-Shared Key Enhancement	(1)	No	Yes	Yes	No

Table 7 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
<b>Switching</b>					
CEF Support for IP Routing between IEEE 802.1Q vLANs	(3)	Yes	Yes	Yes	Yes
MPLS Class of Service Enhancements	(5)	No	No	No	No
MPLS Scalability Enhancements for LSC and ATM LSR	(5)	No	No	No	No
Traceroute Enhancement for MPLS	(5)	No	No	No	No
Virtual Profile CEF Switched	(2)	Yes	Yes	Yes	Yes
<b>Voice, Data, and Phone Connectivity</b>					
Answer Supervision Reporting	(1)	Yes	No	No	No
Cisco H.323, Version 2, Phase 2	(1)	Yes	Yes	Yes	Yes
Configurable Timers in H.225	(2)	Yes	Yes	Yes	Yes
Ecosystem Gatekeeper Interoperability Enhancements, Phase 2	(2)	Yes	Yes	Yes	Yes
Gatekeeper-to-Gatekeeper Redundancy and Load-Sharing	(2)	Yes	Yes	Yes	Yes
H.323 Support for Virtual Interfaces	(2)	Yes	Yes	Yes	Yes
ISDN Network Side for PRI for ETSI Net5 PRI	(1)	Yes	Yes	Yes	Yes
PRI and BRI QSIG Protocol Support on the Cisco 2600, 3600 and MC3810 Series Routers and PRI QSIG on the Cisco 7200	(2)	Yes	Yes	Yes	Yes
Transparent Common Channel Signaling	(3)	Yes	Yes	Yes	Yes
Voice Over Frame Relay Configuration Enhancements	(2)	Yes	Yes	Yes	Yes
<b>WAN</b>					
CUG Selection Facility Suppress Option	(5)	Yes	Yes	Yes	Yes
Frame Relay ELMI Address Registration	(3)	Yes	Yes	Yes	Yes
Frame Relay Fragmentation with Hardware Compression	(5)	Yes	Yes	Yes	Yes
Frame Relay PVC Interface Priority Queueing	(2)	Yes	Yes	Yes	Yes
Frame Relay Switching Diagnostics and Troubleshooting	(5)	Yes	Yes	Yes	Yes
Frame Relay Switching Enhancements	(2)	Yes	Yes	Yes	Yes
Low Latency Queueing for Frame Relay	(2)	Yes	Yes	Yes	Yes
PPP over ATM SVC	(3)	Yes	Yes	Yes	Yes



Table 8 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
<b>Bridging and IBM Networking</b>					
Bridging Between IEEE 802.1Q vLANs	(3)	No	No	Yes	Yes
SDLC SNRM Timer and Window Size Enhancements	(5)	Yes	Yes	Yes	Yes
SNMP Support for IOS vLAN Subinterfaces	(3)	Yes	Yes	Yes	Yes
TN3270 Server Connectivity Enhancements	(5)	Yes	Yes	Yes	Yes
<b>Configuration Fundamentals</b>					
AutoInstall Using DHCP for LAN Interfaces	(5)	Yes	Yes	Yes	Yes
Configuration through SNMP	(3)	No	No	Yes	No
Event MIB	(3)	Yes	Yes	Yes	Yes
Expression MIB Support of Delta, Wildcarding, and Aggregation	(3)	No	No	Yes	No
Individual SNMP Trap Support	(3)	Yes	Yes	Yes	Yes
Interface Index Persistence	(5)	Yes	Yes	Yes	Yes
Interface Range Specification	(5)	Yes	Yes	Yes	Yes
NTP MIB	(5)	Yes	Yes	Yes	Yes
Parser Cache	(5)	Yes	Yes	Yes	Yes
WCCP Redirection on Inbound Interfaces	(3)	No	No	Yes	No
<b>Connectivity/Scalability</b>					
PPPoE on ATM	(1)	Yes	Yes	Yes	Yes
PPP Over Fast Ethernet 802.1Q	(5)	Yes	Yes	Yes	Yes
<b>Interfaces</b>					
Fast Ether Channel Enhancements on Cisco 7200 Series Routers	(5)	Yes	Yes	Yes	Yes
<b>IP Addressing and Services</b>					
HSRP support for MPLS VPNs	(3)	Yes	Yes	Yes	Yes
NAT—Enhanced H.225/H.245 Forwarding Engine	(5)	Yes	Yes	Yes	Yes
NAT—Support for NetMeeting Directory (Internet Locator Service—ILS)	(5)	Yes	Yes	Yes	Yes
NAT—Support of H.323 v2 Call Signalling (FastConnect)	(5)	Yes	Yes	Yes	Yes
NAT—Support of IP Phone to Cisco Call Manager	(5)	Yes	Yes	Yes	Yes
Turbo Access Control Lists	(5)	Yes	Yes	Yes	Yes
<b>IP Multicast</b>					
Bidirectional PIM	(2)	Yes	Yes	Yes	Yes
IGMP, Version 3	(5)	Yes	Yes	Yes	Yes

Table 8 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
PIM Dense Mode State Refresh	(5)	Yes	Yes	Yes	Yes
Router-Port Group Management Protocol	(5)	Yes	Yes	Yes	Yes
Source Specific Multicast	(3)	Yes	Yes	Yes	Yes
<b>IP Routing</b>					
HSRP Support for ICMP Redirects	(3)	Yes	Yes	Yes	Yes
Minimum Masking Ability for NetFlow Router-Based Aggregation Schemes	(2)	Yes	Yes	Yes	Yes
OSPF Flooding Reduction	(2)	Yes	Yes	Yes	Yes
<b>Management</b>					
Service Assurance Agent Enhancement	(1)	Yes	Yes	Yes	Yes
<b>Miscellaneous</b>					
H.323 Version 2 Support	(1)	Yes	Yes	Yes	Yes
Inter-Autonomous Systems MPLS VPN Support	(5)	No	No	Yes	Yes
MPLS Traffic Engineering and Enhancements	(3)	No	No	Yes	Yes
Virtual Switch Interface Master MIB	(3)	No	No	Yes	Yes
VPN Accelerator Card Enhancements	(5)	Yes	No	No	Yes
<b>Mobile Wireless</b>					
General Packet Radio Service Release 1.4	(3)	No	No	No	No
<b>Multiservice Applications—DSL</b>					
CEF Switching for Routed Bridge Encapsulation	(5)	Yes	Yes	Yes	Yes
PPPoE Radius Port Identification	(5)	Yes	Yes	Yes	Yes
<b>Multiservice Applications—Voice</b>					
Interworking Signaling Enhancements for H.323 and SIP VoIP	(5)	Yes	Yes	Yes	Yes
T.38 Fax Relay for Voice over IP H.323	(3)	Yes	Yes	Yes	Yes
<b>Quality of Service</b>					
Class-Based Marking	(3)	Yes	Yes	Yes	Yes
Class-Based Ethernet CoS Matching and Marking	(5)	Yes	Yes	Yes	Yes
Class-Based Policer for the DiffServ AF PHB	(5)	Yes	Yes	Yes	Yes
Class-Based QoS MIB	(5)	Yes	Yes	Yes	Yes
Class-Based Shaping	(3)	No	No	Yes	No
Configurable Per ATM-VC Hold Queue Size	(5)	Yes	Yes	Yes	Yes
COPS for RSVP	(1)	Yes	Yes	Yes	Yes
DiffServ Compliant WRED	(5)	Yes	Yes	Yes	Yes
IP DSCP marking for Frame-Relay PVC	(5)	Yes	Yes	Yes	Yes

Table 8 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
Network-Based Application Recognition	(5)	Yes	Yes	Yes	Yes
Quality of Service Device Manager Command-Line Interface Commands	(5)	Yes	Yes	Yes	Yes
Quality of Service for Virtual Private Networks	(5)	Yes	Yes	Yes	Yes
RSVP Support for Frame Relay	(5)	Yes	Yes	Yes	Yes
RSVP Support for Low Latency Queuing	(3)	Yes	Yes	Yes	Yes
Set ATM CLP Bit	(5)	Yes	Yes	Yes	Yes
<b>Reliability</b>					
PGM Host	(1)	No	No	Yes	Yes
<b>Security</b>					
AAA Broadcast Accounting	(1)	Yes	Yes	Yes	Yes
AAA Server Group Deadtimer	(2)	Yes	Yes	Yes	Yes
Ecosystem Gatekeeper Interoperability Enhancements	(1)	No	No	Yes	Yes
Gateway-to-Gatekeeper Billing Redundancy	(1)	No	No	Yes	No
IKE Extended Authentication	(1)	Yes	Yes	No	Yes
Secure Shell, Version 1 Integrated Client	(3)	Yes	Yes	No	Yes
SSH, Version 1 Support for T Train	(1)	Yes	Yes	Yes	Yes
Wildcard Pre-Shared Key Enhancement	(1)	Yes	Yes	No	Yes
<b>Switching</b>					
CEF Support for IP Routing between IEEE 802.1Q vLANs	(3)	Yes	Yes	Yes	Yes
MPLS Class of Service Enhancements	(5)	No	No	Yes	Yes
MPLS Scalability Enhancements for LSC and ATM LSR	(5)	No	No	Yes	Yes
Traceroute Enhancement for MPLS	(5)	No	No	Yes	Yes
Virtual Profile CEF Switched	(2)	Yes	Yes	Yes	Yes
<b>Voice, Data, and Phone Connectivity</b>					
Answer Supervision Reporting	(1)	No	No	Yes	No
Cisco H.323, Version 2, Phase 2	(1)	Yes	Yes	Yes	Yes
Configurable Timers in H.225	(2)	Yes	Yes	Yes	Yes
Ecosystem Gatekeeper Interoperability Enhancements, Phase 2	(2)	Yes	Yes	Yes	Yes
Gatekeeper-to-Gatekeeper Redundancy and Load-Sharing	(2)	Yes	Yes	Yes	Yes
H.323 Support for Virtual Interfaces	(2)	Yes	Yes	Yes	Yes
ISDN Network Side for PRI for ETSI Net5 PRI	(1)	Yes	Yes	Yes	Yes

**Table 8 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
PRI and BRI QSIG Protocol Support on the Cisco 2600, 3600 and MC3810 Series Routers and PRI QSIG on the Cisco 7200	(2)	Yes	Yes	Yes	Yes
Transparent Common Channel Signaling	(3)	Yes	Yes	Yes	Yes
Voice Over Frame Relay Configuration Enhancements	(2)	Yes	Yes	Yes	Yes
<b>WAN</b>					
CUG Selection Facility Suppress Option	(5)	Yes	Yes	Yes	Yes
Frame Relay ELMI Address Registration	(3)	Yes	Yes	Yes	Yes
Frame Relay Fragmentation with Hardware Compression	(5)	Yes	Yes	Yes	Yes
Frame Relay PVC Interface Priority Queueing	(2)	Yes	Yes	Yes	Yes
Frame Relay Switching Diagnostics and Troubleshooting	(5)	Yes	Yes	Yes	Yes
Frame Relay Switching Enhancements	(2)	Yes	Yes	Yes	Yes
Low Latency Queueing for Frame Relay	(2)	Yes	Yes	Yes	Yes
PPP over ATM SVC	(3)	Yes	Yes	Yes	Yes

**Table 9 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
<b>Bridging and IBM Networking</b>					
Bridging Between IEEE 802.1Q vLANs	(3)	Yes	No	Yes	Yes
SDLC SNRM Timer and Window Size Enhancements	(5)	Yes	Yes	Yes	Yes
SNMP Support for IOS vLAN Subinterfaces	(3)	Yes	Yes	Yes	Yes
TN3270 Server Connectivity Enhancements	(5)	Yes	Yes	Yes	Yes
<b>Configuration Fundamentals</b>					
AutoInstall Using DHCP for LAN Interfaces	(5)	Yes	Yes	Yes	Yes
Configuration through SNMP	(3)	No	Yes	No	No
Event MIB	(3)	Yes	Yes	Yes	Yes
Expression MIB Support of Delta, Wildcarding, and Aggregation	(3)	No	Yes	No	No
Individual SNMP Trap Support	(3)	Yes	Yes	Yes	Yes
Interface Index Persistence	(5)	Yes	Yes	Yes	Yes
Interface Range Specification	(5)	Yes	Yes	Yes	Yes

Table 9 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
NTP MIB	(5)	Yes	Yes	Yes	Yes
Parser Cache	(5)	Yes	Yes	Yes	Yes
WCCP Redirection on Inbound Interfaces	(3)	No	Yes	Yes	No
<b>Connectivity/Scalability</b>					
PPPoE on ATM	(1)	Yes	Yes	Yes	Yes
PPP Over Fast Ethernet 802.1Q	(5)	Yes	Yes	Yes	Yes
<b>Interfaces</b>					
FastEther Channel Enhancements on Cisco 7200 Series Routers	(5)	Yes	Yes	Yes	Yes
<b>IP Addressing and Services</b>					
HSRP support for MPLS VPNs	(3)	Yes	Yes	Yes	Yes
NAT—Enhanced H.225/H.245 Forwarding Engine	(5)	Yes	Yes	Yes	Yes
NAT—Support for NetMeeting Directory (Internet Locator Service—ILS)	(5)	Yes	Yes	Yes	Yes
NAT—Support of H.323 v2 Call Signalling (FastConnect)	(5)	Yes	Yes	Yes	Yes
NAT—Support of IP Phone to Cisco Call Manager	(5)	Yes	Yes	Yes	Yes
Turbo Access Control Lists	(5)	Yes	Yes	Yes	Yes
<b>IP Multicast</b>					
Bidirectional PIM	(2)	Yes	Yes	Yes	Yes
IGMP, Version 3	(5)	Yes	Yes	Yes	Yes
PIM Dense Mode State Refresh	(5)	Yes	Yes	Yes	Yes
Router-Port Group Management Protocol	(5)	Yes	Yes	Yes	Yes
Source Specific Multicast	(3)	Yes	Yes	Yes	Yes
<b>IP Routing</b>					
HSRP Support for ICMP Redirects	(3)	Yes	Yes	Yes	Yes
Minimum Masking Ability for NetFlow Router-Based Aggregation Schemes	(2)	Yes	Yes	Yes	Yes
OSPF Flooding Reduction	(2)	Yes	Yes	Yes	Yes
<b>Management</b>					
Service Assurance Agent Enhancement	(1)	Yes	Yes	Yes	Yes
<b>Miscellaneous</b>					
H.323 Version 2 Support	(1)	Yes	Yes	Yes	Yes
Inter-Autonomous Systems MPLS VPN Support	(5)	Yes	Yes	Yes	Yes
MPLS Traffic Engineering and Enhancements	(3)	Yes	No	Yes	Yes

Table 9 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
Virtual Switch Interface Master MIB	(3)	Yes	No	Yes	Yes
VPN Accelerator Card Enhancements	(5)	Yes	No	No	Yes
<b>Mobile Wireless</b>					
General Packet Radio Service Release 1.4	(3)	No	No	Yes	Yes
<b>Multiservice Applications—DSL</b>					
CEF Switching for Routed Bridge Encapsulation	(5)	Yes	Yes	Yes	Yes
PPPoE Radius Port Identification	(5)	Yes	Yes	Yes	Yes
<b>Multiservice Applications—Voice</b>					
Interworking Signaling Enhancements for H.323 and SIP VoIP	(5)	Yes	No	Yes	Yes
T.38 Fax Relay for Voice over IP H.323	(3)	Yes	Yes	Yes	Yes
<b>Quality of Service</b>					
Class-Based Marking	(3)	Yes	Yes	Yes	Yes
Class-Based Ethernet CoS Matching and Marking	(5)	Yes	Yes	Yes	Yes
Class-Based Policer for the DiffServ AF PHB	(5)	Yes	Yes	Yes	Yes
Class-Based QoS MIB	(5)	Yes	Yes	Yes	Yes
Class-Based Shaping	(3)	No	Yes	Yes	No
Configurable Per ATM-VC Hold Queue Size	(5)	Yes	Yes	Yes	Yes
COPS for RSVP	(1)	Yes	Yes	Yes	Yes
DiffServ Compliant WRED	(5)	Yes	Yes	Yes	Yes
IP DSCP marking for Frame-Relay PVC	(5)	Yes	Yes	Yes	Yes
Network-based Application Recognition	(5)	Yes	Yes	Yes	Yes
Quality of Service Device Manager Command-Line Interface Commands	(5)	Yes	Yes	Yes	Yes
Quality of Service for Virtual Private Networks	(5)	Yes	Yes	Yes	Yes
RSVP Support for Frame Relay	(5)	Yes	Yes	Yes	Yes
RSVP Support for Low Latency Queuing	(3)	Yes	Yes	Yes	Yes
Set ATM CLP Bit	(5)	Yes	Yes	Yes	Yes
<b>Reliability</b>					
PGM Host	(1)	Yes	Yes	Yes	Yes
<b>Security</b>					
AAA Broadcast Accounting	(1)	Yes	Yes	Yes	Yes
AAA Server Group Deadtimer	(2)	Yes	Yes	Yes	Yes
Ecosystem Gatekeeper Interoperability Enhancements	(1)	No	Yes	No	Yes
Gateway-to-Gatekeeper Billing Redundancy	(1)	No	Yes	Yes	No

Table 9 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
IKE Extended Authentication	(1)	Yes	Yes	No	Yes
Secure Shell, Version 1 Integrated Client	(3)	Yes	No	No	Yes
SSH, Version 1 Support for T Train	(1)	Yes	Yes	Yes	Yes
Wildcard Pre-Shared Key Enhancement	(1)	Yes	No	No	Yes
<b>Switching</b>					
CEF Support for IP Routing between IEEE 802.1Q VLANs	(3)	Yes	No	Yes	Yes
MPLS Class of Service Enhancements	(5)	Yes	Yes	Yes	Yes
MPLS Scalability Enhancements for LSC and ATM LSR	(5)	Yes	Yes	Yes	Yes
Traceroute Enhancement for MPLS	(5)	Yes	Yes	Yes	Yes
Virtual Profile CEF Switched	(2)	Yes	Yes	Yes	Yes
<b>Voice, Data, and Phone Connectivity</b>					
Answer Supervision Reporting	(1)	No	Yes	No	No
Cisco H.323, Version 2, Phase 2	(1)	Yes	Yes	Yes	Yes
Configurable Timers in H.225	(2)	Yes	Yes	No	No
Ecosystem Gatekeeper Interoperability Enhancements, Phase 2	(2)	Yes	Yes	Yes	Yes
Gatekeeper-to-Gatekeeper Redundancy and Load-Sharing	(2)	Yes	Yes	No	No
H.323 Support for Virtual Interfaces	(2)	Yes	Yes	Yes	Yes
ISDN Network Side for PRI for ETSI Net5 PRI	(1)	Yes	Yes	Yes	Yes
PRI and BRI QSIG Protocol Support on the Cisco 2600, 3600 and MC3810 Series Routers and PRI QSIG on the Cisco 7200	(2)	Yes	Yes	Yes	Yes
Transparent Common Channel Signaling	(3)	Yes	Yes	Yes	Yes
Voice Over Frame Relay Configuration Enhancements	(2)	Yes	Yes	Yes	Yes
<b>WAN</b>					
CUG Selection Facility Suppress Option	(5)	Yes	Yes	Yes	Yes
Frame Relay ELMI Address Registration	(3)	Yes	Yes	Yes	Yes
Frame Relay Fragmentation with Hardware Compression	(5)	Yes	No	Yes	Yes
Frame Relay PVC Interface Priority Queueing	(2)	Yes	Yes	Yes	Yes
Frame Relay Switching Diagnostics and Troubleshooting	(5)	Yes	Yes	Yes	Yes
Frame Relay Switching Enhancements	(2)	Yes	Yes	Yes	Yes

Table 9 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
Low Latency Queueing for Frame Relay	(2)	Yes	Yes	Yes	Yes
PPP over ATM SVC	(3)	Yes	Yes	Yes	Yes

Table 10 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
<b>Bridging and IBM Networking</b>					
Bridging Between IEEE 802.1Q vLANs	(3)	Yes	Yes	Yes	Yes
SDLC SNRM Timer and Window Size Enhancements	(5)	Yes	Yes	Yes	Yes
SNMP Support for IOS vLAN Subinterfaces	(3)	Yes	Yes	Yes	Yes
TN3270 Server Connectivity Enhancements	(5)	Yes	Yes	Yes	Yes
<b>Configuration Fundamentals</b>					
AutoInstall Using DHCP for LAN Interfaces	(5)	Yes	Yes	Yes	Yes
Configuration through SNMP	(3)	Yes	No	No	Yes
Event MIB	(3)	Yes	Yes	Yes	Yes
Expression MIB Support of Delta, Wildcarding and Aggregation	(3)	Yes	No	No	Yes
Individual SNMP Trap Support	(3)	Yes	Yes	Yes	Yes
Interface Index Persistence	(5)	Yes	Yes	Yes	Yes
Interface Range Specification	(5)	Yes	Yes	Yes	Yes
NTP MIB	(5)	Yes	Yes	Yes	Yes
Parser Cache	(5)	Yes	Yes	Yes	Yes
WCCP Redirection on Inbound Interfaces	(3)	Yes	No	No	Yes
<b>Connectivity/Scalability</b>					
PPPoE on ATM	(1)	Yes	Yes	Yes	Yes
PPP Over Fast Ethernet 802.1Q	(5)	Yes	Yes	Yes	Yes
<b>Interfaces</b>					
FastEther Channel Enhancements on Cisco 7200 Series Routers	(5)	Yes	Yes	Yes	Yes
<b>IP Addressing and Services</b>					
HSRP support for MPLS VPNs	(3)	Yes	Yes	Yes	Yes
NAT—Enhanced H.225/H.245 Forwarding Engine	(5)	Yes	Yes	Yes	Yes



Table 10 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
NAT—Support for NetMeeting Directory (Internet Locator Service—ILS)	(5)	Yes	Yes	Yes	Yes
NAT—Support of H.323 v2 Call Signalling (FastConnect)	(5)	Yes	Yes	Yes	Yes
NAT—Support of IP Phone to Cisco Call Manager	(5)	Yes	Yes	Yes	Yes
Turbo Access Control Lists	(5)	Yes	Yes	Yes	Yes
<b>IP Multicast</b>					
Bidirectional PIM	(2)	Yes	Yes	Yes	Yes
IGMP, Version 3	(5)	Yes	Yes	Yes	Yes
PIM Dense Mode State Refresh	(5)	Yes	Yes	Yes	Yes
Router-Port Group Management Protocol	(5)	Yes	Yes	Yes	Yes
Source Specific Multicast	(3)	Yes	Yes	Yes	Yes
<b>IP Routing</b>					
HSRP Support for ICMP Redirects	(3)	Yes	Yes	Yes	Yes
Minimum Masking Ability for NetFlow Router-Based Aggregation Schemes	(2)	Yes	Yes	Yes	Yes
OSPF Flooding Reduction	(2)	Yes	Yes	Yes	Yes
<b>Management</b>					
Service Assurance Agent Enhancement	(1)	Yes	Yes	Yes	Yes
<b>Miscellaneous</b>					
H.323 Version 2 Support	(1)	Yes	Yes	Yes	Yes
Inter-Autonomous Systems MPLS VPN Support	(5)	Yes	Yes	Yes	Yes
MPLS Traffic Engineering and Enhancements	(3)	Yes	Yes	Yes	Yes
Virtual Switch Interface Master MIB	(3)	Yes	Yes	Yes	Yes
VPN Accelerator Card Enhancements	(5)	No	Yes	Yes	No
<b>Mobile Wireless</b>					
General Packet Radio Service Release 1.4	(3)	No	No	No	No
<b>Multiservice Applications—DSL</b>					
CEF Switching for Routed Bridge Encapsulation	(5)	Yes	Yes	Yes	Yes
PPPoE Radius Port Identification	(5)	Yes	Yes	Yes	Yes
<b>Multiservice Applications—Voice</b>					
Interworking Signaling Enhancements for H.323 and SIP VoIP	(5)	Yes	Yes	Yes	Yes
T.38 Fax Relay for Voice over IP H.323	(3)	Yes	Yes	Yes	Yes
<b>Quality of Service</b>					

Table 10 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
Class-Based Marking	(3)	Yes	Yes	Yes	Yes
Class-Based Ethernet CoS Matching and Marking	(5)	Yes	Yes	Yes	Yes
Class-Based Policer for the DiffServ AF PHB	(5)	Yes	Yes	Yes	Yes
Class-Based QoS MIB	(5)	Yes	Yes	Yes	Yes
Class-Based Shaping	(3)	Yes	No	No	No
Configurable Per ATM-VC Hold Queue Size	(5)	Yes	Yes	Yes	Yes
COPS for RSVP	(1)	Yes	Yes	Yes	Yes
DiffServ Compliant WRED	(5)	Yes	Yes	Yes	Yes
IP DSCP marking for Frame-Relay PVC	(5)	Yes	Yes	Yes	Yes
Network-based Application Recognition	(5)	Yes	Yes	Yes	Yes
Quality of Service Device Manager Command-Line Interface Commands	(5)	Yes	Yes	Yes	Yes
Quality of Service for Virtual Private Networks	(5)	Yes	Yes	Yes	Yes
RSVP Support for Frame Relay	(5)	Yes	Yes	Yes	Yes
RSVP Support for Low Latency Queuing	(3)	Yes	Yes	Yes	Yes
Set ATM CLP Bit	(5)	Yes	Yes	Yes	Yes
<b>Reliability</b>					
PGM Host	(1)	Yes	Yes	Yes	Yes
<b>Security</b>					
AAA Broadcast Accounting	(1)	Yes	Yes	Yes	Yes
AAA Server Group Deadtimer	(2)	Yes	Yes	Yes	Yes
Ecosystem Gatekeeper Interoperability Enhancements	(1)	No	No	No	Yes
Gateway-to-Gatekeeper Billing Redundancy	(1)	Yes	No	No	Yes
IKE Extended Authentication	(1)	No	Yes	Yes	No
Secure Shell, Version 1 Integrated Client	(3)	No	Yes	Yes	No
SSH, Version 1 Support for T Train	(1)	Yes	Yes	Yes	Yes
Wildcard Pre-Shared Key Enhancement	(1)	No	Yes	Yes	No
<b>Switching</b>					
CEF Support for IP Routing between IEEE 802.1Q vLANs	(3)	Yes	Yes	Yes	Yes
MPLS Class of Service Enhancements	(5)	Yes	Yes	Yes	Yes
MPLS Scalability Enhancements for LSC and ATM LSR	(5)	Yes	Yes	Yes	Yes
Traceroute Enhancement for MPLS	(5)	Yes	Yes	Yes	Yes
Virtual Profile CEF Switched	(2)	Yes	Yes	Yes	Yes

Table 10 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
<b>Voice, Data, and Phone Connectivity</b>					
Answer Supervision Reporting	(1)	No	No	No	No
Cisco H.323, Version 2, Phase 2	(1)	Yes	Yes	Yes	Yes
Configurable Timers in H.225	(2)	Yes	Yes	Yes	Yes
Ecosystem Gatekeeper Interoperability Enhancements, Phase 2	(2)	Yes	Yes	Yes	Yes
Gatekeeper-to-Gatekeeper Redundancy and Load-Sharing	(2)	Yes	Yes	Yes	Yes
H.323 Support for Virtual Interfaces	(2)	Yes	Yes	Yes	Yes
ISDN Network Side for PRI for ETSI Net5 PRI	(1)	Yes	Yes	Yes	Yes
PRI and BRI QSIG Protocol Support on the Cisco 2600, 3600 and MC3810 Series Routers and PRI QSIG on the Cisco 7200	(2)	Yes	Yes	Yes	Yes
Transparent Common Channel Signaling	(3)	Yes	Yes	Yes	Yes
Voice Over Frame Relay Configuration Enhancements	(2)	Yes	Yes	Yes	Yes
<b>WAN</b>					
CUG Selection Facility Suppress Option	(5)	Yes	Yes	Yes	Yes
Frame Relay ELMI Address Registration	(3)	Yes	Yes	Yes	Yes
Frame Relay Fragmentation with Hardware Compression	(5)	Yes	Yes	Yes	Yes
Frame Relay PVC Interface Priority Queueing	(2)	Yes	Yes	Yes	Yes
Frame Relay Switching Diagnostics and Troubleshooting	(5)	Yes	Yes	Yes	Yes
Frame Relay Switching Enhancements	(2)	Yes	Yes	Yes	Yes
Low Latency Queueing for Frame Relay	(2)	Yes	Yes	Yes	Yes
PPP over ATM SVC	(3)	Yes	Yes	Yes	Yes

Table 11 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
<b>Bridging and IBM Networking</b>					
Bridging Between IEEE 802.1Q vLANs	(3)	Yes	Yes	No	No
SDLC SNRM Timer and Window Size Enhancements	(5)	Yes	Yes	Yes	Yes

Table 11 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
SNMP Support for IOS vLAN Subinterfaces	(3)	Yes	Yes	Yes	Yes
TN3270 Server Connectivity Enhancements	(5)	Yes	Yes	Yes	Yes
<b>Configuration Fundamentals</b>					
AutoInstall Using DHCP for LAN Interfaces	(5)	Yes	Yes	Yes	Yes
Configuration though SNMP	(3)	No	No	Yes	No
Event MIB	(3)	Yes	Yes	Yes	No
Expression MIB Support of Delta, Wildcarding and Aggregation	(3)	No	No	Yes	No
Individual SNMP Trap Support	(3)	No	No	Yes	No
Interface Index Persistence	(5)	Yes	Yes	Yes	Yes
Interface Range Specification	(5)	Yes	Yes	Yes	Yes
NTP MIB	(5)	Yes	Yes	Yes	Yes
Parser Cache	(5)	Yes	Yes	Yes	Yes
WCCP Redirection on Inbound Interfaces	(3)	No	No	Yes	No
<b>Connectivity/Scalability</b>					
PPPoE on ATM	(1)	Yes	Yes	Yes	Yes
PPP Over Fast Ethernet 802.1Q	(5)	Yes	Yes	Yes	Yes
<b>Interfaces</b>					
FastEther Channel Enhancements on Cisco 7200 Series Routers	(5)	Yes	Yes	Yes	Yes
<b>IP Addressing and Services</b>					
HSRP support for MPLS VPNs	(3)	Yes	Yes	Yes	Yes
NAT—Enhanced H.225/H.245 Forwarding Engine	(5)	Yes	Yes	No	No
NAT—Support for NetMeeting Directory (Internet Locator Service—ILS)	(5)	Yes	Yes	Yes	Yes
NAT—Support of H.323 v2 Call Signalling (FastConnect)	(5)	Yes	Yes	No	No
NAT—Support of IP Phone to Cisco Call Manager	(5)	Yes	Yes	Yes	Yes
Turbo Access Control Lists	(5)	Yes	Yes	Yes	Yes
<b>IP Multicast</b>					
Bidirectional PIM	(2)	Yes	Yes	Yes	Yes
IGMP, Version 3	(5)	Yes	Yes	Yes	Yes
PIM Dense Mode State Refresh	(5)	Yes	Yes	Yes	Yes
Router-Port Group Management Protocol	(5)	Yes	Yes	Yes	Yes
Source Specific Multicast	(3)	Yes	Yes	Yes	Yes

Table 11 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
<b>IP Routing</b>					
HSRP Support for ICMP Redirects	(3)	Yes	Yes	Yes	Yes
Minimum Masking Ability for NetFlow Router-Based Aggregation Schemes	(2)	Yes	Yes	Yes	Yes
OSPF Flooding Reduction	(2)	Yes	Yes	Yes	Yes
<b>Management</b>					
Service Assurance Agent Enhancement	(1)	Yes	Yes	Yes	Yes
<b>Miscellaneous</b>					
H.323 Version 2 Support	(1)	Yes	Yes	Yes	Yes
Inter-Autonomous Systems MPLS VPN Support	(5)	Yes	Yes	No	No
MPLS Traffic Engineering and Enhancements	(3)	Yes	Yes	No	No
Virtual Switch Interface Master MIB	(3)	Yes	Yes	No	No
VPN Accelerator Card Enhancements	(5)	Yes	Yes	No	Yes
<b>Mobile Wireless</b>					
General Packet Radio Service Release 1.4	(3)	No	No	No	No
<b>Multiservice Applications—DSL</b>					
CEF Switching for Routed Bridge Encapsulation	(5)	Yes	Yes	Yes	Yes
PPPoE Radius Port Identification	(5)	Yes	Yes	Yes	Yes
<b>Multiservice Applications—Voice</b>					
Interworking Signaling Enhancements for H.323 and SIP VoIP	(5)	Yes	Yes	Yes	Yes
T.38 Fax Relay for Voice over IP H.323	(3)	Yes	Yes	Yes	Yes
<b>Quality of Service</b>					
Class-Based Marking	(3)	Yes	Yes	Yes	Yes
Class-Based Ethernet CoS Matching and Marking	(5)	Yes	Yes	Yes	Yes
Class-Based Policer for the DiffServ AF PHB	(5)	Yes	Yes	Yes	Yes
Class-Based QoS MIB	(5)	Yes	Yes	Yes	Yes
Class-Based Shaping	(3)	No	No	Yes	No
Configurable Per ATM-VC Hold Queue Size	(5)	Yes	Yes	Yes	Yes
COPS for RSVP	(1)	Yes	Yes	Yes	Yes
DiffServ Compliant WRED	(5)	Yes	Yes	Yes	Yes
IP DSCP marking for Frame-Relay PVC	(5)	Yes	Yes	Yes	Yes
Network-based Application Recognition	(5)	Yes	Yes	Yes	Yes
Quality of Service Device Manager Command-Line Interface Commands	(5)	Yes	Yes	Yes	Yes

Table 11 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
Quality of Service for Virtual Private Networks	(5)	Yes	Yes	Yes	Yes
RSVP Support for Frame Relay	(5)	Yes	Yes	Yes	Yes
RSVP Support for Low Latency Queuing	(3)	Yes	Yes	Yes	Yes
Set ATM CLP Bit	(5)	Yes	Yes	Yes	Yes
<b>Reliability</b>					
PGM Host	(1)	Yes	Yes	No	No
<b>Security</b>					
AAA Broadcast Accounting	(1)	Yes	Yes	Yes	Yes
AAA Server Group Deadtimer	(2)	Yes	Yes	Yes	Yes
Ecosystem Gatekeeper Interoperability Enhancements	(1)	Yes	No	No	No
Gateway-to-Gatekeeper Billing Redundancy	(1)	No	No	Yes	No
IKE Extended Authentication	(1)	Yes	Yes	No	Yes
Secure Shell, Version 1 Integrated Client	(3)	Yes	Yes	No	Yes
SSH, Version 1 Support for T Train	(1)	Yes	Yes	No	Yes
Wildcard Pre-Shared Key Enhancement	(1)	Yes	Yes	No	Yes
<b>Switching</b>					
CEF Support for IP Routing between IEEE 802.1Q vLANs	(3)	Yes	Yes	Yes	Yes
MPLS Class of Service Enhancements	(5)	Yes	Yes	No	No
MPLS Scalability Enhancements for LSC and ATM LSR	(5)	Yes	Yes	No	No
Traceroute Enhancement for MPLS	(5)	Yes	Yes	No	No
Virtual Profile CEF Switched	(2)	Yes	Yes	Yes	Yes
<b>Voice, Data, and Phone Connectivity</b>					
Answer Supervision Reporting	(1)	No	No	No	No
Cisco H.323, Version 2, Phase 2	(1)	Yes	Yes	Yes	Yes
Configurable Timers in H.225	(2)	Yes	Yes	Yes	No
Ecosystem Gatekeeper Interoperability Enhancements, Phase 2	(2)	Yes	Yes	Yes	Yes
Gatekeeper-to-Gatekeeper Redundancy and Load-Sharing	(2)	Yes	Yes	Yes	Yes
H.323 Support for Virtual Interfaces	(2)	Yes	Yes	Yes	Yes
ISDN Network Side for PRI for ETSI Net5 PRI	(1)	Yes	Yes	Yes	Yes
PRI and BRI QSIG Protocol Support on the Cisco 2600, 3600 and MC3810 Series Routers and PRI QSIG on the Cisco 7200	(2)	Yes	Yes	Yes	Yes

Table 11 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
Transparent Common Channel Signaling	(3)	Yes	Yes	Yes	Yes
Voice Over Frame Relay Configuration Enhancements	(2)	Yes	Yes	Yes	Yes
<b>WAN</b>					
CUG Selection Facility Suppress Option	(5)	Yes	Yes	Yes	Yes
Frame Relay ELMI Address Registration	(3)	Yes	Yes	Yes	Yes
Frame Relay Fragmentation with Hardware Compression	(5)	Yes	Yes	Yes	Yes
Frame Relay PVC Interface Priority Queueing	(2)	Yes	Yes	Yes	Yes
Frame Relay Switching Diagnostics and Troubleshooting	(5)	Yes	Yes	Yes	Yes
Frame Relay Switching Enhancements	(2)	Yes	Yes	Yes	Yes
Low Latency Queueing for Frame Relay	(2)	Yes	Yes	Yes	Yes
PPP over ATM SVC	(3)	Yes	Yes	Yes	Yes

Table 12 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
<b>Bridging and IBM Networking</b>				
Bridging Between IEEE 802.1Q vLANs	(3)	No	No	No
SDLC SNRM Timer and Window Size Enhancements	(5)	Yes	Yes	Yes
SNMP Support for IOS vLAN Subinterfaces	(3)	Yes	Yes	No
TN3270 Server Connectivity Enhancements	(5)	Yes	Yes	Yes
<b>Configuration Fundamentals</b>				
AutoInstall Using DHCP for LAN Interfaces	(5)	Yes	Yes	Yes
Configuration through SNMP	(3)	Yes	No	No
Event MIB	(3)	Yes	Yes	Yes
Expression MIB Support of Delta, Wildcarding and Aggregation	(3)	Yes	No	No
Individual SNMP Trap Support	(3)	Yes	Yes	Yes
Interface Index Persistence	(5)	Yes	Yes	Yes
Interface Range Specification	(5)	Yes	Yes	Yes
NTP MIB	(5)	Yes	Yes	Yes
Parser Cache	(5)	Yes	Yes	Yes

Table 12 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
WCCP Redirection on Inbound Interfaces	(3)	Yes	No	No
<b>Connectivity/Scalability</b>				
PPPoE on ATM	(1)	Yes	Yes	No
PPP Over Fast Ethernet 802.1Q	(5)	Yes	Yes	Yes
<b>Interfaces</b>				
FastEther Channel Enhancements on Cisco 7200 Series Routers	(5)	Yes	Yes	Yes
<b>IP Addressing and Services</b>				
HSRP support for MPLS VPNs	(3)	Yes	Yes	Yes
NAT—Enhanced H.225/H.245 Forwarding Engine	(5)	Yes	Yes	Yes
NAT—Support for NetMeeting Directory (Internet Locator Service—ILS)	(5)	Yes	Yes	Yes
NAT—Support of H.323 v2 Call Signalling (FastConnect)	(5)	Yes	Yes	Yes
NAT—Support of IP Phone to Cisco Call Manager	(5)	Yes	Yes	Yes
Turbo Access Control Lists	(5)	Yes	Yes	Yes
<b>IP Multicast</b>				
Bidirectional PIM	(2)	Yes	Yes	Yes
IGMP, Version 3	(5)	Yes	Yes	Yes
PIM Dense Mode State Refresh	(5)	Yes	Yes	Yes
Router-Port Group Management Protocol	(5)	Yes	Yes	Yes
Source Specific Multicast	(3)	Yes	Yes	Yes
<b>IP Routing</b>				
HSRP Support for ICMP Redirects	(3)	Yes	Yes	Yes
Minimum Masking Ability for NetFlow Router-Based Aggregation Schemes	(2)	Yes	Yes	Yes
OSPF Flooding Reduction	(2)	Yes	Yes	Yes
<b>Management</b>				
Service Assurance Agent Enhancement	(1)	Yes	Yes	Yes
<b>Miscellaneous</b>				
H.323 Version 2 Support	(1)	Yes	Yes	Yes
Inter-Autonomous Systems MPLS VPN Support	(5)	No	No	No
MPLS Traffic Engineering and Enhancements	(3)	No	No	No
Virtual Switch Interface Master MIB	(3)	No	No	No
VPN Accelerator Card Enhancements	(5)	No	Yes	No



Table 12 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
<b>Mobile Wireless</b>				
General Packet Radio Service Release 1.4	(3)	No	No	No
<b>Multiservice Applications—DSL</b>				
CEF Switching for Routed Bridge Encapsulation	(5)	Yes	Yes	Yes
PPPoE Radius Port Identification	(5)	Yes	Yes	Yes
<b>Multiservice Applications—Voice</b>				
Interworking Signaling Enhancements for H.323 and SIP VoIP	(5)	Yes	Yes	Yes
T.38 Fax Relay for Voice over IP H.323	(3)	Yes	Yes	Yes
<b>Quality of Service</b>				
Class-Based Marking	(3)	Yes	Yes	Yes
Class-Based Ethernet CoS Matching and Marking	(5)	Yes	Yes	Yes
Class-Based Policer for the DiffServ AF PHB	(5)	Yes	Yes	Yes
Class-Based QoS MIB	(5)	Yes	Yes	Yes
Class-Based Shaping	(3)	Yes	No	No
Configurable Per ATM-VC Hold Queue Size	(5)	Yes	Yes	Yes
COPS for RSVP	(1)	Yes	Yes	Yes
DiffServ Compliant WRED	(5)	Yes	Yes	Yes
IP DSCP marking for Frame-Relay PVC	(5)	Yes	Yes	Yes
Network-based Application Recognition	(5)	Yes	Yes	Yes
Quality of Service Device Manager Command-Line Interface Commands	(5)	Yes	Yes	Yes
Quality of Service for Virtual Private Networks	(5)	Yes	Yes	Yes
RSVP Support for Frame Relay	(5)	Yes	Yes	Yes
RSVP Support for Low Latency Queuing	(3)	Yes	Yes	Yes
Set ATM CLP Bit	(5)	Yes	Yes	Yes
<b>Reliability</b>				
PGM Host	(1)	No	No	No
<b>Security</b>				
AAA Broadcast Accounting	(1)	Yes	Yes	Yes
AAA Server Group Deadtimer	(2)	Yes	Yes	Yes
Cisco H.323, Version 2, Phase 2	(1)	Yes	Yes	No
Ecosystem Gatekeeper Interoperability Enhancements	(1)	No	No	No
Gateway-to-Gatekeeper Billing Redundancy	(1)	No	No	No
IKE Extended Authentication	(1)	No	Yes	Yes

Table 12 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
Secure Shell, Version 1 Integrated Client	(3)	No	Yes	Yes
SSH, Version 1 Support for T Train	(1)	No	Yes	Yes
Wildcard Pre-Shared Key Enhancement	(1)	No	Yes	Yes
<b>Switching</b>				
CEF Support for IP Routing between IEEE 802.1Q vLANs	(3)	Yes	Yes	No
MPLS Class of Service Enhancements	(5)	No	No	No
MPLS Scalability Enhancements for LSC and ATM LSR	(5)	No	No	No
Traceroute Enhancement for MPLS	(5)	No	No	No
Virtual Profile CEF Switched	(2)	Yes	Yes	Yes
<b>Voice, Data, and Phone Connectivity</b>				
Answer Supervision Reporting	(1)	No	No	No
Cisco H.323, Version 2 Phase 2	(1)	Yes	Yes	Yes
Configurable Timers in H.225	(2)	No	No	No
Ecosystem Gatekeeper Interoperability Enhancements, Phase 2	(2)	Yes	Yes	Yes
Gatekeeper-to-Gatekeeper Redundancy and Load-Sharing	(2)	No	No	No
H.323 Support for Virtual Interfaces	(2)	Yes	Yes	No
ISDN Network Side for PRI for ETSI Net5 PRI	(1)	Yes	Yes	Yes
PRI and BRI QSIG Protocol Support on the Cisco 2600, 3600 and MC3810 Series Routers and PRI QSIG on the Cisco 7200	(2)	Yes	Yes	No
Transparent Common Channel Signaling	(3)	Yes	Yes	Yes
Voice Over Frame Relay Configuration Enhancements	(2)	Yes	Yes	No
<b>WAN</b>				
CUG Selection Facility Suppress Option	(5)	Yes	Yes	Yes
Frame Relay ELMI Address Registration	(3)	Yes	Yes	Yes
Frame Relay Fragmentation with Hardware Compression	(5)	Yes	Yes	Yes
Frame Relay PVC Interface Priority Queueing	(2)	Yes	Yes	Yes
Frame Relay Switching Diagnostics and Troubleshooting	(5)	Yes	Yes	Yes
Frame Relay Switching Enhancements	(2)	Yes	Yes	Yes

Table 12 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
Low Latency Queuing for Frame Relay	(2)	Yes	Yes	Yes
PPP over ATM SVC	(3)	Yes	Yes	Yes

Table 13 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
<b>Bridging and IBM Networking</b>					
Bridging Between IEEE 802.1Q vLANs	(3)	No	No	No	No
SDLC SNRM Timer and Window Size Enhancements	(5)	Yes	Yes	Yes	Yes
SNMP Support for IOS vLAN Subinterfaces	(3)	Yes	Yes	Yes	Yes
TN3270 Server Connectivity Enhancements	(5)	Yes	Yes	Yes	Yes
<b>Configuration Fundamentals</b>					
AutoInstall Using DHCP for LAN Interfaces	(5)	Yes	Yes	Yes	Yes
Circuit Interface Identification MIB	(3)	Yes	Yes	Yes	Yes
Event MIB	(3)	Yes	Yes	Yes	Yes
Interface Index Persistence	(5)	Yes	Yes	Yes	Yes
Interface Range Specification	(5)	Yes	Yes	Yes	Yes
MSDP MIB	(5)	Yes	Yes	Yes	Yes
Parser Cache	(5)	Yes	Yes	Yes	Yes
WCCP Redirection on Inbound Interfaces	(3)	Yes	No	No	Yes
<b>Connectivity/Scalability</b>					
PPPoE on ATM	(1)	Yes	Yes	Yes	Yes
PPP over Fast Ethernet 902.1Q	(5)	Yes	Yes	Yes	Yes
<b>IP Addressing and Services</b>					
HSRP Support for MPLS VPNs	(3)	Yes	Yes	Yes	Yes
NAT—Enhanced H.225/H.245 Forwarding Engine	(5)	No	No	No	Yes
NAT—Support for NetMeeting Directory (Internet Locator Service—ILS)	(5)	Yes	Yes	Yes	Yes
NAT—Support of H.323 v2 Call Signalling	(5)	No	No	No	Yes
NAT—Support of IP Phone to Cisco Call Manager	(5)	Yes	Yes	Yes	Yes
<b>IP Multicast</b>					
Bidirectional PIM	(2)	Yes	Yes	Yes	Yes
IGMP, Version 3	(5)	Yes	Yes	Yes	Yes

Table 13 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
PIM Dense Mode State Refresh	(5)	Yes	Yes	Yes	Yes
Router-Port Group Management Protocol	(5)	Yes	Yes	Yes	Yes
Source Specific Multicast	(3)	Yes	Yes	Yes	Yes
<b>IP Routing</b>					
HSRP Support for ICMP Redirects	(3)	Yes	Yes	Yes	Yes
Minimum Masking Ability for NetFlow Router-Based Aggregation Schemes	(2)	Yes	Yes	Yes	Yes
OSPF Flooding Reduction	(2)	Yes	Yes	Yes	Yes
<b>Management</b>					
Service Assurance Agent Enhancement	(1)	Yes	Yes	Yes	Yes
<b>Miscellaneous</b>					
Inter-Autonomous Systems MPLS VPN Support	(5)	No	No	No	No
MPLS Traffic Engineering and Enhancements	(3)	No	No	No	No
Virtual Switch Interface Master MIB	(3)	No	No	No	No
<b>Multiservice Applications—Voice</b>					
Interworking Signaling Enhancements for H.323 and SIP VoIP	(5)	Yes	Yes	Yes	Yes
PPPoE Radius Port Identification	(5)	Yes	Yes	Yes	Yes
<b>Quality of Service</b>					
Class-Based Ethernet CoS Matching and Marking	(5)	Yes	Yes	Yes	Yes
Class-Based QoS MIB	(5)	Yes	Yes	Yes	Yes
Class-Based Shaping	(3)	Yes	No	No	Yes
COPS for RSVP	(1)	Yes	Yes	Yes	No
Diffserv Compliant WRED	(5)	Yes	Yes	Yes	Yes
Distributed CRTP	(5)	Yes	Yes	Yes	Yes
Distributed FRF.11/12	(5)	Yes	Yes	Yes	Yes
Distributed Low Latency Queuing	(5)	Yes	Yes	Yes	Yes
Distributed Traffic Shaping	(5)	Yes	Yes	Yes	Yes
IP DSCP Marking for Frame-Relay PVC	(5)	Yes	Yes	Yes	Yes
Quality of Service Device Manager Command-Line Interface Commands	(5)	Yes	Yes	Yes	Yes
RSVP Support for Frame Relay	(5)	Yes	Yes	Yes	Yes
RSVP Support for Low Latency Queuing	(3)	Yes	Yes	Yes	Yes
Set ATM CLP Bit	(5)	Yes	Yes	Yes	Yes
VIP-based WFQ (dWFQ) support for RSVP	(5)	Yes	Yes	Yes	Yes
<b>Reliability</b>					

Table 13 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
PGM Host	(1)	No	No	No	No
<b>Security</b>					
IKE Extended Authentication	(1)	No	Yes	Yes	No
Secure Shell, Version 1 Integrated Client	(3)	No	Yes	Yes	No
SSH, Version 1 Support for T Train	(1)	No	Yes	Yes	No
Wildcard Pre-Shared Key Enhancement	(1)	No	Yes	Yes	No
<b>Switching</b>					
CEF Support for IP Routing between IEEE 802.1Q vLANs	(3)	Yes	Yes	Yes	Yes
MPLS Class of Service Enhancements	(5)	No	No	No	No
MPLS Scalability Enhancements for LSC and ATM LSR	(5)	No	No	No	No
Traceroute Enhancement for MPLS	(5)	No	No	No	No
Virtual Profile CEF Switched	(2)	Yes	Yes	Yes	Yes
<b>Voice, Data, and Phone Connectivity</b>					
ISDN Network Side for PRI for ETSI Net5 PRI	(1)	Yes	Yes	Yes	Yes
Transparent Common Channel Signaling	(3)	Yes	Yes	Yes	Yes
<b>WAN</b>					
CUG Selection Facility Suppress Option	(5)	Yes	Yes	Yes	Yes
Frame Relay ELMI Address Registration	(3)	Yes	Yes	Yes	Yes
Frame Relay PVC Interface Priority Queueing <sup>1</sup>	(2)	Yes	Yes	Yes	Yes
Frame Relay Switching Enhancements	(2)	Yes	Yes	Yes	Yes
PPP over ATM SVC	(3)	Yes	Yes	Yes	Yes

1. Support for Frame Relay PVC Interface Priority Queueing in RSP images is in nondistributed mode only.

Table 14 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
<b>Bridging and IBM Networking</b>					
Bridging Between IEEE 802.1Q vLANs	(3)	No	No	Yes	Yes
SDLC SNRM Timer and Window Size Enhancements	(5)	Yes	Yes	Yes	Yes
SNMP Support for IOS vLAN Subinterfaces	(3)	Yes	Yes	Yes	Yes
TN3270 Server Connectivity Enhancements	(5)	Yes	Yes	Yes	Yes
<b>Configuration Fundamentals</b>					

Table 14 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
AutoInstall Using DHCP for LAN Interfaces	(5)	Yes	Yes	Yes	Yes
Circuit Interface Identification MIB	(3)	Yes	Yes	Yes	No
Event MIB	(3)	Yes	Yes	Yes	Yes
Interface Index Persistence	(5)	Yes	Yes	Yes	Yes
Interface Range Specification	(5)	Yes	Yes	Yes	Yes
MSDP MIB	(5)	Yes	Yes	Yes	Yes
Parser Cache	(5)	Yes	Yes	Yes	Yes
WCCP Redirection on Inbound Interfaces	(3)	No	No	Yes	No
<b>Connectivity/Scalability</b>					
PPPoE on ATM	(1)	Yes	Yes	Yes	Yes
PPP over Fast Ethernet 902.1Q	(5)	Yes	Yes	Yes	Yes
<b>IP Addressing and Services</b>					
NAT—Enhanced H.225/H.245 Forwarding Engine	(5)	Yes	Yes	Yes	Yes
HSRP Support for MPLS VPNs	(3)	Yes	Yes	Yes	Yes
NAT—Support for NetMeeting Directory (Internet Locator Service—ILS)	(5)	Yes	Yes	Yes	Yes
NAT—Support of H.323 v2 Call Signalling	(5)	Yes	Yes	Yes	Yes
NAT—Support of IP Phone to Cisco Call Manager	(5)	Yes	Yes	Yes	Yes
<b>IP Multicast</b>					
Bidirectional PIM	(2)	Yes	Yes	Yes	Yes
IGMP, Version 3	(5)	Yes	Yes	Yes	Yes
PIM Dense Mode State Refresh	(5)	Yes	Yes	Yes	Yes
Router-Port Group Management Protocol	(5)	Yes	Yes	Yes	Yes
Source Specific Multicast	(3)	Yes	Yes	Yes	Yes
<b>IP Routing</b>					
HSRP Support for ICMP Redirects	(3)	Yes	Yes	Yes	Yes
Minimum Masking Ability for NetFlow Router-Based Aggregation Schemes	(2)	Yes	Yes	Yes	Yes
OSPF Flooding Reduction	(2)	Yes	Yes	Yes	Yes
<b>Management</b>					
Service Assurance Agent Enhancement	(1)	Yes	Yes	Yes	Yes
<b>Miscellaneous</b>					
Inter-Autonomous Systems MPLS VPN Support	(5)	No	No	Yes	Yes
MPLS Traffic Engineering and Enhancements	(3)	No	No	Yes	Yes
Virtual Switch Interface Master MIB	(3)	No	No	Yes	Yes

Table 14 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
<b>Multiservice Applications—Voice</b>					
Interworking Signaling Enhancements for H.323 and SIP VoIP	(5)	Yes	Yes	Yes	Yes
PPPoE Radius Port Identification	(5)	Yes	Yes	Yes	Yes
<b>Quality of Service</b>					
Class-Based Ethernet CoS Matching and Marking	(5)	Yes	Yes	Yes	Yes
Class-Based QoS MIB	(5)	Yes	Yes	Yes	Yes
Class-Based Shaping	(3)	No	No	Yes	No
COPS for RSVP	(1)	No	No	Yes	Yes
Diffserv Compliant WRED	(5)	Yes	Yes	Yes	Yes
Distributed CRTP	(5)	Yes	Yes	Yes	Yes
Distributed FRF.11/12	(5)	Yes	Yes	Yes	Yes
Distributed Low Latency Queuing	(5)	Yes	Yes	Yes	Yes
Distributed Traffic Shaping	(5)	Yes	Yes	Yes	Yes
IP DSCP Marking for Frame-Relay PVC	(5)	Yes	Yes	Yes	Yes
Quality of Service Device Manager Command-Line Interface Commands	(5)	Yes	Yes	Yes	Yes
RSVP Support for Frame Relay	(5)	Yes	Yes	Yes	Yes
RSVP Support for Low Latency Queuing	(3)	Yes	Yes	Yes	Yes
Set ATM CLP Bit	(5)	Yes	Yes	Yes	Yes
VIP-based WFQ (dWFQ) support for RSVP	(5)	Yes	Yes	Yes	Yes
<b>Reliability</b>					
PGM Host	(1)	No	No	Yes	Yes
<b>Security</b>					
IKE Extended Authentication	(1)	Yes	Yes	No	Yes
Secure Shell Version 1 Integrated Client	(3)	Yes	Yes	No	Yes
SSH Version 1 Support for T train	(1)	Yes	Yes	No	Yes
Wildcard Pre-Shared Key Enhancement	(1)	Yes	Yes	No	Yes
<b>Switching</b>					
CEF Support for IP Routing between IEEE 802.1Q vLANs	(3)	Yes	Yes	Yes	Yes
MPLS Class of Service Enhancements	(5)	No	No	Yes	Yes
MPLS Scalability Enhancements for LSC and ATM LSR	(5)	No	No	Yes	Yes
Traceroute Enhancement for MPLS	(5)	No	No	Yes	Yes
Virtual Profile CEF Switched	(2)	Yes	Yes	Yes	Yes

Table 14 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
<b>Voice, Data, and Phone Connectivity</b>					
ISDN Network Side for PRI for ETSI Net5 PRI	(1)	Yes	Yes	Yes	Yes
Transparent Common Channel Signaling	(3)	Yes	Yes	Yes	Yes
<b>WAN</b>					
CUG Selection Facility Suppress Option	(5)	Yes	Yes	Yes	Yes
Frame Relay ELMI Address Registration	(3)	Yes	Yes	Yes	Yes
Frame Relay PVC Interface Priority Queueing <sup>1</sup>	(2)	Yes	Yes	Yes	Yes
Frame Relay Switching Enhancements	(2)	Yes	Yes	Yes	Yes
PPP over ATM SVC	(3)	Yes	Yes	Yes	Yes

1. Support for Frame Relay PVC Interface Priority Queueing in RSP images is in non-distributed mode only.

Table 15 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
<b>Bridging and IBM Networking</b>					
Bridging Between IEEE 802.1Q vLANs	(3)	Yes	Yes	Yes	Yes
SDLC SNRM Timer and Window Size Enhancements	(5)	Yes	Yes	Yes	Yes
SNMP Support for IOS vLAN Subinterfaces	(3)	Yes	Yes	Yes	Yes
TN3270 Server Connectivity Enhancements	(5)	Yes	Yes	Yes	Yes
<b>Configuration Fundamentals</b>					
AutoInstall Using DHCP for LAN Interfaces	(5)	Yes	Yes	Yes	Yes
Circuit Interface Identification MIB	(3)	Yes	Yes	Yes	Yes
Event MIB	(3)	Yes	Yes	Yes	Yes
Interface Index Persistence	(5)	Yes	Yes	Yes	Yes
Interface Range Specification	(5)	Yes	Yes	Yes	Yes
MSDP MIB	(5)	Yes	Yes	Yes	Yes
Parser Cache	(5)	Yes	Yes	Yes	Yes
WCCP Redirection on Inbound Interfaces	(3)	No	Yes	No	No
<b>Connectivity/Scalability</b>					
PPPoE on ATM	(1)	Yes	Yes	Yes	Yes
PPP over Fast Ethernet 902.1Q	(5)	Yes	Yes	Yes	Yes
<b>IP Addressing and Services</b>					
HSRP Support for MPLS VPNs	(3)	Yes	Yes	Yes	Yes



Table 15 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
NAT—Enhanced H.225/H.245 Forwarding Engine	(5)	Yes	Yes	Yes	Yes
NAT—Support for NetMeeting Directory (Internet Locator Service—ILS)	(5)	Yes	Yes	Yes	Yes
NAT—Support of H.323 v2 Call Signalling	(5)	Yes	Yes	Yes	Yes
NAT—Support of IP Phone to Cisco Call Manager	(5)	Yes	Yes	Yes	Yes
<b>IP Multicast</b>					
Bidirectional PIM	(2)	Yes	Yes	Yes	Yes
IGMP, Version 3	(5)	Yes	Yes	Yes	Yes
PIM Dense Mode State Refresh	(5)	Yes	Yes	Yes	Yes
Router-Port Group Management Protocol	(5)	Yes	Yes	Yes	Yes
Source Specific Multicast	(3)	Yes	Yes	Yes	Yes
<b>IP Routing</b>					
HSRP Support for ICMP Redirects	(3)	Yes	Yes	Yes	Yes
Minimum Masking Ability for NetFlow Router-Based Aggregation Schemes	(2)	Yes	Yes	Yes	Yes
OSPF Flooding Reduction	(2)	Yes	Yes	Yes	Yes
<b>Management</b>					
Service Assurance Agent Enhancement	(1)	Yes	Yes	Yes	Yes
<b>Miscellaneous</b>					
Inter-Autonomous Systems MPLS VPN Support	(5)	Yes	Yes	Yes	Yes
MPLS Traffic Engineering and Enhancements	(3)	Yes	Yes	Yes	Yes
Virtual Switch Interface Master MIB	(3)	Yes	Yes	Yes	Yes
<b>Multiservice Applications—Voice</b>					
Interworking Signaling Enhancements for H.323 and SIP VoIP	(5)	Yes	Yes	Yes	Yes
PPPoE Radius Port Identification	(5)	Yes	Yes	Yes	Yes
<b>Quality of Service</b>					
Class-Based Ethernet CoS Matching and Marking	(5)	Yes	Yes	Yes	Yes
Class-Based QoS MIB	(5)	Yes	Yes	Yes	Yes
Class-Based Shaping	(3)	No	Yes	No	No
COPS for RSVP	(1)	Yes	No	No	No
Diffserv Compliant WRED	(5)	Yes	Yes	Yes	Yes
Distributed CRTP	(5)	Yes	Yes	Yes	Yes
Distributed FRF.11/12	(5)	Yes	Yes	Yes	Yes
Distributed Low Latency Queuing	(5)	Yes	Yes	Yes	Yes

Table 15 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
Distributed Traffic Shaping	(5)	Yes	Yes	Yes	Yes
IP DSCP Marking for Frame-Relay PVC	(5)	Yes	Yes	Yes	Yes
Quality of Service Device Manager Command-Line Interface Commands	(5)	Yes	Yes	Yes	Yes
RSVP Support for Frame Relay	(5)	Yes	Yes	Yes	Yes
RSVP Support for Low Latency Queuing	(3)	Yes	Yes	Yes	Yes
Set ATM CLP Bit	(5)	Yes	Yes	Yes	Yes
VIP-based WFQ (dWFQ) support for RSVP	(5)	Yes	Yes	Yes	Yes
<b>Reliability</b>					
PGM Host	(1)	Yes	Yes	Yes	Yes
<b>Security</b>					
IKE Extended Authentication	(1)	Yes	No	Yes	Yes
Secure Shell, Version 1 Integrated Client	(3)	Yes	No	Yes	Yes
SSH, Version 1 Support for T Train	(1)	Yes	No	Yes	Yes
Wildcard Pre-Shared Key Enhancement	(1)	Yes	No	Yes	Yes
<b>Switching</b>					
CEF Support for IP Routing between IEEE 802.1Q VLANs	(3)	Yes	Yes	Yes	Yes
MPLS Class of Service Enhancements	(5)	Yes	Yes	Yes	Yes
MPLS Scalability Enhancements for LSC and ATM LSR	(5)	Yes	Yes	Yes	Yes
Traceroute Enhancement for MPLS	(5)	Yes	Yes	Yes	Yes
Virtual Profile CEF Switched	(2)	Yes	Yes	Yes	Yes
<b>Voice, Data, and Phone Connectivity</b>					
ISDN Network Side for PRI for ETSI Net5 PRI	(1)	Yes	Yes	Yes	Yes
Transparent Common Channel Signaling	(3)	Yes	Yes	Yes	Yes
<b>WAN</b>					
CUG Selection Facility Suppress Option	(5)	Yes	Yes	Yes	Yes
Frame Relay ELMI Address Registration	(3)	Yes	Yes	Yes	Yes
Frame Relay PVC Interface Priority Queueing <sup>1</sup>	(2)	Yes	Yes	Yes	Yes
Frame Relay Switching Enhancements	(2)	Yes	Yes	Yes	Yes
PPP over ATM SVC	(3)	Yes	Yes	Yes	Yes

1. Support for Frame Relay PVC Interface Priority Queueing in RSP images is in nondistributed mode only.

Table 16 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
<b>Bridging and IBM Networking</b>					
Bridging Between IEEE 802.1Q vLANs	(3)	Yes	Yes	Yes	No
SDLC SNRM Timer and Window Size Enhancements	(5)	Yes	Yes	Yes	Yes
SNMP Support for IOS vLAN Subinterfaces	(3)	Yes	Yes	Yes	Yes
TN3270 Server Connectivity Enhancements	(5)	Yes	Yes	Yes	Yes
<b>Configuration Fundamentals</b>					
AutoInstall Using DHCP for LAN Interfaces	(5)	Yes	Yes	Yes	Yes
Circuit Interface Identification MIB	(3)	Yes	Yes	Yes	Yes
Event MIB	(3)	Yes	Yes	Yes	Yes
Interface Index Persistence	(5)	Yes	Yes	Yes	Yes
Interface Range Specification	(5)	Yes	Yes	Yes	Yes
MSDP MIB	(5)	Yes	Yes	Yes	Yes
Parser Cache	(5)	Yes	Yes	Yes	Yes
WCCP Redirection on Inbound Interfaces	(3)	Yes	No	No	Yes
<b>Connectivity/Scalability</b>					
PPPoE on ATM	(1)	Yes	Yes	Yes	Yes
PPP over Fast Ethernet 902.1Q	(5)	Yes	Yes	Yes	Yes
<b>IP Addressing and Services</b>					
HSRP Support for MPLS VPNs	(3)	Yes	Yes	Yes	Yes
NAT—Enhanced H.225/H.245 Forwarding Engine	(5)	Yes	Yes	Yes	No
NAT—Support for NetMeeting Directory (Internet Locator Service—ILS)	(5)	Yes	Yes	Yes	Yes
NAT—Support of H.323 v2 Call Signalling	(5)	Yes	Yes	Yes	No
NAT—Support of IP Phone to Cisco Call Manager	(5)	Yes	Yes	Yes	Yes
<b>IP Multicast</b>					
Bidirectional PIM	(2)	Yes	Yes	Yes	Yes
IGMP, Version 3	(5)	Yes	Yes	Yes	Yes
PIM Dense Mode State Refresh	(5)	Yes	Yes	Yes	Yes
Router-Port Group Management Protocol	(5)	Yes	Yes	Yes	Yes
Source Specific Multicast	(3)	Yes	Yes	Yes	Yes
<b>IP Routing</b>					
HSRP Support for ICMP Redirects	(3)	Yes	Yes	Yes	Yes
Minimum Masking Ability for NetFlow Router-Based Aggregation Schemes	(2)	Yes	Yes	Yes	Yes

Table 16 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
OSPF Flooding Reduction	(2)	Yes	Yes	Yes	Yes
<b>Management</b>					
Service Assurance Agent Enhancement	(1)	Yes	Yes	Yes	Yes
<b>Miscellaneous</b>					
Inter-Autonomous Systems MPLS VPN Support	(5)	Yes	Yes	Yes	No
MPLS Traffic Engineering and Enhancements	(3)	Yes	Yes	Yes	No
Virtual Switch Interface Master MIB	(3)	Yes	Yes	Yes	No
<b>Multiservice Applications—Voice</b>					
Interworking Signaling Enhancements for H.323 and SIP VoIP	(5)	Yes	Yes	Yes	Yes
PPPoE Radius Port Identification	(5)	Yes	Yes	Yes	Yes
<b>Quality of Service</b>					
Class-Based Ethernet CoS Matching and Marking	(5)	Yes	Yes	Yes	Yes
Class-Based QoS MIB	(5)	Yes	Yes	Yes	Yes
Class-Based Shaping	(3)	Yes	No	No	Yes
COPS for RSVP	(1)	Yes	Yes	Yes	Yes
Diffserv Compliant WRED	(5)	Yes	Yes	Yes	Yes
Distributed CRTP	(5)	Yes	Yes	Yes	Yes
Distributed FRF.11/12	(5)	Yes	Yes	Yes	Yes
Distributed Low Latency Queuing	(5)	Yes	Yes	Yes	Yes
Distributed Traffic Shaping	(5)	Yes	Yes	Yes	Yes
IP DSCP Marking for Frame-Relay PVC	(5)	Yes	Yes	Yes	Yes
Quality of Service Device Manager Command-Line Interface Commands	(5)	Yes	Yes	Yes	Yes
RSVP Support for Frame Relay	(5)	Yes	Yes	Yes	Yes
RSVP Support for Low Latency Queuing	(3)	Yes	Yes	Yes	Yes
Set ATM CLP Bit	(5)	Yes	Yes	Yes	Yes
VIP-based WFQ (dWFQ) support for RSVP	(5)	Yes	Yes	Yes	Yes
<b>Reliability</b>					
PGM Host	(1)	Yes	Yes	Yes	No
<b>Security</b>					
IKE Extended Authentication	(1)	No	Yes	Yes	No
Secure Shell, Version 1 Integrated Client	(3)	No	Yes	Yes	No
SSH, Version 1 Support for T Train	(1)	No	Yes	Yes	No
Wildcard Pre-Shared Key Enhancement	(1)	No	Yes	Yes	No

Table 16 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
<b>Switching</b>					
CEF Support for IP Routing between IEEE 802.1Q vLANs	(3)	Yes	Yes	Yes	Yes
MPLS Class of Service Enhancements	(5)	Yes	Yes	Yes	No
MPLS Scalability Enhancements for LSC and ATM LSR	(5)	Yes	Yes	Yes	No
Traceroute Enhancement for MPLS	(5)	Yes	Yes	Yes	No
Virtual Profile CEF Switched	(2)	Yes	Yes	Yes	Yes
<b>Voice, Data, and Phone Connectivity</b>					
ISDN Network Side for PRI for ETSI Net5 PRI	(1)	Yes	Yes	Yes	Yes
Transparent Common Channel Signaling	(3)	Yes	Yes	Yes	Yes
<b>WAN</b>					
CUG Selection Facility Suppress Option	(5)	Yes	Yes	Yes	Yes
Frame Relay ELMI Address Registration	(3)	Yes	Yes	Yes	Yes
Frame Relay PVC Interface Priority Queueing <sup>1</sup>	(2)	Yes	Yes	Yes	Yes
Frame Relay Switching Enhancements: Shaping and Policing	(2)	Yes	Yes	Yes	Yes
PPP over ATM SVC	(3)	Yes	Yes	Yes	Yes

1. Support for Frame Relay PVC Interface Priority Queueing in RSP images is in nondistributed mode only.

Table 17 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/ IP Sec 3DES
<b>Bridging and IBM Networking</b>					
Bridging Between IEEE 802.1Q vLANs	(3)	No	No	No	No
SDLC SNRM Timer and Window Size Enhancements	(5)	Yes	Yes	Yes	Yes
SNMP Support for IOS vLAN Subinterfaces	(3)	Yes	Yes	Yes	Yes
TN3270 Server Connectivity Enhancements	(5)	Yes	Yes	Yes	Yes
<b>Configuration Fundamentals</b>					
AutoInstall Using DHCP for LAN Interfaces	(5)	Yes	Yes	Yes	Yes
Circuit Interface Identification MIB	(3)	Yes	Yes	Yes	Yes
Event MIB	(3)	Yes	Yes	Yes	Yes
Interface Index Persistence	(5)	Yes	Yes	Yes	Yes

Table 17 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/ IP Sec 3DES
Interface Range Specification	(5)	Yes	Yes	Yes	Yes
MSDP MIB	(5)	Yes	Yes	Yes	Yes
Parser Cache	(5)	Yes	Yes	Yes	Yes
WCCP Redirection on Inbound Interfaces	(3)	No	Yes	No	No
<b>Connectivity/Scalability</b>					
PPPoE on ATM	(1)	Yes	Yes	Yes	No
PPP over Fast Ethernet 902.1Q	(5)	Yes	Yes	Yes	Yes
<b>IP Addressing and Services</b>					
HSRP support for MPLS VPNs	(3)	Yes	Yes	Yes	Yes
NAT—Enhanced H.225/H.245 Forwarding Engine	(5)	No	Yes	Yes	Yes
NAT—Support for NetMeeting Directory (Internet Locator Service—ILS)	(5)	Yes	Yes	Yes	Yes
NAT—Support of H.323 v2 Call Signalling	(5)	No	Yes	Yes	Yes
NAT—Support of IP Phone to Cisco Call Manager	(5)	Yes	Yes	Yes	Yes
<b>IP Multicast</b>					
Bidirectional PIM	(2)	Yes	Yes	Yes	Yes
IGMP, Version 3	(5)	Yes	Yes	Yes	Yes
PIM Dense Mode State Refresh	(5)	Yes	Yes	Yes	Yes
Router-Port Group Management Protocol	(5)	Yes	Yes	Yes	Yes
Source Specific Multicast	(3)	Yes	Yes	Yes	Yes
<b>IP Routing</b>					
HSRP Support for ICMP Redirects	(3)	Yes	Yes	Yes	Yes
Minimum Masking Ability for NetFlow Router-Based Aggregation Schemes	(2)	Yes	Yes	Yes	Yes
OSPF Flooding Reduction	(2)	Yes	Yes	Yes	Yes
<b>Management</b>					
Service Assurance Agent Enhancement	(1)	Yes	Yes	Yes	Yes
<b>Miscellaneous</b>					
Inter-Autonomous Systems MPLS VPN Support	(5)	No	No	No	No
MPLS Traffic Engineering and Enhancements	(3)	No	No	No	No
Virtual Switch Interface Master MIB	(3)	No	No	No	No
<b>Multiservice Applications—Voice</b>					
Interworking Signaling Enhancements for H.323 and SIP VoIP	(5)	Yes	Yes	Yes	Yes
PPPoE Radius Port Identification	(5)	Yes	Yes	Yes	Yes

Table 17 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/IP Sec 3DES
<b>Quality of Service</b>					
Class-Based Ethernet CoS Matching and Marking	(5)	Yes	Yes	Yes	Yes
Class-Based QoS MIB	(5)	Yes	Yes	Yes	Yes
Class-Based Shaping	(3)	No	Yes	No	No
COPS for RSVP	(1)	Yes	No	No	No
Diffserv Compliant WRED	(5)	Yes	Yes	Yes	Yes
Distributed CRTP	(5)	Yes	Yes	Yes	Yes
Distributed FRF.11/12	(5)	Yes	Yes	Yes	Yes
Distributed Low Latency Queuing	(5)	Yes	Yes	Yes	Yes
Distributed Traffic Shaping	(5)	Yes	Yes	Yes	Yes
IP DSCP Marking for Frame-Relay PVC	(5)	Yes	Yes	Yes	Yes
Quality of Service Device Manager Command-Line Interface Commands	(5)	Yes	Yes	Yes	Yes
RSVP Support for Frame Relay	(5)	Yes	Yes	Yes	Yes
RSVP Support for Low Latency Queuing	(3)	Yes	Yes	Yes	Yes
Set ATM CLP Bit	(5)	Yes	Yes	Yes	Yes
VIP-based WFQ (dWFQ) support for RSVP	(5)	Yes	Yes	Yes	Yes
<b>Reliability</b>					
PGM Host	(1)	No	No	No	No
<b>Security</b>					
IKE Extended Authentication	(1)	Yes	No	Yes	Yes
Secure Shell, Version 1 Integrated Client	(3)	Yes	No	Yes	Yes
SSH, Version 1 Support for T Train	(1)	Yes	No	Yes	Yes
Wildcard Pre-Shared Key Enhancement	(1)	Yes	No	Yes	Yes
<b>Switching</b>					
CEF Support for IP Routing between IEEE 802.1Q vLANs	(3)	Yes	Yes	Yes	No
MPLS Class of Service Enhancements	(5)	No	No	No	No
MPLS Scalability Enhancements for LSC and ATM LSR	(5)	No	No	No	No
Traceroute Enhancement for MPLS	(5)	No	No	No	No
Virtual Profile CEF Switched	(2)	Yes	Yes	Yes	Yes
<b>Voice, Data, and Phone Connectivity</b>					
ISDN Network Side for PRI for ETSI Net5 PRI	(1)	Yes	Yes	Yes	Yes
Transparent Common Channel Signaling	(3)	Yes	Yes	Yes	No

Table 17 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/ IP Sec 3DES
<b>WAN</b>					
CUG Selection Facility Suppress Option	(5)	Yes	Yes	Yes	Yes
Frame Relay ELMI Address Registration	(3)	Yes	Yes	Yes	Yes
Frame Relay PVC Interface Priority Queueing <sup>1</sup>	(2)	Yes	Yes	Yes	Yes
Frame Relay Switching Enhancements: Shaping and Policing	(2)	Yes	Yes	Yes	Yes
PPP over ATM SVC	(3)	Yes	Yes	Yes	Yes

1. Support for Frame Relay PVC Interface Priority Queueing in RSP images is in nondistributed mode only.

## New and Changed Information

The following sections list the new hardware and software features supported by the Cisco 7000 family for Release 12.1 T.

### New Software Features in Release 12.1(5)T1

There are no new software features supported in Cisco IOS Release 12.1(5)T1.

### New Hardware Features in Release 12.1(5)T1

There are no new hardware features supported in Cisco IOS Release 12.1(5)T1.

### New Software Features in Release 12.1(5)T

The following new software features are supported by the Cisco 7000 family for Cisco IOS Release 12.1(5)T:

#### AutoInstall Using DHCP for LAN Interfaces

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

The AutoInstall Using DHCP for LAN Interfaces feature replaces the use of the Bootstrap Protocol (BOOTP) with the use of the Dynamic Host Configuration Protocol (DHCP) for Cisco IOS AutoInstall over LAN interfaces. AutoInstall is a Cisco IOS software feature that provides for the configuration of a new routing device automatically when the device is initialized. DHCP (defined in RFC 2131) is based on the Bootstrap Protocol, which provides the framework for passing configuration information to hosts on a TCP/IP network. DHCP adds the capability of automatic allocation of reusable network addresses and additional configuration options. In Cisco IOS Release 12.1(5)T, the IP address procurement phase of the AutoInstall process is now accomplished using DHCP for Ethernet, Token Ring, and FDDI



interfaces. Prior to this release, IP addresses for LAN interfaces were obtained using BOOTP during the AutoInstall process. The AutoInstall Using DHCP for LAN Interfaces feature also enables the routing device to recognize IP address allocation messages coming from regular BOOTP servers, providing a seamless transition for those devices already using BOOTP servers for AutoInstall. Additionally, this feature enables uploading of configuration files using unicast TFTP.

## CEF Switching for Routed Bridge Encapsulation

Platforms: Cisco 7200 series routers

The CEF Switching for Routed Bridge Encapsulation feature adds Cisco Express Forwarding (CEF) switching support to ATM routed bridge encapsulation (RBE). Prior to this release, ATM RBE supported only fast switching and process switching.

The ATM RBE feature is used to route IP over bridged RFC 1483 Ethernet traffic from a stub-bridged LAN.

## Cisco 7200-I/O-GE+E and Cisco 7200-I/O-2FE/E Input/Output Controllers

Platforms: Cisco 7200 VXR routers

The Cisco 7200-I/O-GE+E is an Input/Output controller that provides one Gigabit Ethernet and one Ethernet port. It is equipped with a GBIC receptacle for 1000 megabits per second (Mbps) operation and an RJ-45 receptacle for 10 Mbps operation.

The Cisco 7200-I/O-2FE/E is an Input/Output controller that provides two autosensing Fast Ethernet ports and is equipped with two RJ-45 receptacles for 10/100 Mbps operation.

I/O controllers support the following features:

- Dual EIA/TIA-232 channels for local console and auxiliary ports
- NVRAM for storing the system configuration and environmental monitoring logs
- Two PC card slots that hold Flash Disks or Flash memory cards for storing the default Cisco IOS software image
- Flash memory for storing the boot helper image
- Two environmental sensors for monitoring the cooling air as it enters and leaves the chassis

## Cisco Quality of Service Device Manager 2.0 Support

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

Cisco Quality of Service Device Manager (QDM) is a web-based Java application with which users can configure and monitor advanced IP-based Quality of Service (QoS) functionality within Cisco routers using a graphical user interface (GUI).

QDM 2.0 is available as a separate product download and is free of charge. If you would like to install or reinstall QDM, see the *Release and Installation Notes for Cisco Quality of Service Device Manager 2.0* on Cisco.com and the Documentation CD-ROM.

## Class-Based Ethernet CoS Matching & Marking

Platforms: Cisco 7200 series and Cisco 7500 series routers

The Class-Based Ethernet Class of Service (CoS) Matching & Marking extends IOS capabilities to match packets by looking at the CoS value of the packet and mark packets with user defined CoS values. This feature can be used for L2 CoS to L3 TOS mapping. CoS Matching & Marking can be configured via the IOS QoS Mod CLI framework.

## Class-Based Quality of Service Management Information Base

Platforms: Cisco 7200 series with NPE150 or higher for T1/E1/Ethernet rates, Cisco 7200 series with NPE200 or higher for T3 rates, Cisco 7500/ Route Switch Processor (RSP)

The Class-Based Quality of Service Management Information Base (Class-Based QoS MIB) provides read access to class-based QoS configurations. This MIB also provides QoS statistics information based on the Modular QoS CLI, including information regarding class map and policy map parameters.

This Class-Based QoS MIB is actually two MIBs: CISCO-CLASS-BASED-QOS-MIB and CISCO-CLASS-BASED-QOS-CAPABILITY-MIB.

## Closed User Group Selection Facility Suppress Option

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

A closed user group (CUG) selection facility is a specific encoding element that allows a destination data terminal equipment (DTE) to identify the CUG to which the source and destination DTEs belong. The Closed User Group Selection Facility Suppress Option feature enables a user to configure an X.25 data communications equipment (DCE) interface or X.25 profile with a DCE station type to remove the CUG selection facility from incoming call packets destined for the preferential CUG only or for all CUGs. You can also remove the selection facility from a CUG with outgoing access (CUG/OA).

## Configurable per ATM-VC Hold Queue Size

Platforms: Cisco 7200 series routers

Using the Configurable per ATM-VC Hold Queue Size feature, customers can specify the number of packets contained in the hold queue, per virtual circuit (VC), on ATM adapters that support per-VC queueing. By default, the queueing mechanism in use determines the size of the hold queue, and, therefore, the number of packets contained in the queue. Customers can expand the default hold queue size and change (or vary) the number of packets the queue can contain. With this new feature, the hold queue can contain a maximum of 1024 packets. This feature provides a new command, called **vc-hold-queue**, with which the customer can specify the number of packets contained in the per-VC hold queue. This can be a number from 5 to 1024.

## DiffServ Compliant WRED

Platforms: Cisco 7200 series and Cisco 7500 series routers

The DiffServe Compliant WRED feature extends the functionality of WRED (weighted random early detection) to enable support for Differentiated Services (DiffServ) and Assured Forwarding (AF) Per Hop Behavior (PHB). This feature enables WRED to be compliant with the DiffServ standard and the AF PHB standard being developed by the Internet Engineering Task Force (IETF). Customers can implement AF PHB by coloring packets according to DSCP values and then assigning preferential drop

probabilities to those packets. This feature adds two new commands, **random-detect dscp** and **dscp**. It also adds two new arguments, *dscp-based* and *prec-based*, to two existing WRED-related commands—the **random-detect** (interface) command and the **random-detect-group** command.

## Distributed CRTP

Platforms: Cisco 7500 series routers

The Distributed Compressed Real-Time Transport Protocol (dCRTP) feature compresses the combined 40-byte IP/UDP/RTP packet headers to between two and four bytes on packets traveling on a Cisco 7500 series router with a Versatile Interface Processor (VIP) in distributed fast-switching and distributed Cisco Express Forwarding (dCEF) environments. This compression reduces the packet size, improves the speed of packet transmission, and reduces packet latency.

Before Cisco IOS Release 12.1(5)T, if compression of TCP or Real-Time Transport Protocol (RTP) headers was enabled on a Cisco 7500 series router with a VIP, the compression was performed in the process-switching path. That meant that packets traversing interfaces that had TCP or RTP header compression enabled were queued and passed up to the Route Switch Processor (RSP) to be switched. This procedure slowed down transmission of the packet, and therefore some users preferred to fast-switch uncompressed TCP and RTP packets rather than enable TCP and RTP compression.

If the dCRTP feature is enabled, the header compression of the combined IP/UDP/RTP header occurs by default in the distributed fast-switched path or the distributed Cisco Express Forwarding-switched (dCEF-switched) path, depending on which switching method is enabled on the interface.

If distributed fast-switching or distributed Cisco Express Forward switching are disabled, TCP or RTP header compression will occur in the process-switched path as before.

For additional information on dCRTP, see the *Distributed Compressed Real-Time Transport Protocol* feature module on Cisco.com and the Documentation CD-ROM.

## Distributed Low Latency Queuing

Platforms: Cisco 7500 series routers

The Low Latency Queueing feature, which was introduced for some router platforms in Cisco IOS Release 12.0(7)T, is now available for VIP-enabled Cisco 7500 series routers. The VIP-enabled Cisco 7500 series version of the Low Latency Queueing feature, which contains significant functionality differences from the standard Low Latency Queueing feature, is called Distributed Low Latency Queueing.

The Distributed Low Latency Queueing feature brings the ability to specify low latency behavior for a traffic class. Low Latency Queueing allows delay-sensitive data such as voice to be dequeued and sent first (before packets in other queues are dequeued), giving delay-sensitive data preferential treatment over other traffic.

The Distributed Low Latency Queueing feature also introduces the ability to limit the depth of a device transmission ring. Before the introduction of Distributed Low Latency Queueing, the maximum transmission ring depth was not a user-configurable parameter. Therefore, particles could accumulate on a transmission ring without limitation, which could result in unavoidable high latencies. The Distributed Low Latency Queueing feature allows users to limit the number of particles that may exist on a transmission ring, effectively lowering the latency incurred by packets sitting on that transmission ring.

For additional information on Distributed Low Latency Queueing, see the *Distributed Low Latency Queueing* feature module on Cisco.com and on the Documentation CD-ROM.

## Distributed Traffic Shaping

Platforms: Cisco 7500 series routers

The DTS feature is one element used to manage the bandwidth of an interface to avoid congestion, to meet remote site requirements, and to conform to a service rate that is provided on that interface.

DTS uses queues to buffer traffic surges that can congest a network. Data is buffered and then sent into the network at a regulated rate. This ensures that traffic will behave to the configured descriptor, as defined by command information rate (CIR), Committed Burst (Bc), and Excess Burst (Be). With the defined average bit rate and burst size that is acceptable on that shaped entity, you can derive a time interval value.

DTS provides two types of shape commands: average and peak. When shape average is configured, the interface sends no more than the Bc for each interval, achieving an average rate no higher than the CIR. When shape peak is configured, the interface sends Bc plus Be bits in each interval.

In a link layer network such as Frame Relay, the network sends messages with the forward explicit congestion notification (FECN) or backwards explicit congestion notification (BECN) if there is congestion. With the DTS feature, the traffic shaping adaptive mode takes advantage of these signals and adjusts the traffic descriptors. This approximates the rate to the available bandwidth along the path.

For additional information on Distributed Traffic Shaping, see the *Distributed Traffic Shaping* feature module on Cisco.com and the Documentation CD-ROM.

## FastEther Channel Enhancements on Cisco 7200 Series Routers

Platforms: Cisco 7200 series routers

FastEther Channel provides higher bidirectional bandwidth, redundancy, and load sharing. Up to four Fast Ethernet interfaces can be bundled in a port-channel, and the router or switch can support up to four port-channels. The FastEther Channel feature is capable of load balancing traffic across the Fast Ethernet links. Unicast, broadcast, and multicast traffic is distributed across the links providing higher performance and redundant parallel paths. In the event of a link failure, traffic is redirected to remaining links within the FastEther Channel without user intervention.

In this release of the FastEther Channel feature, IP traffic is distributed over the port-channel interface while traffic from other routing protocols is sent over a single link. Bridged traffic is distributed based on the Layer 3 information in the packet. If the Layer 3 information does not exist in the packet, the traffic is sent over the first link.

FastEther Channel supports all features currently supported on the Fast Ethernet interface. You must configure these features on the port-channel interface rather than on the individual Fast Ethernet interfaces. FastEther Channel connections are fully compatible with Cisco IOS virtual LAN (VLAN) and routing technologies. The Inter-Switch Link (ISL) VLAN trunking protocol can carry multiple VLANs across a FastEther Channel, and routers attached to FastEther Channel links can provide full multiprotocol routing with support for host standby using Host Standby Router Protocol (HSRP).

The port-channel (consisting of up to four Fast Ethernet interfaces) is treated as a single interface. Port-channel is used in the Cisco IOS software to maintain compatibility with existing commands on the Catalyst 5000 switch. You create the FastEther Channel by using the **interface port-channel** interface configuration command. You can assign up to four Fast Ethernet interfaces to a port-channel by using the **channel-group** interface configuration command

## Frame Relay Fragmentation with Hardware Compression

Platforms: Cisco 7200 series routers

The Frame Relay Fragmentation with Hardware Compression feature introduces the following functionality:

### Frame Relay Fragmentation and Hardware Compression Interoperability

This new feature enables FRF.12, FRF.11 Annex C, and Cisco proprietary fragmentation to work with hardware compression on interfaces and virtual circuits (VCs) using Cisco proprietary or Internet Engineering Task Force (IETF) encapsulation types.

### Hardware Compression and Header Compression Interoperability

The Frame Relay Fragmentation with Hardware Compression feature introduces a new, proprietary hardware and software compression protocol called data-stream compression, which can be used on the same VC or interface as header compression. Data-stream compression is functionally equivalent to FRF.9 compression and must be used with Cisco proprietary encapsulation. Frame Relay fragmentation can also be enabled.

### Hardware Compression and Software Compression Interoperability

The Frame Relay Fragmentation with Hardware Compression feature provides hardware and software compression interoperability when hardware compression is configured on one side of the link and software compression is configured on the other side.

## Frame Relay Switching Diagnostics and Troubleshooting

Platforms: Cisco 7200 series routers

The Frame Relay Switching Diagnostics and Troubleshooting feature enhances Frame Relay switching functionality by providing tools to diagnose problems in switched Frame Relay networks. The **show frame-relay pvc** command has been enhanced to display detailed reasons why packets were dropped from switched PVCs. The command will also display the local status, the Network-to-Network (NNI) status, and the overall status of NNI PVCs. If a network problem is observed, the new **debug frame-relay switching** command can be used to display the status of packets on switched PVCs at regular intervals. This new debug command displays information such as the number of packets that were switched, why packets were dropped, and changes in status of physical links and PVCs.

## IGMP, Version 3

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

Internet Group Management Protocol (IGMP) is a protocol used by IP v4 systems to report IP multicast group memberships to neighboring multicast routers. On networks with hosts directly attached, IGMP, Version 3 (IGMP v3) adds support for “source filtering,” which enables a multicast receiver to signal to a router which groups it wants to receive multicast traffic from, and from which sources this traffic is expected. Based on this membership information, Cisco IOS software only forwards traffic that is requested by the host (or by other routers via Protocol Independent Multicast (PIM)) to that network. In addition to restricting traffic on the network of the receiver host, IGMP v3 membership information may also be propagated to multicast routing protocols to enable the forwarding of traffic from permitted sources or to restrict traffic from denied sources along the entire multicast data delivery path.

In the Source Specific Multicast feature, introduced in Cisco IOS Release 12.1(5)T, hosts must explicitly include sources when joining a multicast group (this is known as “channel subscription”). IGMP v3 is the industry-designated standard protocol for hosts to signal channel subscriptions in SSM.

In deployment cases where IGMP v3 cannot be used (for example, if it is not supported by the receiver host or its applications), there are two other mechanisms to enable Source Specific Multicast (SSM): URL Rendezvous Directory (URD) and IGMP v3 lite. Both of these features were introduced with SSM in Cisco IOS Release 12.1(5)T.

## Inter-Autonomous Systems MPLS VPN Support

Platforms: Cisco 7200 series and Cisco 7500 series routers

The inter-autonomous systems for MPLS VPNs feature provides a seamless integration of autonomous systems and service providers. Separate autonomous systems from different service providers can communicate by exchanging IP v4 network layer reachability information (NLRI) in the form of VPN-IP v4 addresses. The autonomous systems' border edge routers use exterior border gateway protocol (EBGP) to exchange that information. Then, an interior gateway protocol (IGP) distributes the network layer information for VPN-IP v4 prefixes throughout each VPN and each autonomous system.

## Interface Index Persistence

Platforms: Cisco 7200 series and Cisco 7500 series routers

One of the most commonly used identifiers used in SNMP-based network management applications is the Interface Index (ifIndex) value. IfIndex is a unique identifying number associated with a physical or logical interface; as far as most software is concerned, the ifIndex is the name of the interface. Although there is no requirement in the relevant RFCs that the correspondence between particular ifIndex values and their interfaces be maintained across reboots, applications such as device inventory, billing, and fault detection increasingly depend on the maintenance of this correspondence.

Cisco IOS Release 12.1(5)T adds support for an ifIndex value that can persist across reboots, so that users can avoid the workarounds previously required for consistent interface identification. The Interface Index Persistence feature allows for greater accuracy when collecting and processing network management data by uniquely identifying input and output interfaces for traffic flows and SNMP statistics. Relating each interface to a known entity (such as an ISP customer) allows network management data to be more effectively utilized.

## Interface Range Specification

Platforms: Cisco 7200 series and Cisco 7500 series routers

The Interface Range Specification feature allows specification of a range of interfaces to which subsequent commands are applied and supports definition of macros that contain an interface range. The Interface Range Specification feature is implemented with the **range** keyword, which is used with the **interface** command. In the interface configuration mode with the **range** keyword, all entered commands are applied to all interfaces within the range until you exit interface configuration mode.

## Interworking Signalling Enhancements for H.323 and SIP VoIP

Platforms: Cisco 7200 series and Cisco 7500 series routers

The Interworking Signaling Enhancements for H.323 and SIP VoIP feature enables VoIP networks to properly signal the setup and tear-down of calls when interworking with PSTN networks. These enhancements ensure that in-band tones and announcements are generated when needed so that the voice path is cut-through at the appropriate point of call setup and that early alerting (ringing) does not occur. In addition, support for network-side ISDN and the reducing of speech clipping is addressed.

## IP DSCP Marking for Frame-Relay PVC

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

The functionality of configuring a policy on a main or a subinterface to match and set IP type of service (ToS) and differentiated services code point (DSCP) bits has existed in Cisco IOS Release 12.0S and Cisco IOS Release 12.0(7)XE. This feature was introduced to Cisco IOS 12.1(2)T with the added support of configuring a policy on an ATM PVC. This feature extends the support of Frame-Relay PVC in Cisco IOS Release 12.1(5)T.

## MPLS Class of Service Enhancements

Platforms: Cisco 7200 series and Cisco 7500 series routers

When a customer transmits IP packets from one site to another, the IP precedence field (the first three bits in the header of an IP packet) specifies the class of service (CoS) such as latency or the percent of bandwidth allowed for a particular class of service. The service provider might want to set an MPLS packet's CoS to a different value.

CoS transparency allows the service provider to set the MPLS experimental field instead of overwriting the value in the customer's IP precedence field. The IP header remains available for the customer's use; the IP packet CoS is not changed as the packet travels through the multiprotocol label switching (MPLS) network.

## MPLS Egress NetFlow Accounting

Platforms: Cisco 7200 series and Cisco 7500 series routers

The MPLS egress NetFlow accounting feature allows you to capture Internet Protocol (IP) flow information for packets undergoing MPLS label disposition; that is, packets that arrive on a router as MPLS and are transmitted as IP.

Previously, you captured NetFlow data only for flows that arrived on the packet in IP format. When an edge router performed MPLS label imposition (received an IP packet and transmitted it as an MPLS packet), NetFlow data was captured when the packet entered the network. Inside the network, the packet was switched based only on MPLS information, and thus NetFlow information was not captured until after the last label was removed.

One common application of the MPLS egress NetFlow accounting feature allows you to capture the MPLS virtual private network (VPN) IP flows that are traveling from one site of a VPN to another site of the same VPN through the service provider backbone.

Formerly, you captured flows only for IP packets on the ingress interface of a router. You could not capture flows for MPLS encapsulated frames, which were switched through Cisco Express Forwarding (CEF) from the input port. Therefore, in an MPLS VPN environment you captured flow information as packets were received from a customer edge (CE) router and forwarded to the backbone. However, you could not capture flow information as packets were transmitted to a CE router because those packets were received as MPLS frames.

The MPLS egress NetFlow accounting feature lets you capture the flows on the outgoing interfaces.

## MPLS Scalability Enhancements for LSC and ATM LSR

Platforms: Cisco 7200 series and Cisco 7500 series routers

The MPLS label switch controller (LSC), combined with slave ATM switch, supports scalable integration of IP services over an ATM network. The MPLS LSC enables the slave ATM switch to:

- Participate in an MPLS network
- Directly peer with IP routers
- Support the IP features in Cisco Internetwork Operating System (IOS) software

The MPLS LSC supports highly scalable integration of MPLS (IP+ATM) services by using a direct peer relationship between the ATM switch and MPLS routers. This direct peer relationship removes the limitation on the number of IP edge routers (typical of traditional IP-over-ATM networks), allowing service providers to meet growing demands for IP services. The MPLS LSC also supports direct and rapid implementation of advanced IP services over ATM networks using ATM switches.

MPLS combines the performance and virtual circuit capabilities of Layer 2 (data link layer) switching with the scalability of Layer 3 (network layer) routing capabilities. This combination enables service providers to deliver solutions for managing growth, providing differentiated services, and leveraging existing networking infrastructures.

The MPLS LSC architecture provides the flexibility to:

- Run applications over any combination of Layer 2 technologies
- Support any Layer 3 protocol while scaling the network to meet future needs

## MSDP MIB

Platforms: Cisco 7500 series routers

The Multicast Source Discovery Protocol (MSDP) MIB feature adds support in Cisco IOS software for the MSDP MIB. This MIB describes objects used for managing MSDP operations using Simple Network Management Protocol (SNMP). Documentation for this MIB exists in the form of an Internet Draft titled “Multicast Source Discovery Protocol MIB” (draft-ietf-msdp-mib-03.txt) and is available through the Internet Engineering Task Force (IETF) at <http://www.ietf.org>. Refer to the following document for further information:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t5/dt5msdp.htm>

## NAT—Enhanced H.225/H.245 Forwarding Engine

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

During the call setup between H.323 terminals, H.225/H.245 protocols are used. The protocol messages contain embedded IP addresses and ports. If a message passes through a NAT router, it has to be decoded, translated and encoded back to the packet. This enhancement extends support to all messages in H.225/H.245 protocols and all embedded addresses.

## NAT—Support of H.323 v2 Call Signalling (FastConnect)

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

Cisco IOS Network Address Translation (NAT) supports all H.225 and H.245 message types, including Fast Connect and Alerting as part of H.323 v2. Any product that makes use of these message types will be able to pass through a Cisco IOS NAT configuration without any static configuration.



## NAT—Support of IP Phone to Cisco Call Manager

Platforms: Cisco 7200 series and Cisco 7500 series routers

Cisco IP Phones use the Selsius Skinny Station Protocol to connect with and register to the Cisco Call Manager (CCM). Messages flow back and forth that include IP address and Port information which is used to identify other IP Phone users with which a call can be placed.

To be able to deploy Cisco IOS Network Address Translation (NAT) between the IP Phone and CCM in a scalable environment, NAT needs to be able to detect the Selsius Skinny Station Protocol and understand the information passed within the messages.

When an IP Phone attempts to connect to the CCM and it matches the configured NAT translation rules, NAT will translate the original source IP address and replace it with one from the configured pool. This new address is what will be reflected in the CCM and be visible to other IP Phone users.

## NAT—Support for NetMeeting Directory (Internet Locator Service—ILS)

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

Microsoft NetMeeting is a Windows-based application that enables multi-user interaction and collaboration from a users PC over the Internet or an intranet. Support for the NetMeeting Directory (ILS) allows connections by name from the directory built into the NetMeeting application. Destination IP addresses do not need to be known in order for a connection to be made.

## Network-Based Application Recognition

Platforms: Cisco 7100 series and Cisco 7200 series routers

Network-Based Application Recognition (NBAR) is a classification engine that recognizes a wide variety of applications, including Web-based and other difficult-to-classify protocols that utilize dynamic TCP/UDP port assignments. When an application is recognized and classified by NBAR, a network can invoke services for that specific application. NBAR ensures that network bandwidth is used efficiently by working with QoS features to provide bandwidth guarantees and limits, traffic shaping, and packet marking.

NBAR introduces several new classification features:

- Classification of applications which dynamically assign TCP/UDP port numbers
- Classification of HTTP traffic by URL, HOST, or MIME type
- Classification of Citrix ICA traffic by application name
- Classification of application traffic using subport information

NBAR can also classify static port protocols. Although Access Control Lists (ACLs) can also be used for this purpose, NBAR is easier to configure and can provide classification statistics that are not available when using ACLs.

NBAR provides a special Protocol Discovery feature that determines which application protocols are traversing a network at any given time. The Protocol Discovery feature captures key statistics associated with each protocol in a network. These statistics can be used to define traffic classes and QoS policies for each traffic class.

For additional information on NBAR, see the *Network-Based Application Recognition* feature module on Cisco.com and the Documentation CD-ROM.

## NTP MIB

Platforms: Cisco 7100 series and Cisco 7500 series routers

The Network Time Protocol (NTP) is used to synchronize timekeeping among a set of distributed time servers and clients. The Cisco NTP MIB enables users to remotely monitor an NTP server using the Simple Network Management Protocol (SNMP), provided the MIB itself is implemented on that server. Use of the NTP MIB to monitor the NTP status of routing devices is accomplished using software on a Network Management System (NMS). There are no new or modified Cisco IOS software commands associated with this feature.

The Cisco implementation of the NTP MIB is based on NTP version 3 (RFC-1305). The MIB objects are all read-only. SNMP requests are processed by reading the corresponding variables from the NTP subsystem and returning them in the response. The NTP MIB defines a set of NTP server system objects, including an NTP server peers table and an NTP server filter register table. For complete details on the Cisco implementation of the NTP MIB, see the MIB file itself (CISCO-NTP-MIB.my, available through Cisco.com at <http://www.cisco.com/public/mibs/v2/>).

## Parser Cache

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

The Parser Cache feature optimizes the parsing (translation) of Cisco IOS software configuration command lines by remembering how to parse recently encountered command lines. This feature was developed to improve the scalability of the Cisco IOS software command-line interface (CLI) parser when processing large configuration files. This improvement is especially useful for those cases in which thousands of virtual circuits must be configured for interfaces, or hundreds of access lists (ACLs) are required. The parser chain cache can rapidly recognize and translate configuration lines which differ slightly from previously used configuration lines (for example, pvc 0/100, pvc 0/101, and so on). Testing indicates an improvement to load time of between 30% and 36% for large configuration files when using the parser cache.

The parser cache is enabled by default on all platforms using Cisco IOS 12.1(5)T or later. A new command, **[no] parser cache**, allows the disabling or re-enabling of this feature.

## PIM Dense Mode State Refresh

Platforms: Cisco 7200 series and Cisco 7500 series routers

The PIM Dense Mode State Refresh feature keeps the pruned state in PIM dense mode from timing out by periodically forwarding a control message down the source-based distribution tree. The control message refreshes the prune state on the outgoing interfaces of each router in the distribution tree.

## PPPoE Radius Port Identification

Platforms: Cisco 7200 series and Cisco 7500 series routers

The PPPoE RADIUS Port Identification feature extends the concepts of NAS port and NAS port type to include VLAN ID for PPPoE over 802.1Q VLANs. It also adds the NAS port format-d extension, which was originally created for PPPoE over ATM and PPPoVLAN, to LACs and allows an LNS to forward to a RADIUS server the NAS port format-d information sent to it by an LAC.

The PPPoE RADIUS Port Identification feature brings consistency to the command-line keywords and value formats used to identify a NAS port and port type to a RADIUS server for the PPPoE over ATM, PPPoE over 802.1Q VLAN, and PPPoE over L2TP tunnels.

## PPP Over Fast Ethernet 802.1Q

Platforms: Cisco 7200 series and Cisco 7500 series routers

The PPPoE over IEEE 802.1Q Encapsulation feature adds support for running PPP over Ethernet over IEEE 802.1Q encapsulation. IEEE 802.1Q encapsulation enables you to interconnect a VLAN capable router with another VLAN capable device.

## Quality of Service for Virtual Private Networks

Platforms: Cisco 7100 series and Cisco 7200 series routers

With the introduction of the Quality of Service for Virtual Private Networks (QoS for VPNs) feature, packets can now be classified before tunneling and encryption occur (a process known as preclassification). The preclassification process is important because all tunnel traffic that is not preclassified is treated identically, making traffic flows impossible to adjust in congested environments.

When the QoS for VPN feature is enabled, the QoS features on the output interface classify packets before encryption, allowing traffic flows to be adjusted in congested environments. The end result is more effective packet tunneling.

For additional information on the QoS for VPNs feature, see the *Quality of Service for Virtual Private Networks* feature module on Cisco.com and the Documentation CD-ROM.

## Router-Port Group Management Protocol

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

The Router-Port Group Management Protocol (RGMP) feature introduces a Cisco protocol that restricts IP multicast traffic in switched networks. RGMP is a Layer 2 protocol that enables a router to communicate to a switch (or a networking device that is functioning as a Layer 2 switch) the multicast group for which the router would like to receive or forward traffic. RGMP restricts multicast traffic at the ports of RGMP-enabled switches that lead to interfaces of RGMP-enabled routers. RGMP is designed for switched Ethernet backbone networks running Protocol Independent Multicast (PIM) sparse mode.

## RSVP Support for Frame Relay

Platforms: Cisco 7200 series and Cisco 7500 series routers

Queueing manages congestion on a router interface or a virtual circuit (VC). In a Frame Relay environment, the congestion point may not be the interface itself, but it may be the VC because of the committed information rate (CIR). For real-time traffic (voice flows) to be transmitted in a timely manner, the data rate must not exceed the CIR or packets might be dropped causing voice quality issues. Frame Relay traffic shaping (FRTS) is configured on the interfaces to control the outbound traffic rate by preventing the router from exceeding the CIR. This means that fancy queueing such as class-based weighted fair queueing (CBWFQ), low latency queueing (LLQ), and weighted fair queueing (WFQ), can run on the VC to provide the quality of service (QoS) guarantees for the traffic.

Previously, RSVP reservations were not constrained by the CIR of the flow's outbound VC. As a result, oversubscription could occur when the sum of the RSVP traffic and other traffic exceeded the CIR.

The RSVP support for Frame Relay feature allows RSVP to work with per VC (data link connection identifier (DLCI)) queueing for voice-like flows. Traffic shaping must be enabled in a Frame Relay environment for accurate admission control of resources (bandwidth and queues) at the congestion point; that is, the VC itself. Specifically, RSVP can work with VCs defined at the interface and subinterface levels. There is no limit to the number of VCs that can be configured per interface or subinterface.

## SDLC SNRM Timer and Window Size Enhancements

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

The SDLC SNRM Timer and Window Size Enhancements feature introduces a new window size setting for SDLC configurations, and a new timeout setting for the SNRM frame. These enhancements change the operation of SDLC processing on a multidrop line.

### Window Size Setting

Prior to this feature, all SDLC addresses on the multidrop had the same window count. Now the window count can be configured on a Physical Unit (PU) or SDLC address level. This enhancement gives a controller a different window size than other devices on the interface, and allows devices attached to the multidrop to be sized individually.

### Timeout Setting for SNRM Frame

Cisco IOS software SDLC implementation currently utilizes a common response timer (T1) for all outstanding commands. Calculating the maximum frame size and line speed produces a minimum time of 3.5 seconds for receiving acknowledgments; thus, polling stations used for link activation utilize this 3.5-second timer. This is a problem on a multidrop, because stations that do not respond to the SNRM will have 3.5 seconds of downtime-waiting before the next station that is active is polled. This enhancement reduces the time to stations that are waiting idle, as opposed to those that are active.

## Set ATM CLP Bit

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

The Cell Lost Priority (CLP) bit in the ATM header of a cell provides a method of controlling the discarding of cells in a congested ATM environment. A CLP bit contains two settings: 0 or 1. Cells with a CLP bit setting of 1 are discarded before cells with a CLP bit setting of 0.

Before the introduction of the ATM CLP Setting feature, the CLP bit was automatically set to 0 when Cisco routers converted packets into ATM cells for ATM networks.

The ATM CLP Setting feature allows users to control the CLP bit setting on routers with the PA-A3 port adapter. The CLP bit is set on each packet individually, and the default CLP bit setting is 0. The application of the ATM CLP Setting feature changes the CLP bit setting to 1. Therefore, users have the option to leave each packet with the default CLP bit setting of 0 or to establish a new CLP bit setting of 1.

ATM CLP Setting is documented as part of the Class-Based Packet Marking feature.

## TN3270 Server Connectivity Enhancements

Platforms: Cisco 7200 series and Cisco 7500 series routers

The TN3270 Server Connectivity Enhancements feature, an enhancement to the existing TN3270 Server feature, provides the following new functions:

- Dynamic LU naming
- Inverse DNS nailing
- TN3270 Server security enhancements

## Traceroute Enhancement for MPLS

Platforms: Cisco 7200 series and Cisco 7500 series routers

The traceroute enhancements for MPLS feature introduces two new commands that enable you to manage the time to live (TTL) field in an MPLS header.

- The **mpls ip ttl-expiration pop** command lets you specify how a packet with an expired time to live (TTL) value is forwarded. You can specify that the packet be forwarded by the global IP routing table or by the packet's original label stack. The forwarding method is determined by the number of labels in the packet. You specify the number of labels as part of the command. If the packet contains the same or fewer labels than you specified, it is forwarded through the use of the global IP routing table. If the packet contains more labels than you specified, the packet is forwarded through the use of the original label stack.
- The **mpls ip propagate-ttl** command controls the generation of the time to live (TTL) field in the MPLS header when labels are first added to an IP packet. By default, this command is enabled, which means the TTL field is copied from the IP header. The command allows a traceroute command to show all the hops in the network.

Use the no form of the **mpls ip propagate-ttl** command to use a fixed TTL value (255) for the first label of the IP packet. This hides the structure of the MPLS network from a traceroute command. You can specify the types of packets to be hidden by using the forwarded and local arguments. Specifying **no mpls ip propagate-ttl forwarded** allows the structure of the MPLS network to be hidden from customers but not from the provider. This is the most common application of the command.

## Class Based Policer for the DiffServ AF PHB

Platforms: Cisco 7200 series

Traffic policing is used to control the rate of traffic flowing across an interface.

The Class Based Policer for the DiffServ AF PHB feature performs the following functions:

- Limits the input or output transmission rate of a class of traffic based on user-defined criteria
- Marks packets by setting the IP precedence value, the Quality of Service (QoS) group, or the differentiated services code point (DSCP) value

For additional information on the Traffic Policing feature, see the *Traffic Policing* feature module on Cisco.com and on the Documentation CD-ROM.

## Turbo Access Control Lists

Platforms: Cisco 7200 series routers

Access control lists (ACLs) are normally searched sequentially to find a matching rule, and ACLs are ordered specifically to take this factor into account. Because of the increasing needs and requirements for security filtering and packet classification, ACLs can expand to the point that searching the ACL adds a significant amount of time and memory when packets are being forwarded. Moreover, the time taken by the router to search the list is not always consistent, adding a variable latency to the packet forwarding. A high CPU load is necessary for searching an ACL with several entries.

The Turbo ACL feature compiles the ACLs into a set of lookup tables, while maintaining the first match requirements. Packet headers are used to access these tables in a small, fixed number of lookups, independently of the existing number of ACL entries. The benefits of this feature include:

- For ACLs larger than 3 entries, the CPU load required to match the packet to the pre-determined packet-matching rule is lessened. The CPU load is fixed, regardless of the size of the ACL, allowing for larger ACLs without incurring any CPU overhead penalties. The larger the ACL, the greater the benefit.
- The time taken to match the packet is fixed, so that latency of the packets are smaller (significantly in the case of large ACLs) and more importantly, consistent, allowing better network stability and more accurate transit times.

For additional information on the Turbo ACL feature, see the *Turbo Access Control Lists* feature module on Cisco.com and the Documentation CD-ROM.

## VIP-Based Distributed FRF.11/12

Platforms: Cisco 7500 series routers

The Voice Over Frame Relay using FRF.11 and FRF.12 capabilities currently available in Cisco IOS Release 12.1 T are now available, with some modifications, on VIP-enabled Cisco 7500 series routers. The new feature is called VIP-Based Distributed FRF.11 and FRF.12 (VIP-Based FRF.11 and FRF.12).

For additional information on VIP-Based FRF.11 and FRF.12, see the *Versatile Interface Processor-Based Distributed FRF.11 and FRF.12* feature module on Cisco.com and the Documentation CD-ROM.

## VIP-Based WFQ Support for RSVP

Platforms: Cisco 7500 series routers

In earlier software releases, Resource Reservation Protocol (RSVP) on Cisco 7500 series routers would leverage Route Switch Processor-based (RSP-based) weighted fair-queuing to guarantee bandwidth to RSVP flows.

RSVP now interoperates with distributed weighted fair-queuing (dWFQ), thus offloading the RSP of the overhead of the queueing function and improving RSVP scalability. RSVP support of dWFQ is transparent to the user.

## VPN Accelerator Card Enhancements

Platforms: Cisco 7100 series and Cisco 7200 series routers

The VPN Accelerator Card Enhancements feature displays the packet statistics of the VPN accelerator card and controller. It is available on the Cisco 7100 series router with the ISA and the ISM. It is available on the Cisco 7200 series router only if an ISA is installed.

The ISA is a single-width service adapter and the ISM is a single-width service module. Each provides high-performance, hardware-assisted tunneling and encryption services suitable for Virtual Private Network (VPN) remote access, site-to-site intranet, and extranet applications. In addition each provides platform scalability and security while working with all services necessary for successful VPN deployments—security, quality of service (QoS), firewall and intrusion detection, and service-level validation and management.

## New Hardware Features in Release 12.1(5)T

The following new hardware features are supported by the Cisco 7000 family for Cisco IOS Release 12.1(5)T:

### Cisco 7200-I/O-GE+E and Cisco 7200-I/O-2FE/E Input/Output Controllers

Platforms: Cisco 7200 VXR series routers

The Cisco 7200-I/O-GE+E is an Input/Output controller that provides one Gigabit Ethernet and one Ethernet port. It is equipped with a GBIC receptacle for 1000 megabits per second (Mbps) operation and an RJ-45 receptacle for 10 Mbps operation.

The Cisco 7200-I/O-2FE/E is an Input/Output controller that provides two autosensing Fast Ethernet ports and is equipped with two RJ-45 receptacles for 10/100 Mbps operation.

I/O controllers support the following features:

- Dual EIA/TIA-232 channels for local console and auxiliary ports
- NVRAM for storing the system configuration and environmental monitoring logs
- Two PC card slots that hold Flash Disks or Flash memory cards for storing the default Cisco IOS software image
- Flash memory for storing the boot helper image
- Two environmental sensors for monitoring the cooling air as it enters and leaves the chassis

### Dynamic Packet Transport OC-12c Port Adapter for 7200

Platforms: Cisco 7200 series and Cisco 7200 VXR series routers

The dual-width OC-12c Dynamic Packet Transport (DPT) port adapter is available on Cisco 7200 series routers and Cisco 7200 VXR series routers. The DPT is an OC-12c interface used in Cisco 7200 series and Cisco 7200 VXR routers to provide a shared IP-over-SONET capability.

The following benefits are offered by the DPT for the Cisco 7200 and Cisco 7200 VXR series routers:

- Accommodates large-scale network topology
- Applicable IEEE 802.3 standards
- Supports Intelligent Protection Switching (IPS)

## MIX-Enabled 2/4/8 Port Multichannel T1/E1 Port Adapter with CSU/DSU

Platforms: Cisco 7200 series routers

The Multiservice Interchange (MIX) port adapter adds time-division multiplexing (TDM) connection capabilities that enable you to combine types of traffic traveling through Cisco 7200 VXR series routers. On the Cisco 7200 VXR series router, MIX enables TDM connections between two ports on the same MIX-enabled port adapter.

MIX functions permit connection of TDM streams to support applications that are sensitive to time delay, such as voice and video, and provide customers the flexibility to manage this traffic through the router as traditional TDM connections or in a packet-based format. In addition, Extended Availability Drop and Insert (EADI) capabilities have been added, which allow MIX connections to stay up through a router reload.

The 2/4/8 Port Multichannel T1/E1 port adapters are now enabled with a Multiservice Interchange (MIX) card. The MIX card enables the connection of TDM traffic from any port on a MIX-enabled port adapter to any other port on the same MIX-enabled port adapter on the Cisco 7200 VXR platform.

The following port adapters are currently MIX-enabled:

- PA-MCX-2TE1
- PA-MCX-4TE1
- PA-MCX-8TE1

## Multiport T1/E1 ATM Port Adapters with Inverse Multiplexing over ATM

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

The inverse multiplexing over ATM (IMA) port adapter is a single-width port adapter that allows Cisco 7100 series, Cisco 7200 series, and Cisco 7500 series routers to support inverse multiplexing over ATM. These port adapters support WAN uplinks at speeds ranging from 1.544 Mbps to 12.288 Mbps for T1 connections and from 2.048 Mbps to 16.384 Mbps for E1 connections.

With the scalable Cisco ATM IMA solution, network designers and managers can deploy only the bandwidth they need, using multiple T1 or E1 connections instead of more expensive T3 or OC-3 lines to bridge LANs and ATM WAN applications. Enterprises and branch offices can aggregate traffic from multiple lower-bandwidth physical transmission media, such as T1 or E1 pipes, to transmit voice and data at high-bandwidth connection speeds.

## Network Services Engine

Platforms: Cisco 7200 series routers

The network services engine (NSE) is the latest processor engine for Cisco 7200 VXR routers. The NSE delivers wire rate OC-3 throughput while running concurrent high-touch WAN edge services. It is the first Cisco processing engine to offer integrated hardware acceleration increasing Cisco 7200 VXR series system performance by 50 to 300% for combined “high touch” edge services. NSE takes advantage of a new technology called Parallel eXpress Forwarding (PXF).



## NPE-400

Platforms: Cisco 7200 VXR routers

NPE-400 is a new version of network processing engine for Cisco 7200 VXR routers with the following enhancements:

- RM7000 microprocessor that operates at an internal clock speed of 350 MHz
- Up to 512 MB ECC SDRAM
- 100 MHz SysAD and memory bus speed
- 4 MB Layer 3 cache

The NPE-400 leverages technology from the NPE-225 and NSE-1 to provide a higher performance NPE card.

## OC-12 Dynamic Packet Transport Interface Processor

Platforms: Cisco 7500 Series Routers

The OC-12c Dynamic Packet Transport (DPT) Interface Processor is available on Cisco 7500 series routers. The DPT is an OC-12c interface that uses second-generation Versatile Interface Processor (VIP2) technology to provide a shared IP-over-SONET capability and it complies with IEEE 802.3 specifications for multicast and broadcast media. The DPTIP assembly consists of a VIP2 with a dual-width DPT interface processor permanently attached to it.

## One-Port Enhanced ESCON Channel Port Adapter

Platforms: Cisco 7200 series routers

The High Performance Enterprise Systems Connection (ESCON) port adapter provides a single channel interface for Cisco 7200-series routers. In some situations, this interface can eliminate the need for a separate front-end processor (FEP). The HP ESCON PA contains one ESCON I/O connector.

The HP ESCON PA is a high-speed port adapter. A Fast Ethernet port adapter is an example of another type of high-speed port adapter. A single Cisco 7200-series router can support up to three high-speed port adapters.

The HP ESCON PA provides a single channel attachment interface for connecting Cisco 7200 series routers to an ESCON director or to a mainframe channel.

A mainframe channel (referred to as a channel) is an intelligent processor that manages the protocol on the communications media and controls the data transfer to and from the main central processing unit (CPU) storage. Devices called input/output processors (IOPs) communicate between the host CPU and the channel. One IOP controls multiple channels. There is no relationship between the number of CPUs and the number of IOPs.

The channel relieves the mainframe CPU of direct communication with input/output (I/O) devices, which saves processing cycles and allows data processing and communications tasks to run concurrently. Channels use one or more channel paths as the links between mainframes and I/O devices. I/O devices are connected directly to control units, which provide the logical capabilities required to operate and control the I/O devices.

For more information see the *PA-4C-E 1-Port High-Performance ESCON Channel Port Adapter Installation and Configuration* guide.

## PA-GE Gigabit Ethernet Port Adapter

Platforms: Cisco 7200 series routers

The single port Gigabit Ethernet Port Adapter (PA-GE) provides a Gigabit Ethernet connection for the Cisco 7200 series router. This port adapter, which offers moderate performance, is suitable for campus, enterprise edge and wide-area network (WAN) aggregation applications. When used on the campus, the Cisco 7200 series router with the PA-GE connects the enterprise WAN to the Gigabit Ethernet campus backbone. At the enterprise edge, the PA-GE connects the WAN to the Gigabit Ethernet campus backbone. When the Cisco 7200 series router is used for WAN aggregation, the PA-GE provides intra-pop connectivity between the router and high-speed WAN core devices, such as the Cisco 12000 series router. The PA-GE may be inserted into any open port adapter slot on Cisco 7200VXR routers.

## PA-MC-T3+

Platforms: Cisco 7200 series and Cisco 7500 series routers

The PA-MC-2T3+ is a single-width port adapter that provides two T3 interface connections using BNC connectors. Each T3 interface can be independently configured to be either channelized or unchannelized. A channelized T3 provides 28 T1 lines multiplexed into the T3. Each T1 line can be configured into one or more serial interface data channels.

An unchannelized T3 provides a single serial interface data channel that may be configured to use all of the T3 bandwidth or a fractional portion of it. This mode is compatible with several vendors of fractional (subrate) DS3 data service units (DSUs).

The PA-MC-2T3+ has the following features and physical characteristics:

- Supports both channelized and unchannelized operations.
- Transmits and receives data bidirectionally at the T3 rate of 44.736 Mbps.
- Conforms to relevant specifications for DS3 (Digital Signal Level 3) circuits.
- Supports RFC 1406 and RFC 1407 (CISCO-RFC-1407-CAPABILITY.my). For RFC 1406, Cisco supports all tables except the FarEnd table.

For more information see the *PA-MC-2T3+ Multichannel T3 Port Adapter Installation and Configuration* guide.

## New Software Features in Release 12.1(3)T

The following new software features are supported by the Cisco 7000 family for Cisco IOS Release 12.1(3)T:

### Bridging Between IEEE 802.1Q VLANs

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

The Bridging Between IEEE 802.1Q VLANs feature provides the ability to connect a network of hosts over a simple bridging-access device to a remote access concentrator. This feature supports the following IEEE 802.1Q (dot1q) functionality:

- Integrated routing and bridging (IRB) supports connectivity for multiple VLANs using a Bridge Group Virtual Interface (BVI) to associate a bridge group.
- Transparent bridging (TB) supports connectivity for multiple VLANs bridged between dot1q interfaces and other interface encapsulations or other types of interface media.
- Per-VLAN Spanning Tree (PVST+) for IEEE 802.1Q trunks supports dot1q trunks to map multiple spanning trees to a single spanning tree.

This feature enables interoperability and compatibility between dot1q encapsulated interfaces and all supported interface medias, such as Inter-Switch Link (ISL) encapsulated interfaces. The packets on the dot1q link contain a standard Ethernet or Fast Ethernet frame and the VLAN information associated with that frame. To interoperate with existing Cisco routers, run spanning tree per-VLAN over ISL or PVST, where a single spanning tree caters to every VLAN in the domain, PVST+ runs spanning tree on a per VLAN basis, and a default VLAN 1 spanning tree (also called Common Spanning Tree) tunnels to the IEEE 802.1Q specific VLAN.

### CEF Support for IP Routing Between IEEE 802.1Q VLANs

Platforms: Cisco 7200 series and Cisco 7500 series routers

Beginning with this release, Cisco Express Forwarding (CEF) is supported on interfaces on which IEEE 802.1Q encapsulation has been enabled at the subinterface level. You no longer have to disable CEF operation on interfaces that are using IEEE 802.1Q encapsulation on VLAN subinterfaces.

### Circuit Interface Identification MIB

Platforms: Cisco 7500 series routers

The Circuit Interface Identification MIB feature adds support for a new Cisco enterprise MIB, used to assist in SNMP monitoring of circuit-based interfaces. The Circuit Interface MIB (CISCO-CIRCUIT-INTERFACE-MIB) provides a MIB object, which can be used to identify individual circuit-based interfaces (for example, interfaces using ATM or Frame-Relay). This user-specified identification is then returned when linkup and linkdown SNMP traps are generated for the interface.

The Circuit Interface MIB consists of a single table, with each row comprising a sequence of two objects: circuit interface description (cciDescr) and circuit interface status (cciStatus). The cciDescr object is used to identify circuits using a textual description of up to 255 characters specified by the user (note that MIB objects are modified using network management system applications, and cannot be configured using the Cisco IOS command-line interface). When the row is created by a user, a value is set for the cciDescr object. The table is indexed by ifIndex from the IF-MIB. The cciStatus is the RowStatus object for the rows in the table. The cciStatus object can be set to only two values by the user: createAndGo(4), which creates a new row, and destroy(6), which removes an existing row. If the

row is created successfully, the cciStatus is active(1). When creating a new row, set the cciDescr object along with the cciStatus in a single **snmp set pdu** command. If the row is already active, only the cciDescr object can be modified. The other option is to delete the row first by setting the cciStatus to destroy(6), and then recreate the row with a new value for cciDescr. When creating a new row, the ifIndex is validated first. If the ifIndex value is not valid, the row is not created and an error code is returned. Similarly, if, when an interface is deleted, there was a corresponding row in this table, that row is deleted automatically.

After an identifying description is created for an interface by a user, the description (the cciDescr object) is sent along with the other varbinds as part of linkup and linkdown trap notifications.

For further details, see the CISCO-CIRCUIT-INTERFACE-MIB.my file, available from the Cisco.com MIB site at <http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

## Class-Based Marking

Platforms: Cisco 7200 series routers

The Class-Based Packet Marking feature provides users with a user-friendly command-line interface for efficient packet marking by which users can differentiate packets by designating them different identifying values. The Class-Based Packet Marking feature allows users to perform the following tasks:

- Mark packets by setting the IP precedence bits or the IP differentiated services code point (DSCP) in the IP Type of Service (ToS) byte.
- Associate a local QoS group value with a packet.

After setting the IP precedence bits or the IP DSCP, a user can classify a packet based on the IP precedence bit or IP DSCP value. These classifications are then used to apply user-defined differentiated QoS services to the packet.

Associating a packet with a local QoS group allows users to associate a group ID with a packet. The group ID can be used to classify packets into QoS groups based on prefix, autonomous system, and community string.

A user can set up to 8 IP precedence markings, 64 IP DSCP markings, and 100 QoS group markings.

## Class-Based Shaping

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

Class-based traffic shaping allows you to control the traffic that leaves an interface in order to match its transmission to the speed of the remote, target interface and to ensure that the traffic conforms to policies contracted for it. Traffic adhering to a particular profile can be shaped to meet downstream requirements, thereby eliminating bottlenecks in topologies with data-rate mismatches.

Using the Class-Based Shaping feature, you can do the following:

- Configure Generic Traffic Shaping (GTS) on a traffic class
- Specify average-rate or peak-rate traffic shaping
- Configure class-based weighted fair queueing (CBWFQ) inside GTS
- Enable class-based shaping on any interface that supports GTS.

## Event MIB

Platforms: Cisco 7200 series and Cisco 7500 series routers

The Event MIB is an asynchronous notification mechanism standardized for use by network management systems using Simple Network Management Protocol (SNMP).

The Event MIB provides the ability to monitor the Cisco Management Information Base (MIB) objects on the local or remote system using SNMP and take simple action whenever a trigger condition is met. By allowing notifications based on events, the Network Management Server does not need to constantly poll managed devices to find out if something has changed.

Support of the Event MIB has been added to Cisco IOS software to work with existing network management systems and, when combined with the currently integrated Expression MIB support, provides a flexible and efficient way to monitor complex conditions on network devices. By allowing SNMP notifications to take place only when a specified condition occurs, Event MIB support reduces the load on affected devices, significantly improving the scalability of network management solutions.

## Expression MIB Support of Delta, Wildcarding, and Aggregation

Platforms: Cisco 7100 series and Cisco 7200 series routers

This feature adds support of the Delta, Wildcarding, and Aggregation features in the Distributed Management Expression MIB (EXPRESSION-MIB) to Cisco IOS software for use by SNMP.

The Delta function enables the Expression MIB to use Delta values of an object instead of absolute values when evaluating an expression. Delta is obtained by taking the difference between the current value of an object and its previous value.

The Wildcarding function of the Expression MIB allows evaluation of multiple instances of an object. This is useful in cases when an expression needs to be applied to all instances of an object. You do not need to individually specify all instances of an object in the expression. Rather, you only need to set the `expWildcardedObject` in `expObjectTable` to TRUE for the respective object.

Aggregation is performed using the sum function in the Expression MIB. The operand to the sum function must be a wildcarded object. The result of the sum function is the sum of values of all instances of the wildcarded object.

For a complete description of Expression MIB functionality, see the *Distributed Management Expression MIB* Internet-Draft document, available through the IETF at <http://www.ietf.org/ids.by.wg/disman.html>.

## Frame Relay ELMI Address Registration

Platforms: Cisco 7200 series and Cisco 7500 series routers

The Frame Relay ELMI Address Registration feature enables a network management system (NMS) to detect connectivity among the switches and routers in a network using the Enhanced Local Management Interface (ELMI) protocol. During ELMI version negotiation, neighboring devices exchange their management IP addresses and `ifIndex`. The NMS polls the devices to collect this connectivity information.

Before this feature was introduced, NMSs could detect only the topology of routers or the topology of switches. This feature enables the NMS to detect switch and router interconnection and create an end-to-end network topology map for network administrators.

The Cisco Frame Relay MIB has been enhanced to support the new ELMI information. The NMS uses the MIB to extract the IP address and `ifIndex` of devices neighboring the managed device.

## General Packet Radio Service Release 1.4

Platforms: Cisco 7200 series routers



### Note

General Packet Radio Service (GPRS) Release 1.4 is a specially licensed feature that is available only through a controlled image release in Cisco IOS Release 12.1(3)T. GPRS Release 1.4 is the recommended upgrade for both GPRS Release 1.2 (available in Cisco IOS Release 12.1(1)GA) and GPRS Release 1.3 (available in Cisco IOS Release 12.1(2)GB). For more information about acquiring GPRS Release 1.4, please contact your Cisco sales representative. Customer documentation for GPRS Release 1.4 is available on Cisco.com and the documentation CD-ROM.

General Packet Radio Service (GPRS) is defined and standardized by the European standards body ETSI. GPRS is an IP packet-based data service for GSM networks. The GPRS network essentially consists of two major elements, the serving GPRS support node (SGSN) and gateway GPRS support node (GGSN).

The GGSN is a wireless gateway that allows mobile cellular phone users to access the public data network (PDN) or specified private IP networks. User sessions are connected from a mobile station through a device called a Base Station Subsystem (BSS) and then to a Serving GPRS Service Node (SGSN).

The connection between the SGSN and the GGSN is enabled through a protocol called the GPRS Tunneling Protocol (GTP). Finally, the connection between the GGSN and the PDN is enabled through the Internet Protocol (IP).

In order to assign mobile user sessions an IP address, the GGSN uses the Dynamic Host Configuration Protocol (DHCP). To authorize and authenticate the remote users, the GGSN can use a RADIUS server. DHCP and RADIUS services can be specified for the global configuration, using GPRS DHCP and RADIUS commands, or for each access point configured for the GGSN.

## HSRP Support for ICMP Redirects

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

The HSRP Support for Internet Control Message Protocol (ICMP) Redirects feature enables Internet Control Message Protocol (ICMP) redirection on interfaces configured with the Hot Standby Router Protocol (HSRP).

When running HSRP, it is important to prevent hosts from discovering the interface (or real) MAC addresses of routers in the HSRP group. If a host is redirected by ICMP to the real MAC address of a router, and that router later fails, then packets from the host are lost. Previously, ICMP redirect messages were automatically disabled on interfaces configured with HSRP.

This feature now enables ICMP redirects on interfaces configured with HSRP. This functionality filters outgoing ICMP redirect messages through HSRP, where the next-hop IP address may be changed to an HSRP virtual IP address.

## HSRP Support for MPLS VPNs

Platforms: Cisco 7200 series and Cisco 7500 series routers

The HSRP support for Multiprotocol Label Switching (MPLS) VPNs feature enables ICMP redirection on interfaces configured with the Hot Standby Router Protocol (HSRP).

The Internet Control Message Protocol (ICMP) is a network layer Internet protocol that provides message packets to report errors and other information relevant to IP processing. ICMP provides many diagnostic functions and can send and redirect error packets to hosts.

HSRP provides network redundancy in a way that ensures that user traffic immediately and transparently recovers from first-hop failures in network edge devices and access circuits. By sharing an IP address and a MAC (Layer 2) address, two or more routers can act as a single virtual router to the hosts on a LAN. The members of the router group continually exchange status messages by detecting when a router goes down. This HSRP group consists of an active router and a standby router to replace the active router should it fail. The address of this HSRP group is referred to as the “virtual ip address.”

When running HSRP, it is important to prevent the host from discovering the primary MAC addresses in its standby group. If a host is redirected by ICMP to a standby group that later fails, the packets are lost. Previously, ICMP redirect messages were disabled on interfaces configured with HSRP. This was done to avoid the host from being directed away from the virtual IP address (the HSRP group address that provides redundancy) to the interface IP and MAC address of a single router. If this single router failed, redundancy was lost.

The HSRP Support for the ICMP Redirect Messages feature now enables ICMP redirects on interfaces configured with HSRP. This feature works by filtering outgoing ICMP redirect messages through HSRP, where the next-hop IP address is changed to an HSRP virtual IP address.

## Individual SNMP Trap Support

Platforms: Cisco 7200 series routers

The Individual SNMP Trap Support feature adds the ability to enable or disable SNMP system management notifications (traps) individually. SNMP traps that can be specified are authentication, linkup, linkdown, and coldstart. This feature expands the functionality of the **snmp-server enable traps snmp** command.

## MPLS Traffic Engineering and Enhancements

Platforms: Cisco 7200 series and Cisco 7500 series routers

Multiprotocol Label Switching (MPLS) traffic engineering software enables an MPLS backbone to replicate and expand upon the traffic engineering capabilities of Layer 2 ATM and Frame Relay networks. MPLS is an integration of Layer 2 and Layer 3 technologies. By making traditional Layer 2 features available to Layer 3, MPLS enables traffic engineering.

Traffic engineering is essential for service provider and Internet service provider (ISP) backbones. Such backbones must support a high use of transmission capacity, and the networks must be very resilient so that they can withstand link or node failures.

MPLS traffic engineering

- Enhances standard Interior Gateway Protocols (IGPs), such as IS-IS or OSPF, to automatically map packets onto the appropriate traffic flows
- Transports traffic flows across a network using MPLS forwarding

- Determines the routes for traffic flows across a network based on the resources the traffic flow requires and the resources available in the network
- Employs “constraint-based routing,” in which the path for a traffic flow is the shortest path that meets the resource requirements (constraints) of the traffic flow
- Recovers from link or node failures by adapting to the new constraints presented by the changed topology
- Transports packets using MPLS forwarding crossing a multihop label-switched path (LSP)

## PPP over ATM SVC

Platforms: Cisco 7200 series and Cisco 7500 series routers

As DSL deployment continues to grow, ATM PVC provisioning becomes extremely cumbersome. Network Access Providers (NAPs) must nail up each PVC between subscriber and NAP. Terminating point and quality of service of PVCs are predetermined and provisioned. With the PPP over ATM Switched Virtual Circuit (SVC) support feature you can choose services and the quality of those services based upon ATM address. When an end user initiates a connection to a service, an ATM SVC is set up with a desired destination using a configured ATM address. After the ATM SVC is set up, a PPP session is established on the ATM SVC. NAPs or Network Service Providers (NSPs) can use PPP over ATM to authenticate and authorize users to use its services.

End users can run PPP over ATM SVC on Win98/2000 on a PC with an asymmetric digital subscriber line (ADSL) Network Interface card (NIC) attached to a DSL or an ATM25 card attached to an ATM25 LAN connected to an ADSL remote office (ATU-R). PPP sessions may terminate at the NAP or tunneled to an NSP.

PPP over ATM SVC supports the following functions:

- SVCs using ATM Forum UNI 3.1 protocol
- Termination of ATM calls




---

**Note** This release does not support ATM dialout calls.

---

- International Code Designator (ICD) ATM End System Address (AESA) address format for SVCs
- Acceptance of offered ATM calls where the Called Party Address exactly matches the full ATM address assigned to a port
- Best-effort SVCs
- SVCs with asymmetric peak cell rate (PCR) values. Outgoing and incoming PCR values of SVCs can be different
- SVCs with a PCR granularity of no more than 83 CPS(32kbps)
- SVCs with an egress PCR range that includes 83 to 21,000 CPS(32kbps to 8Mbps)
- SVCs with an ingress PCR range that includes 83 to 2,000 CPS(32kbps to 768kbps)
- Compliance with requirements of RFC-2364 including Broadband Low Layer Information (B-LLI) negotiation of VC-multiplexed and Logical Link Control/Subnetwork Access Protocol (LLC/SNAP) encapsulation of PPP over ATM.
- ATM Adaptation Layer 5 (AAL5).



- SVCs with ingress and egress (AAL5) common part convergence sublayer (CPCS) service data unit (SDU) maximum size of at least 1506 bytes when supporting LLC/SNAP encapsulation, and 1502 bytes when supporting virtual circuit multiplexed encapsulation.
- Maximum Transmission Unit (MTU) negotiation as described in RFC-1626, “*Default IP MTU size for use over ATM AAL5*”.
- Shaping of each egress PVC and SVC (up to the maximum number supported for the interface) to no more than the PCR specified during connection establishment.
- Egress traffic shaping on a per-ATM service category basis.
- Link Control Protocol (LCP) configuration options
- Internet Protocol Control Protocol (IPCP) configuration options
- Network Control Program (NCP) types including IP.
- PPP idle timeout and absolute timeout.
- Forwarding Information Base (FIB) switching and fast-switching.
- RADIUS
- RADIUS attributes to identify the session-user as an SVC user. Attributes 30 and 31, (Called-Station-Id and Calling-Station-Id) identify Called Party Address and Calling Party Address of SVC calls. NAS Port Type identifies the SVC virtual path identifier (VPI)/virtual channel identifier (VCI) and the ATM interface.
- Same ATM address on multiple ports. This feature enables ATM switches to balance sessions across interfaces with same ATM address.
- Configuration of maximum number of SVCs of each ATM service category type.
- Configuration of maximum amount of equivalent bandwidth allowed to all SVCs. SVC calls are rejected when bandwidth taken exceeds specified maximum amount of allocated bandwidth.
- Configuration of maximum amount of equivalent bandwidth allowed for each ATM service category. SVC calls are rejected when bandwidth taken would exceed specified maximum amount of bandwidth allocated for the specified ATM service category, such as ubr and vbr-nrt.
- 2000 PPP over ATM SVC sessions on a Cisco 7200 series router with an NPE-200 with 128MB DRAM.

## RSVP Support for Low Latency Queuing

Platforms: Cisco 7200 series and Cisco 7500 series routers

RSVP is a network-control protocol that provides a means for reserving network resources—primarily bandwidth—to guarantee that applications transmitting end-to-end across networks achieve the desired quality of service (QoS).

RSVP enables real-time traffic (which includes voice flows) to reserve resources necessary for low latency and bandwidth guarantees.

Voice traffic has stringent delay and jitter requirements. It must have very low delay and minimal jitter per hop to avoid degradation of end-to-end QoS. This calls for an efficient queuing implementation that can service voice traffic at almost strict priority in order to minimize delay and jitter.

RSVP uses weighted fair queuing (WFQ) to provide fairness among flows and to assign a low weight to a packet to attain priority. However, the preferential treatment provided by RSVP is insufficient to minimize the jitter because of the nature of the queuing algorithm itself. As a result, the low latency and jitter requirements of voice flows might not be met in the prior implementation of RSVP and WFQ.

RSVP provides admission control. However, to provide the bandwidth and delay guarantees for voice traffic and get admission control, RSVP must work with LLQ. The RSVP support for LLQ feature allows RSVP to classify voice flows and queue them into the priority queue within the LLQ system while simultaneously providing reservations for nonvoice flows by getting a reserved queue.

## Secure Shell, Version 1 Integrated Client

Platforms: Cisco 7200 series and Cisco 7500 series routers

Secure Shell (SSH) is a protocol that provides a secure, remote connection to another router. There are currently two versions of SSH, available, SSH, Version 1 and SSH Version 2. Only SSH, Version 1 is implemented in Cisco IOS.

The Secure Shell, Version 1 Integrated Client feature is an application that runs on a reliable transport layer, such as TCP/IP, and provides strong authentication and encryption. The SSH client enables a Cisco router to make a secure, encrypted connection to another Cisco router or device running an SSH, Version 1 server. This connection provides functionality that is similar to an outbound Telnet connection except that the connection is encrypted. With authentication and encryption, the SSH client provides a secure communication over an insecure network.

The SSH client in Cisco IOS works with publicly and commercially available SSH servers. The SSH client supports DES (56-bit) and Triple DES (168-bit) encryption using random number generation.

The SSH client also supports user ID and password authentication using standard authentication methods: local authentication, RADIUS, and TACACS+.

The SSH, Version 1 Integrated Client feature uses the RSA algorithm to generate key pairs for authentication.

## SNMP Support for IOS vLAN Subinterfaces

Platforms: Cisco 7200 series and Cisco 7500 series routers

The SNMP support for IOS vLAN Subinterfaces feature provides MIB-2 interfaces sparse table support for Fast Ethernet subinterfaces. This enhancement is similar to the functionality supported in Frame Relay subinterfaces.

Sparse table support for the interfaces table on Fast Ethernet subinterfaces provides customers accustomed to Frame Relay subinterfaces the same functionality.

## Source Specific Multicast

Platforms: Cisco 7200 series and Cisco 7500 series routers

The Source Specific Multicast (SSM) feature is an extension of IP multicast, where datagram traffic is forwarded to receivers from only those multicast sources to which the receivers have explicitly joined. When SSM is used, only source-specific multicast distribution trees (no shared trees) are created.

Source specific multicast (SSM) is a datagram delivery model that best supports one-to-many applications, also known as broadcast applications. SSM is the core networking technology for the implementation of Cisco solutions targeted for audio and video broadcast application environments.

## Transparent Common Channel Signaling

Platforms: Cisco 7200 series and Cisco 7500 series routers

Transparent CCS allows the connection of two PBXs with digital interfaces that use a proprietary or unsupported CCS protocol without the need for interpretation of CCS signaling for call processing. T1/E1 traffic 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 PBXs are not routed, but follow a preconfigured route to the destination.

## T.38 Fax Relay for Voice over IP H.323

Platforms: Cisco 7200 series routers

The T.38 Fax Relay for VoIP H.323 feature provides standards-based Fax Relay protocol support on Cisco2600 series, Cisco3600 series, and CiscoMC3810 series multiservice gateways. The Cisco proprietary Fax Relay solution is sometimes not an ideal solution for Enterprise and Service Provider customers who have implemented a mixed vendor network. Because the T.38 Fax Relay protocol is standards based, Cisco gateways and gatekeepers will now be able to interoperate with third-party T.38-enabled gateways and gatekeepers in a mixed vendor network where real time Fax Relay capabilities are required.

## Virtual Switch Interface Master MIB

Platforms: Cisco 7200 series and Cisco 7500 series routers

The Virtual Switch Interface Master MIB provides a standardized vehicle for monitoring the operation of the VSI protocol within a Label Switch Controller (LSC). It also displays the results of the protocol operations. Specifically, with the VSI Master MIB you can monitor:

- Connections between an LSC and the switch it controls
- The status of the interfaces in the switch
- Virtual circuits (VCs) that are maintained across the interfaces

With the VSI Master MIB you can enlist Simple Network Management Protocol (SNMP) to monitor the status of the VSI protocol and the results of its operations.

This MIB is primarily oriented toward management of Multiprotocol Label Switching (MPLS) systems. As such, the MIB resides in routers that are also LSCs. These are routers that are VSI capable, and whose network control application is MPLS.

## WCCP Redirection on Inbound Interfaces

Platforms: Cisco 7200 series and Cisco 7500 series routers

The WCCP Redirection on Inbound Interfaces feature adds support to Cisco IOS software for the redirection of Web Cache Coordination Protocol Version 2 (WCCPv2) traffic on inbound interfaces. Prior to this release, WCCP was implemented as an output feature only, with packets classified by WCCP after a routing table lookup. With Cisco IOS release 12.1(3)T, you can now configure an interface for inbound redirection using CEF, dCEF, fast forwarding, and process forwarding paths. WCCP redirection on inbound interfaces avoids the processing overhead created by CEF on outbound interfaces.

## New Hardware Features in Release 12.1(3)T

The following new hardware features are supported by the Cisco 7000 family for Cisco IOS Release 12.1(3)T:

### PA-VXB and PA-VXC

Platforms: Cisco 7200 series and Cisco 7500 series routers

The PA-VXB and the PA-VXC are multichannel packet voice port adapters that allow Cisco 7200 series, Cisco 7200 VXR, and Cisco 7500 series routers to become dedicated packet voice hubs or packet voice gateways that connect to both private branch exchanges (PBXs) and the Public Switched Telephone Network (PSTN). This allows packet voice and packet fax calls to be placed over the wide-area network (WAN) and sent through the gateway into the traditional circuit-switched voice infrastructure.

The PA-VXB and the PA-VXC are single-width port adapters with two universal ports that are configurable for either T1 or E1 connection. The PA-VXB contains 12 high-performance digital signal processors (DSPs) that support up to 48 medium-complexity or 24 high-complexity channels of compressed voice. The PA-VXC contains 30 high-performance DSPs that support up to 60 medium-complexity or 120 high-complexity channels of compressed voice.

In Voice over IP, the DSP segments the voice signal into frames, which are then coupled in groups of two and stored in voice packets. These voice packets are transported using IP in compliance with ITU-T specification H.323. Because Voice over IP is a delay-sensitive application, you must have a well-engineered network end-to-end to use it successfully. Fine-tuning your network to adequately support Voice over IP involves a series of protocols and features geared toward quality of service (QoS). Traffic shaping considerations must be taken into account to ensure the reliability of the voice connection.

## New Software Features in Release 12.1(2)T

The following new software features are supported by the Cisco 7000 family for Cisco IOS Release 12.1(2)T:

### AAA Server Group Deadtimer

Platforms: Cisco 7200 series routers

The AAA Server Group Deadtimer feature allows each authentication, authorization, and accounting (AAA) server to be fully configured in the server group. Thus, you can direct AAA traffic to separate groups of servers that have different operational characteristics.

With the introduction of this feature, deadline has been added as a new attribute to the server group structure. In addition, a separate timer has been attached to each server host in every server group. Therefore, when a server is found to be unresponsive after numerous retransmissions and time-outs, the server is assumed to be dead. The timers attached to each server host in all server groups are triggered. In essence, the timers are checked and subsequent requests to a server (once it is assumed dead) are directed to alternate timers, if configured. When the network access server receives a reply from the server, it checks and stops all configured timers (if running) for that server in all server groups.

If the timer has expired, only the server to which the timer is attached is assumed to be alive. This becomes the only server that can be tried for later AAA requests using the server groups to which the timer belongs.

## Bidirectional PIM

Platforms: Cisco 7200 series and Cisco 7500 series routers

Bidirectional PIM (bidir-PIM) is a variant of the Protocol Independent Multicast (PIM) suite of routing protocols for IP multicast. Bidir-PIM is derived from the mechanisms of Protocol Independent Multicast sparse mode (PIM SM) and shares many of its protocol elements. In short, bidir-PIM is PIM SM with shared tree, but no shortest path tree operations. Bidir-PIM also has unconditional forwarding of source traffic toward the Route Processor (RP) upstream on the shared tree, but no registering process for sources as in PIM SM. These modifications are necessary and sufficient to allow forwarding of traffic in all routers solely based on the (\*, G) multicast routing entries. This feature eliminates any source-specific state and allows scaling capability to an arbitrary number of sources.

## Configurable Timers in H.225

Platforms: Cisco 7200 series routers

With the Configurable Timers in H.225 feature you can configure the H.255 TCP connection timeout value for all out-going call attempts (on a per VoIP dial-peer basis).

In previous releases of the Cisco IOS software, the call attempt timeout was 15 seconds and could not be changed. In some cases, however, users might need a shorter timeout value to facilitate a faster failover. In other cases, users might need a greater timeout value.

The Configurable Timers in H.225 feature addresses those needs by providing the ability to override the default of 15 seconds and to configure the timeout value.

## Ecosystem Gatekeeper Interoperability Enhancements, Phase 2

Platforms: Cisco 7200 series routers

The Ecosystem Gatekeeper Interoperability Enhancements, Phase 2 feature supplements the existing support for alternate gatekeepers and adds support for the alternate gatekeeper field (altGKInfo) to the admission rejection (ARJ). This allows a gateway to move between gatekeepers during the admission request (ARQ) phase.

## Frame Relay PVC Interface Priority Queueing

Platforms: Cisco 7200 series and Cisco 7500 series routers

The Frame Relay PVC Interface Priority Queueing (FR PIPQ) feature provides an interface-level priority queueing scheme in which prioritization is based on destination PVC rather than packet contents. For example, with FR PIPQ you can configure a PVC transporting voice traffic to have absolute priority over a PVC transporting signalling traffic, and a PVC transporting signalling traffic to have absolute priority over a PVC transporting data.

FR PIPQ provides four levels of priority: high, medium, normal, and low. The Frame Relay packet is examined at the interface for the data-link connection identifier (DLCI) value. The packet is then sent to the correct priority queue based on the priority level configured for that DLCI.

## Frame Relay Switching Enhancements

Platforms: Cisco 7200 series and Cisco 7500 series routers

The Frame Relay Switching Enhancements feature enables a router in a Frame Relay network to be used as a Frame Relay switch. This feature provides the following functionality:

### Traffic Shaping on Switched PVCs

You can now configure Frame Relay traffic shaping on switched permanent virtual connections (PVCs). By applying traffic shaping to switched PVCs, you enable a router to be used as a Frame Relay port concentrator in front of a Frame Relay switch. The Frame Relay switch shapes the concentrated traffic before sending it into the network.

### Frame Relay Switching over ISDN B-Channels

The Frame Relay Switching Enhancements feature enables you to transport Frame Relay data over ISDN so that small offices can be hubbed out of larger offices rather than connecting them directly to the core network. The hub router acts as a Frame Relay switch, switching between ISDN and serial interfaces.

### Traffic Policing on UNI DCE

The Frame Relay Switching Enhancements feature brings traffic policing functionality to user to network interface data communications equipment (UNI DCEs) in Frame Relay networks. When enabled on the interface, policing prevents traffic congestion by discarding or setting the discard eligible (DE) bit on packets that exceed specified traffic parameters.

### Congestion Management on Switched PVCs

The Frame Relay Switching Enhancements feature enables a router in a Frame Relay network to manage outgoing traffic congestion on switched PVCs. When Frame Relay congestion management is enabled, the router manages congestion by setting BECN and FECN bits on packets, and by discarding packets that are marked with the DE bit and that exceed a specified level of congestion.

## Gatekeeper-to-Gatekeeper Redundancy and Load-Sharing

Platforms: Cisco 7200 series routers

The Gatekeeper to Gatekeeper Redundancy and Load-Sharing feature expands the capability that is provided by the Redundant H.323 Zone Support feature. With the Redundant H.323 Zone Support feature, the location requests (LRQs) are sent simultaneously (in a “blast” fashion) to all of the gatekeepers in the list. The gateway registers with the gatekeeper that responds first. Then, if that gatekeeper becomes unavailable, the gateway registers with another gatekeeper from the list.

The Gatekeeper to Gatekeeper Redundancy and Load-Sharing Mechanism feature enhances this capability so that you can choose whether the LRQs are sent simultaneously or sequentially (one-at-a-time) to the remote gatekeepers in the list. If the LRQs are sent sequentially, a *delay* is inserted after the first LRQ and before the next LRQ is sent. This delay allows the first gatekeeper to respond before the LRQ is sent to the next gatekeeper. The order in which LRQs are sent to the gatekeepers is based on the order in which the gatekeepers are listed (using either the **zone prefix** command or the **gw-type-prefix** command).

## H.323 Support for Virtual Interfaces

Platforms: Cisco 7200 series routers

With the H.323 Support for Virtual Interfaces feature, you can configure the IP address of the gateway, so that the IP address included in the H.323 packet is deterministic and consistently indicates the same address for the source.

In previous releases of the Cisco IOS software, the source address included in the H.323 packet could vary depending on the protocol (RAS, H.225, H.245, or RTP). This makes it difficult to configure firewall applications to work with H.323 messages.

The H.323 Support for Virtual Interfaces feature addresses that difficulty providing the capability to explicitly configure an IP address to be used for all protocols.

## Low Latency Queueing for Frame Relay

Platforms: Cisco 7200 series routers

Low Latency Queueing for Frame Relay is a feature that provides a strict priority queue (PQ) for voice traffic and weighted fair queues for other classes of traffic.

Using this feature you can configure classes of traffic according to protocol, interface, or access lists, and then define policy maps to establish how the classes are handled in the PQ and in weighted fair queues.

Queues are set up on a per-permanent virtual circuit (PVC) basis: each PVC has a PQ and an assigned number of fair queues. The fair queues are assigned weights proportional to the bandwidth requirements of each class; a class requiring twice the bandwidth of another will have half the weight.

The PQ is policed to ensure that the fair queues are not starved of bandwidth. When you configure the PQ, you specify in kbps the maximum amount of bandwidth available to that queue. Packets that exceed that maximum are dropped.

## Minimum Masking Ability for NetFlow Router-Based Aggregation Schemes

Platforms: Cisco 7200 series and Cisco 7500 series routers

With the Minimum Masking Ability for NetFlow Router-Based Aggregation Schemes feature you can set a minimum mask size. The IP address that is added to the aggregation cache is added to the maximum user-entered mask and the routing table mask.

To enable this feature on a Source Prefix or a Destination Prefix, or both, configure the desired Minimum Mask value using the NetFlow aggregation commands. The Minimum Mask value used by the router selects the granularity of the NetFlow data that will be collected.

The mask values range from 1 to 32. For coarse NetFlow collection granularity select a small Minimum Mask value. For fine NetFlow collection granularity select a large Minimum Mask value.

## OSPF Flooding Reduction

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

The explosive growth of the Internet has placed the focus on the scalability of Interior Gateway Protocols such as Open Shortest Path First (OSPF). The networks using OSPF are becoming larger every day and will continue to expand to accommodate the demand to connect to the Internet.

Internet service providers and customers with large networks have regularly complained that OSPF has a traffic overhead, even when the network topology is stable.

By design, OSPF requires link-state advertisements (LSAs) to be refreshed as they expire after 3600 seconds. Some implementations have tried to improve the flooding by reducing the frequency to refresh from 30 minutes to approximately 50 minutes. This solution reduces the amount of refresh traffic but requires at least one refresh before the LSA expires.

The OSPF Flooding Reduction feature works by reducing unnecessary refreshing and flooding of already known and unchanged information. To achieve this reduction, the LSAs are now flooded with the higher bit set, thus making them DoNotAge LSAs.

## PRI QSIG on the Cisco 7200

Platforms: Cisco 7200 series routers

QSIG protocol support allows Cisco voice switching services to connect PBXs, key systems, and central office switches that communicate by using the QSIG protocol, which is becoming the standard for PBX interoperability in Europe and North America. QSIG is a variant of ISDN D-channel signaling. With QSIG, Cisco networks emulate the functionality of the public-switched telephone network (PSTN), and QSIG signaling messages allow the dynamic establishment of voice connections across a Cisco WAN to a peer router, which can then transport the signaling and voice packets to a second private integrated services network exchange (PINX). In addition, QSIG support can enable a toll-bypass application.

## Virtual Profile CEF Switched

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

Using the Virtual Profile CEF Switched feature you can apply a per-user level configuration onto an Async and ISDN B-channel interface. VP CEF previously supported process switching and low-end system fast switching.

VP CEF switching provides improved performance by using Forwarding Information Base (FIB) to look up a route for a forwarding packet. FIB look-ups are superior to the cache tables used in fast switching because they are populated by routing topology rather than traffic and use the optimal switching decision.

VP CEF switching enables you to use VP in other new technologies that requires CEF switching, such as MPLS/BGP VPN, and dCEF with ISDN interfaces.



## Voice Over Frame Relay Configuration Enhancements

Platforms: Cisco 7200 series routers

Voice over Frame Relay functionality has been updated in this release, so that configuration on all supported platforms is nearly identical. In Cisco IOS Release 12.0(4)T, when support for Voice over Frame Relay using FRF.11 and FRF.12 was introduced, configuration procedures were different depending on the router platform used.

Some commands introduced in earlier Cisco IOS releases have been removed or modified. Refer to the *“Voice over Frame Relay Using FRF.11 and FRF.12 Configuration Updates”* feature module for a description of the configuration procedures effective in this release.

This feature provides consistency for configuration requirements across the hardware models that support Voice over Frame Relay: the Cisco 2600 and 3600 series routers, the Cisco 7200 series routers, and the Cisco MC3810 multiservice access concentrator. In previous releases, configuration procedures on the Cisco MC3810 were different from those on other routers.

## New Hardware Features in Release 12.1(1)T

The following new hardware features are supported by the Cisco 7000 family for Cisco IOS Release 12.1(1)T:

### Two-Port Moderate-Capacity T1 and E1 Digital Voice Port Adapter

Platforms: Cisco 7200 series routers

Cisco digital voice port adapters for the Cisco 7200 series routers provide large-scale voice and fax termination for PBXs, and the Public Switched Telephone Network (PSTN) using Voice over IP (VoIP) or Voice over Frame Relay (VoFR).

The digital voice port adapter is a highly integrated solution offering a leap forward in voice-channel density and application flexibility. This single-width port adapter incorporates two universal ports that can be configured for either T1 or E1 connections with high-performance digital signal processors that support up to 48 channels of compressed voice. Integrated channel service units/digital service units (CSU/DSU) echo cancellation, and digital signal level 0 (DS-0) drop and insert functionality eliminate the need for external line-termination devices and multiplexers, simplifying network design and management.

## New Software Features in Release 12.1(1)T

The following new software features are supported by the Cisco 7000 family for Cisco IOS Release 12.1(1)T:

### AAA Broadcast Accounting

Platforms: Cisco 7200 series routers

The AAA Broadcast Accounting feature allows accounting information to be sent to multiple authentication, authorization, and accounting (AAA) servers at the same time; that is, accounting information can be broadcast to one or more AAA servers simultaneously. This functionality allows service providers to send accounting information to their own private AAA servers and to the AAA servers of their end customers. It also provides redundant billing information for voice applications.

With the introduction of this feature, broadcasting is now allowed among groups of servers. The server groups can be either RADIUS or TACACS+. And each server group can define its backup servers for failover independently of other groups. (Failover is a process that may occur when more than one server has been defined within a server group. Failover refers to the following process: information is sent to the first server in a server group; if the first server is unavailable, the information is sent to the next server in the server group. This process continues until the information is successfully received by one of the servers within the server group or until the list of available servers within the server group is exhausted.

Thus, service providers and their end customers can use different protocols (RADIUS or TACACS+) for the accounting server. Service providers and their end customers can also specify their backup servers independently. As for voice applications, redundant accounting information can be managed independently through a separate group with its own failover sequence.

## Answer Supervision Reporting

Platforms: Cisco 7200 series routers

The Answer Supervision Reporting feature is an enhancement to the information request (IRR) Registration, Admission, and Status (RAS) protocol message that enables Gatekeepers to maintain call accounting information by reporting the call connection time of connected calls to the Gatekeeper.

In H.323 configurations, direct call-routed signaling is utilized by the endpoint (gateway). Gatekeepers do not have real-time knowledge or control over the state of a call and are dependent on the endpoints to provide them the necessary real-time information, such as the call connect time, call termination time, and call termination reason.

When a call ends, the gateway sends a Disengage Request (DRQ) message with the BillingInformationToken (which contains the duration of the call) to the Gatekeeper. However, if the Gatekeeper does not receive the DRQ message for some reason, the Gatekeeper does not receive the information about call start or duration, and the accounting information is no maintained accurately.

The Answer Supervision Reporting feature addresses the need to report the call connection time to the Gatekeeper upon call connection and at periodic intervals thereafter. The Answer Supervision Reporting feature adds a proprietary Cisco parameter, the call connection time parameter, to the perCallInfo parameter in the nonStandardData field, which is located in the IRR message. When a CONNECT message is received, the originating gateway sends the unsolicited IRR message to its Gatekeeper. On sending a CONNECT message, the terminating gateway sends the unsolicited IRR message to its Gatekeeper. If the admission confirmation message has a nonzero value for the IRRfrequency parameter, the gateway sends the unsolicited IRR message to its Gatekeeper at periodic intervals, which are determined by the value in the IRRfrequency parameter.

With the exception of containing the call connection time in the perCallInfo parameter, the IRR message and its functionality remains the same.

## Cisco H.323, Version 2, Phase 2

Platforms: Cisco 7200 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.

Cisco H.323 Version 2, Phase 2 adds the following benefits to Cisco H.323 gatekeepers, gateways, and proxies:

- H.323 Version 2 Fast Connect enables endpoints to establish media channels for audio exchange without waiting for a separate H.245 connection to be opened.
- H.245 tunneling enables H.245 messages to be encapsulated within Q.931 messages using H.225 (using Fast Connect) without the use of a separate H.245 TCP connection.
- H.450.2 Call Transfer (without consultation) and H.450.3 Call Deflection provide a limited subset of features to support Internet call waiting.
- H.235 security allows only duly authorized and authenticated gateways to access Gatekeeper resources.
- Translation of Foreign Exchange Station (FXS) hookflash to H.245 user input along with the previously suggested translation of H.245 user input to Foreign Exchange Office (FXO) hookflash provides end-to-end hookflash relay in FXS-to-FXO configurations.
- Gatekeeper Transaction Message Protocol (GKTMP) for the Cisco Gatekeeper with a corresponding user API for the UNIX environment, allows a third party to develop elements to control and utilize a Gatekeeper for applications beyond what is directly supported in Cisco IOS Release 12.1(1)T.
- Cisco Gatekeeper supports the Gatekeeper MIB, which allows SNMP management.
- Gateway support for the Alternate Endpoint field in Advanced Communications Function (ACF) enables third-party gatekeepers to provide more robust call establishment.
- Gateway support for network-based billing number on a per-interface basis enables third-party gatekeepers to obtain per-call interface usage information for billing or other purposes.
- Gateway support for the voice-port description enables third-party gatekeepers to obtain customer-specific, per-call interface usage information for billing or other purposes.

## COPS for RSVP

Platforms: Cisco 7200 series and Cisco 7500 series routers

Common Open Policy Service (COPS) is a protocol for communicating network traffic policy information to network devices. Resource Reservation Protocol (RSVP) is a means for reserving network resources—primarily bandwidth—to guarantee that applications transmitting end-to-end across the Internet will perform at the desired speed and quality. Combined, COPS with RSVP gives network managers centralized monitoring and control of RSVP, including the ability to:

- Ensure adequate bandwidth and jitter and delay bounds for time-sensitive traffic such as voice transmission
- Ensure adequate bandwidth for multimedia applications such as video conferencing and distance learning
- Prevent bandwidth-hungry applications from delaying top-priority flows or harming the performance of other applications customarily run over the same network

## Ecosystem Gatekeeper Interoperability Enhancements

Platforms: Cisco 7200 series routers

The Ecosystem Gatekeeper Interoperability Enhancements feature supplements the existing support for alternate gatekeepers and adds support for the alternate gatekeeper field (altGKInfo) to the gatekeeper rejection (GRJ) and registration rejection (RRJ) messages. This allows a gateway to move between gatekeepers during the gatekeeper request (GRQ) and registration request (RRQ) phases.

The altGKInfo consists of two subfields: the alternateGatekeeper and the altGKisPermanent flag. The alternateGatekeeper is the list of alternate gatekeepers. The altGKisPermanent flag indicates whether the gatekeepers in the associated alternateGatekeeper field are permanent or temporary.

If the current state of altGKisPermanent flag is true, then the new altGKInfo of any registration, admission, and status (RAS) messages received from one of the alternate gatekeepers is accepted, and the new list replaces the existing list.

If the current state of altGKisPermanent flag is false, then the altGKInfo of any RAS messages received from one of the alternate gatekeepers is ignored.

If the current permanent gatekeeper becomes nonresponsive and the altGKisPermanent flag is set to false, then the gateway sets the internal state of the altGKisPermanent flag to true. This setting enables the gateway to accept the alternate gatekeeper list from one of the gatekeepers in the existing alternate gatekeeper list.

The handling of the altGKInfo field varies depending on whether it is included in a GRJ or an RRJ message.

## Gateway-to-Gatekeeper Billing Redundancy

Platforms: Cisco 7200 series routers

The Gateway-to-Gatekeeper Billing Redundancy feature enhances the accounting capabilities of the Cisco H.323 Gateway and provides support for Vocaltec Gatekeepers. The Gateway-to-Gatekeeper Billing Redundancy feature provides redundant billing information to an alternate gatekeeper if the primary gatekeeper to which a gateway is registered becomes unavailable.

During the process of establishing a call, the primary gatekeeper sends an admission confirmation (ACF) message to the registered gateway. The ACF message includes the user billing information and an access token. To provide the billing information to an alternate gatekeeper if the primary gatekeeper is unavailable when the call session ends, the access token information sent in the ACF message is now also included in the disengage request (DRQ) message that is sent to the alternate gatekeeper.

This feature enables the alternate gatekeeper to obtain the billing information required to successfully complete the transaction.

## H.323 Version 2 Support

Platforms: Cisco 7200 series routers

Cisco H.323 Version 2 Phase 2 upgrades Cisco IOS software by adding the following optional features 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.
- H.245 Tunneling of DTMF Relay in conjunction with Fast Connect—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.450.2 Call Transfer--Call Transfer allows an H.323 endpoint to redirect an answered call to another H.323 endpoint. CiscoGateways support H.450.2 Call Transfer as the transferred and transferred-to party.
- 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.
- Translation of FXS 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.
- 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. In addition it will provide for the protection of specific messages related to OSP (Open Settlement Protocol) and other messages as required via encryption tokens.
- Gatekeeper Transaction Message Protocol (GKTMP) and RAS Messages--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.
- Gatekeeper and 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.
- Gatekeeper C Code Generic API for GKTMP in a Unix Environment--This API allows 3rd party applications running in a Unix host to send and receive GKTMP messages to a CiscoGatekeeper. This API may be used to develop back-end services such as authentication, billing and address translation.
- Gateway Support for 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.

## IKE Extended Authentication

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

IKE Extended Authentication (XAUTH) is a draft RFC developed by the Internet Engineering TaskForce (IETF) based on the Internet Key Exchange (IKE) protocol. XAUTH allows all Cisco IOS authentication methods, including those based on RADIUS or TACACS+ servers, to perform both user and device authentication for remote users and clients.

The XAUTH feature is an extension to the IKE feature, and does not replace IKE authentication.

## ISDN Network Side for PRI for ETSI Net5 PRI

Platforms: Cisco 7200 series and Cisco 7500 series routers

The ISDN Network Side PRI feature enables Cisco IOS to replicate the public switched network interface to a PBX that is compatible with the ETSI Net5 switch type.

Routers and PBXs are both traditionally customer premises equipment (CPE) with respect to the public switched network interfaces. For Voice over IP (VoIP) applications, it is desirable to interface access servers to PBXs with the access server representing the public switched network.

Enterprise organizations use the current VoIP features with Cisco products as a method to reduce long distance costs for phone calls within and outside of their organizations. However, there are times that a call cannot go over VoIP and the call needs to be placed using the public switched telephone network (PSTN). The customer then must have two devices connected to a PBX so that some calls can be placed using VoIP and some calls can be placed over the PSTN. By contrast, with this feature, Cisco access servers can connect directly to user-side CPE devices such as PBXs. Voice calls and data calls can be placed without requiring two different devices to be connected to the PBXs.

With this feature, the access server can provide a standard ISDN PRI network-side interface to the PBXs and can mimic the behavior of legacy phone switches. To a PBX, the access server functions as a Net5 PRI switch. No change in PBX capability or behavior is required.

## PPPoE on ATM

Platforms: Cisco 7200 series and Cisco 7500 series routers

The Point-to-Point Protocol over Ethernet (PPPoE) on ATM feature provides the ability to connect a network of hosts over a simple bridging-access device to a remote access concentrator. With this model, each host utilizes its own PPPoE stack and the user is presented with a familiar user interface. Access control, billing and type of service can be handled on a per-user, rather than a per-site, basis. Before a point-to-point connection over Ethernet can be provided, each PPP session must learn the Ethernet address of the remote peer and establish a unique session identifier. A unique session identifier is provided by the PPPoE Discovery Stage Protocol.

## PGM Host

Platforms: Cisco 7200 series and Cisco 7500 series routers

Pragmatic General Multicast (PGM) is a reliable multicast transport protocol for multicast applications that require reliable, ordered, duplicate-free multicast data delivery from multiple sources to multiple receivers. PGM guarantees that a receiver in a multicast group either receives all data packets from transmissions and retransmissions, or detects unrecoverable data packet loss. PGM is offered as a

solution for multicast applications with basic reliability requirements. PGM has two main parts: a host element (also referred to as the transport layer of the PGM protocol) and a network element (also referred to as the network layer of the PGM protocol).

The transport layer of the PGM protocol consists of two main parts: a source part and a receiver part. The transport layer defines how multicast applications send and receive reliable, ordered, duplicate-free multicast data from multiple sources to multiple receivers. The PGM Host feature is the Cisco implementation of the transport layer of the PGM protocol.

The network layer of the PGM protocol defines how intermediate network devices (such as routers and switches) handle PGM transport data as the data flows through a network. The PGM Router Assist feature is the Cisco implementation of the network layer of the PGM protocol. Refer to the “IP Multicast” section of the *Cisco IOS IP and IP Routing Configuration Guide* for information about the PGM Router Assist feature.

## Service Assurance Agent Enhancement

Platforms: Cisco 7200 series and Cisco 7500 series routers

The Service Assurance (SA) Agent is both an enhancement to and a new name for the Response Time Reporter (RTR) feature that was introduced in Cisco IOS release 11.2. Using this feature you can monitor network performance between a Cisco router and a remote device (which can be another Cisco router, an IP host, or a mainframe host, by measuring key Service Level Agreement (SLA) metrics such as response time, network resources, availability, jitter, connect time, packet loss, and application performance). You can perform troubleshooting, problem analysis, and notification based on the statistics collected by the SA Agent.

The SA Agent Enhancement feature introduces new performance measurement operations and enhancements to assist in the measurement of SLAs. With Cisco IOS release 12.1(1)T, the SA Agent provides new capabilities so that you can:

- Measure FTP file download response time using the new FTP operation
- Monitor one-way latency reporting through enhancements to the Jitter operation
- Configure a new option for the DHCP operation
- Manually enable a responder port
- Verify data for the UDPEcho operation
- Configure new options for the **rtr schedule** command
- Restart an operation

## SSH Version 1 Support for T Train

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

Secure Shell (SSH) is a protocol that provides a secure, remote connection to a router. There are currently two versions of SSH available, SSH Version 1 and SSH Version 2. Only SSH Version 1 is implemented in Cisco IOS.

The SSH server feature enables an SSH client to make a secure, encrypted connection to a Cisco router. This connection provides functionality that is similar to an inbound Telnet connection. The SSH server in Cisco IOS works with publicly and commercially available SSH clients.

## Wildcard Pre-Shared Key Enhancement

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

A wildcard pre-shared key allows a group of remote users with the same level of authentication to share an IKE pre-shared key. The remote peer pre-shared key must match the local peer pre-shared key for IKE authentication to occur. The term “wildcard” means that any remote peer with the pre-shared key can access the local peer, regardless of the remote peer IP address assignment. The term “pre-shared key” is a shared secret key exchanged during IKE negotiation.

A wildcard pre-shared key is usually distributed through a secure out-of-band channel. In a remote peer-to-local-peer scenario, any remote peer with the IKE pre-shared key configured can establish IKE security associations with the local peer.

The Wildcard Pre-shared Key feature is an enhancement to the **crypto isakmp key** global configuration command. With a wildcard IP address of 0.0.0.0 and pre-shared key authentication method configured on the local router, the local router can authenticate the IKE security associations with any remote peer that has a matching wildcard pre-shared key.

## MIBs

### Current MIBs

If you have an account with Cisco.com, you can find the current list of Management Information Bases (MIBs) supported by Cisco. To reach the *Cisco Network Management Toolkit*, log in to Cisco.com, and click **Service & Support: Software Center: Network Mgmt Software: Cisco Network Management Toolkit: Cisco MIBs**.

### 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 NMS applications. You can update from deprecated MIBs to the replacement MIBs as shown in Table 18.

*Table 18* **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 decided
OLD-CISCO-DECNET-MIB	To be decided
OLD-CISCO-ENV-MIB	CISCO-ENVMON-MIB
OLD-CISCO-FLASH-MIB	CISCO-FLASH-MIB
OLD-CISCO-INTERFACES-MIB	IF-MIB CISCO-QUEUE-MIB
OLD-CISCO-IP-MIB	To be decided
OLD-CISCO-MEMORY-MIB	CISCO-MEMORY-POOL-MIB
OLD-CISCO-NOVELL-MIB	NOVELL-IPX-MIB
OLD-CISCO-SYS-MIB	(Compilation of other OLD* MIBs)



*Table 18 Deprecated and Replacement MIBs (continued)*

Deprecated MIB	Replacement
OLD-CISCO-SYSTEM-MIB	CISCO-CONFIG-COPY-MIB
OLD-CISCO-TCP-MIB	CISCO-TCP-MIB
OLD-CISCO-TS-MIB	To be decided
OLD-CISCO-VINES-MIB	CISCO-VINES-MIB
OLD-CISCO-XNS-MIB	To be decided

## Important Notes

The following sections contain important notes about Cisco IOS Release 12.1 T that apply to Cisco 7000 family routers.

### Image Deferral, Cisco IOS Release 12.1(5)T1

All Cisco 7200 series and Cisco 7500 series images in Cisco IOS Release 12.1(5)T have been deferred to Cisco IOS Release 12.1(5)T1 due to the following caveats:

- CSCds35103—ATM-PA3 ucode not working with peer PA3s having very old ucode
- CSCds39413—%TCP-6-NOBUFF: TTY0, no buffer available message
- CSCds62602—VIP2-40 still not seen even after rommon upgrade to Version 122.0
- CSCds69801—NPE-400: Could not load 121-5.T image, BUS error received



#### Note

Disclaimer: In order to increase network availability, Cisco recommends that you upgrade affected IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected IOS images. Any pending order will be substituted by the replacement software images. **PLEASE BE AWARE THAT FAILURE TO UPGRADE THE AFFECTED IOS IMAGES MAY RESULT IN NETWORK DOWNTIME.** The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images will apply to the replacement images.

### RSP-based MQC

As of Cisco IOS Release 12.1(5)T, RSP-based MQC features will no longer be supported and will be replaced by VIP-based MQC features.

See CSCds82672 in the *Caveats for Cisco IOS Release 12.1 T*. for more information.

## ICaveat CSCdr91706 and IOS HTTP Vulnerability

A defect in multiple releases of Cisco IOS software will cause a Cisco router or switch to halt and reload if the IOS HTTP service is enabled, browsing to `http://router-ip/anytext?/` is attempted, and the enable password is supplied when requested. This defect can be exploited to produce a denial of service (DoS) attack.

The vulnerability, identified as Cisco bug ID CSCdr91706, affects virtually all mainstream Cisco routers and switches running Cisco IOS software releases 12.0 through 12.1, inclusive. This is not the same defect as CSCdr36952.

The vulnerability has been corrected and Cisco is making fixed releases available for free to replace all affected IOS releases. Customers are urged to upgrade to releases that are not vulnerable to this defect as shown in detail below.

This vulnerability can only be exploited if the enable password is known or not set.

You are strongly encouraged to read the complete advisory, which is available at <http://www.cisco.com/warp/public/707/ioshttpserverquery-pub.shtml>.

## Last Maintenance Release of Cisco IOS Release 12.1 T

The last maintenance release of the 12.1 T release train is 12.1(5)T. The migration path for customers who need bug fixes for the 12.1 T features is the 12.2 mainline release. The 12.2 mainline release has the complete feature content of 12.1 T and will eventually reach general deployment (GD).

The last maintenance release was renamed from 12.1(4)T to 12.1(5)T to synchronize with its parent software base, the 12.1(5) mainline release, and to reflect that 12.1(5)T has all the bug fixes of the 12.1(5) mainline release. The 12.1 T release train is a superset of the 12.1 mainline release; hence any defect fixed in the 12.1 mainline is also fixed in 12.1 T. The set of features for 12.1(4)T is the same as that for 12.1(5)T. There was no change in the feature content of the release. The release was renamed so that the releases would be consistent with the Cisco release process.

## Image Deferral, Cisco IOS Release 12.1(3a)T2

The following images were deferred from Cisco IOS Release 12.1(3a)T2 to Cisco IOS Release 12.1(3a)T3:

- c7200-ds-mz
- c7200-ix-mz
- c7200-js-mz

These images were deferred due to the following caveats:

- CSCdr54535—Service-policy output on PA-A3 deleted after link down/up
- CSCdr52838—POTENT: Add support for PA recovery from watchdog timer expiration

**Note**

---

If you wish to avoid risk of having your system affected by the above-identified defect, you may replace it with the replacement image described above. If you do so, the same licenses, terms and conditions that governed your rights and obligations, and those of Cisco, with respect to the deferred image shall govern them with respect to the replacement image. If, on the other hand, you decide not to replace the deferred image, you proceed at your own risk. Manufacturing is discontinuing shipment of IOS Affected and, instead, will ship Software Solution.

---

For additional information on Cisco IOS Release 12.1 deferrals, including the Cisco IOS Release 12.1(3)T deferral, see the *What's Hot for Cisco IOS Software Release 12.1* documentation at Cisco.com. To reach the *What's Hot for Cisco IOS Software Release 12.1* document, log in to Cisco.com and follow this path:

**Service & Support: Software Center: Cisco IOS Software: Cisco IOS 12.1: What's Hot for Cisco IOS Software Release 12.1**

## Image Deferral, Cisco IOS Release 12.1(3a)T1

The c7200-is-mz and c7200-js-mz images were deferred from Cisco IOS Release 12.1(3a)T1 to Cisco IOS Release 12.1(3a)T2 due to the following caveat:

CSCDr97080—7200 Crashed when switching MPLS/VPN traffic in 12.1(3)T

**Note**

---

If you wish to avoid risk of having your system affected by the above-identified defect, you may replace it with the replacement image described above. If you do so, the same licenses, terms and conditions that governed your rights and obligations, and those of Cisco, with respect to the deferred image shall govern them with respect to the replacement image. If, on the other hand, you decide not to replace the deferred image, you proceed at your own risk. Manufacturing is discontinuing shipment of IOS Affected and, instead, will ship Software Solution.

---

For additional information on Cisco IOS Release 12.1 deferrals, including the Cisco IOS Release 12.1(3)T deferral, see the *What's Hot for Cisco IOS Software Release 12.1* documentation at Cisco.com. To reach the *What's Hot for Cisco IOS Software Release 12.1* document, log in to Cisco.com and follow this path:

**Service & Support: Software Center: Cisco IOS Software: Cisco IOS 12.1: What's Hot for Cisco IOS Software Release 12.1**

## Image Deferral, Cisco IOS Release 12.1(3)T

The c7200-is-mz and c7200-js-mz images were deferred from Cisco IOS Release 12.1(3)T to Cisco IOS Release 12.1(3a)T1 due to the following caveat:

CSCdr88376—FR LLQ: data packets appear in voice queue



### Note

If you wish to avoid risk of having your system affected by the above-identified defect, you may replace it with the replacement image described above. If you do so, the same licenses, terms and conditions that governed your rights and obligations, and those of Cisco, with respect to the deferred image shall govern them with respect to the replacement image. If, on the other hand, you decide not to replace the deferred image, you proceed at your own risk. Manufacturing is discontinuing shipment of IOS Affected and, instead, will ship Software Solution.

For additional information on Cisco IOS Release 12.1 deferrals, including the Cisco IOS Release 12.1(3)T deferral, see the *What's Hot for Cisco IOS Software Release 12.1* documentation at Cisco.com. To reach the *What's Hot for Cisco IOS Software Release 12.1* document, log in to Cisco.com and follow this path:

**Service & Support: Software Center: Cisco IOS Software: Cisco IOS 12.1: What's Hot for Cisco IOS Software Release 12.1**

## Cisco IOS Release 12.1(3)T and 12.1(3a)T1 Voice Issues

Due to a number of issues with H.323 and SIP voice support on the AS5300, AS5800, Cisco 2600, 3600, 7200 series and MC3810 which arose in Cisco IOS Release 12.1 T, use of maintenance release 12.1(3)T and 12.1(3a)T1 is strongly discouraged.

Due to the many customers who use these products for dial applications and significant new functionality introduced in these releases, this version of software is being made available for dial applications.

The problems with voice in this release are being tracked in the following DDTS reports:

- CSCdr78203 PC-to-phone one way audio problem
- CSCdr79120 Some information elements not passed between ISDN and H.323
- CSCdr78379 A simple call via a SW (T1pri) cannot connect
- CSCdr75660 Like CSCdr64591. Alerting but no ringback in ISDN
- CSCdr90963 Inband tones/announcements do not propagate for most ISDN switches
- CSCdr90711 Internet Call Waiting times out

For a more detailed Field Notice report see:

<http://www.cisco.com/warp/public/770/fn12860.shtml>

## Cisco IOS Software Product Numbering Change Announcement

Starting with releases 12.1(1) and 12.1(1)T, Cisco IOS software product numbers will be modified to fit within an 18-character product number field.

Because a Cisco IOS software product number remains at a maximum of 18 alphanumeric characters, the dots that provided delineation of release level have been eliminated to allow product number expansion. This will accommodate more products and features.

From Cisco IOS software release 12.1(1) onwards, decimal points or periods or dots (“.”) in Cisco IOS software product numbers are removed. This implementation minimizes changes and risks to customer and partner ordering systems that are interfacing with Cisco’s ERP system.

For more information, refer to Product Bulletin 1087.

## Caveats

Caveats describe unexpected behavior in Cisco IOS software releases. Severity 1 caveats are the most serious caveats; severity 2 caveats are less serious.

For information on caveats in Cisco IOS Release 12.1 T, see *Caveats for Cisco IOS Release 12.1 T*.

All caveats in Release 12.1 are also in Release 12.1 T.

For information on caveats in Cisco IOS Release 12.1, see *Caveats for Cisco IOS Release 12.1*, which lists severity 1 and 2 caveats and is located on Cisco.com and on the Documentation CD-ROM.



### 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, go to Cisco.com and click **Login**. Then click **Service & Support: Software Center: Cisco IOS Software: Cisco IOS Bug Toolkit: Cisco Bug Navigator II**. Another option is to go to [http://www.cisco.com/cgi-bin/Support/Bugtool/launch\\_bugtool.pl](http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl).

## Related Documentation

The following sections describe the documentation available for Cisco 7000 family routers. These documents consist of hardware and software installation guides, Cisco IOS configuration 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 on the Documentation CD-ROM.

Use these release notes with the following documents:

- Release-Specific Documents, page 94
- Platform-Specific Documents, page 94
- Feature Modules, page 95
- Cisco IOS Software Documentation Set, page 95

## Release-Specific Documents

The following documents are specific to Release 12.1 and are located on Cisco.com and on the Documentation CD-ROM:

- *Cross-Platform Release Notes for Cisco IOS Release 12.1*

On Cisco.com at:

**Technical Documents: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 12.1**

On the Documentation CD-ROM at:

**Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 12.1: 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 12.1 T*

See *Caveats for Cisco IOS Release 12.1* and *Caveats for Cisco IOS Release 12.1 T*, which contain caveats applicable to all platforms for all maintenance releases of Cisco IOS Release 12.1 and Cisco IOS Release 12.1 T.

On Cisco.com at:

**Technical Documents: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 12.1: Release Notes: Caveats**

On the Documentation CD-ROM at:

**Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 12.1: 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 **Service & Support: Software Center: Cisco IOS Software: Cisco IOS Bug Toolkit: Cisco Bug Navigator II**. Another option is to go to <http://www.cisco.com/support/bugtools>.

---

## Platform-Specific Documents

These documents are available for Cisco 7000 family routers on Cisco.com and on 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: Documentation Home Page: 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 Release 12.1 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: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 12.1: New Feature Documentation**

On the Documentation CD-ROM at:

**Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 12.1 T: New Feature Documentation**

## 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 that are shipped with your order in electronic form on the Documentation CD-ROM, unless you specifically order the printed versions.

## Documentation Modules

Each module in the Cisco IOS documentation set consists of two books: a configuration guide and a corresponding command reference. Chapters in a configuration guide describe protocols, configuration tasks, 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 and on the Documentation CD-ROM, two master hot-linked documents provide information for the Cisco IOS software documentation set.

On Cisco.com at:

**Technical Documents: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 12.1: Configuration Guides and Command References**

On the Documentation CD-ROM at:

**Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 12.1: Configuration Guides and Command References**

## Release 12.1 Documentation Set

Table 19 describes the contents of the Cisco IOS Release 12.1 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 on 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 12.1**

On the Documentation CD-ROM at:

**Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 12.1**

*Table 19 Cisco IOS Software Release 12.1 Documentation Set*

Books	Major Topics
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Configuration Fundamentals Configuration Guide</i></li> <li>• <i>Cisco IOS Configuration Fundamentals Command Reference</i></li> </ul>	Configuration Fundamentals Overview Cisco IOS User Interfaces Cisco IOS File Management Cisco IOS System Management Cisco IOS User Interfaces Commands Cisco IOS File Management Commands Cisco IOS System Management Commands
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Bridging and IBM Networking Configuration Guide</i></li> <li>• <i>Cisco IOS Bridging and IBM Networking Command Reference, Volume I</i></li> <li>• <i>Cisco IOS Bridging and IBM Networking Command Reference, Volume II</i></li> </ul>	Using Cisco IOS Software Overview of SNA Internetworking Bridging IBM Networking
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Dial Services Configuration Guide: Terminal Services</i></li> <li>• <i>Cisco IOS Dial Services Configuration Guide: Network Services</i></li> <li>• <i>Cisco IOS Dial Services Command Reference</i></li> </ul>	Preparing for Dial Access Modem Configuration and Management ISDN and Signalling Configuration PPP Configuration Dial-on-Demand Routing Configuration Dial-Backup Configuration Terminal Service Configuration Large-Scale Dial Solutions Cost-Control Solutions Virtual Private Networks X.25 on ISDN Solutions Telco Solutions Dial-Related Addressing Services Interworking Dial Access Scenarios



Table 19 Cisco IOS Software Release 12.1 Documentation Set (continued)

Books	Major Topics
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Interface Configuration Guide</i></li> <li>• <i>Cisco IOS Interface Command Reference</i></li> </ul>	Interface Configuration Overview Configuring LAN Interfaces Configuring Serial Interfaces Configuring Logical Interfaces
<ul style="list-style-type: none"> <li>• <i>Cisco IOS IP and IP Routing Configuration Guide</i></li> <li>• <i>Cisco IOS IP and IP Routing Command Reference</i></li> </ul>	IP Addressing and Services IP Routing Protocols IP Multicast
<ul style="list-style-type: none"> <li>• <i>Cisco IOS AppleTalk and Novell IPX Configuration Guide</i></li> <li>• <i>Cisco IOS AppleTalk and Novell IPX Command Reference</i></li> </ul>	AppleTalk and Novell IPX Overview Configuring AppleTalk Configuring Novell IPX
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS, and XNS Configuration Guide</i></li> <li>• <i>Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS, and XNS Command Reference</i></li> </ul>	Apollo Domain, Banyan VINES, DECnet, ISO CLNS, and XNS Overview Configuring Apollo Domain Configuring Banyan VINES Configuring DECnet Configuring ISO CLNS Configuring XNS
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Multiservice Applications Configuration Guide</i></li> <li>• <i>Cisco IOS Multiservice Applications Command Reference</i></li> </ul>	Multiservice Applications Overview Voice Video Broadband
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Quality of Service Solutions Configuration Guide</i></li> <li>• <i>Cisco IOS Quality of Service Solutions Command Reference</i></li> </ul>	Quality of Service Overview Classification Congestion Management Congestion Avoidance Policing and Shaping Signalling Link Efficiency Mechanisms Quality of Service Solutions
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Security Configuration Guide</i></li> <li>• <i>Cisco IOS Security Command Reference</i></li> </ul>	Security Overview Authentication, Authorization, and Accounting (AAA) Security Server Protocols Traffic Filtering and Firewalls IP Security and Encryption Other Security Features
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Switching Services Configuration Guide</i></li> <li>• <i>Cisco IOS Switching Services Command Reference</i></li> </ul>	Cisco IOS Switching Services Overview Cisco IOS Switching Paths Cisco Express Forwarding NetFlow Switching Multiprotocol Label Switching Multilayer Switching Multicast Distributed Switching Virtual LANs LAN Emulation

*Table 19 Cisco IOS Software Release 12.1 Documentation Set (continued)*

Books	Major Topics
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Wide-Area Networking Configuration Guide</i></li> <li>• <i>Cisco IOS Wide-Area Networking Command Reference</i></li> </ul>	<ul style="list-style-type: none"> <li>Wide-Area Networking Overview</li> <li>Configuring ATM</li> <li>Configuring Frame Relay</li> <li>Configuring Frame Relay-ATM Interworking</li> <li>Configuring SMDS</li> <li>Configuring X.25 and LAPB</li> </ul>
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Configuration Guide Master Index</i></li> <li>• <i>Cisco IOS Command Reference Master Index</i></li> <li>• <i>Cisco IOS Debug Command Reference</i></li> <li>• <i>Cisco IOS Dial Services Quick Configuration Guide</i></li> <li>• <i>Cisco IOS Software System Error Messages</i></li> <li>• <i>New Features in 12.1-Based Limited Lifetime Releases</i></li> <li>• <i>New Features in Release 12.1 T</i></li> <li>• Release Notes (Release note and caveat documentation for 12.1-based releases and various platforms)</li> </ul>	

## Obtaining Documentation

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

### World Wide Web

You can access the most current Cisco documentation on the World Wide Web at the following sites:

- <http://www.cisco.com>
- <http://www-china.cisco.com>
- <http://www-europe.cisco.com>

### 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](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 product 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](mailto:bug-doc@cisco.com).

To submit your comments by mail, for your convenience many documents contain a response card behind the front cover. 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

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools. For Cisco.com registered users, additional troubleshooting tools are available from the TAC website.

### 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/>

If you cannot resolve your technical issue by using the TAC online resources, Cisco.com registered users 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.

---

This document is to be used in conjunction with the documents listed in the “Related Documentation” section on page 93.

Access Registrar, AccessPath, Are You Ready, ATM Director, Browse with Me, CCDA, CCDE, CDDP, CCIE, CCNA, CCNP, CCSI, CD-PAC, *CiscoLink*, the Cisco NetWorks logo, Cisco Powered Network logo, Cisco Systems Networking Academy, Fast Step, FireRunner, Follow Me Browsing, FormShare, GigaStack, IGX, Intelligence in the Optical Core, Internet Quotient, IP/VC, iQ Breakthrough, iQ Expertise, iQ FastTrack, iQ Logo, iQ Readiness Scorecard, Kernel Proxy, MGX, Natural Network Viewer, Network Registrar, the Networkers logo, *Packet*, PIX, Point and Click Internetworking, Policy Builder, RateMUX, ReyMaster, ReyView, ScriptShare, Secure Script, Shop with Me, SlideCast, SMARTnet, SVX, TrafficDirector, TransPath, VlanDirector, Voice LAN, Wavelength Router, WebViewer, Workgroup Director, and Workgroup Stack are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, Empowering the Internet Generation, are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, Cisco, the Cisco Certified Internetwork Expert Logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Collision Free, Enterprise/Solver, EtherChannel, EtherSwitch, FastHub, FastLink, FastPAD, IOS, IP/TV, IPX, LightStream, LightSwitch, MICA, NetRanger, Post-Routing, Pre-Routing, Registrar, StrataView Plus, Stratm, SwitchProbe, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. or its affiliates in the U.S. and certain other countries.

All other brands, names, or trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0010R)

Copyright © 2000, Cisco Systems, Inc.  
All rights reserved.

