



Release Notes for Cisco 4000 Series for Cisco IOS Release 12.1T

November 27, 2000



Note

See Important Notes, page 24 for information concerning Cisco IOS Release 12.1(5)T.



Note

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

These release notes for the Cisco 4000 series describe the enhancements provided in Cisco IOS Release 12.1(5)T. These release notes are updated as needed.

For a list of the software caveats that apply to Cisco IOS Release 12.1T, 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 CCO and the Documentation CD-ROM.

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

Contents

These release notes describe the following topics:

- System Requirements, page 2
- New and Changed Information, page 14
- Limitations and Restrictions, page 25
- Caveats, page 26
- Related Documentation, page 26



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

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

78-10715-04 Rev. B0

- Obtaining Documentation, page 31
- Obtaining Technical Assistance, page 32

System Requirements

This section describes the system requirements for Release 12.1(5)T:

- Memory Recommendations, page 2
- Hardware Supported, page 3
- Determining the Software Version, page 4
- Upgrading to a New Software Release, page 4
- Feature Set Tables, page 4

Memory Recommendations

Table 1 lists the recommended minimum memory for the Cisco 4000 series for Cisco IOS Release 12.1(5)T.

Table 1 Memory Requirements for the Cisco 4000 Series

Feature Set by Platform	Image Name	Recommended Flash Memory	Recommended DRAM Memory	Runs From	
Cisco 4500/4500-M, Cisco 4700/4700-M	IP	c4500-i-mz	8 MB	32 MB	RAM
	IP Plus	c4500-is-mz	8 MB	32 MB	RAM
	IP Plus IPsec 56	c4500-is56i-mz	8 MB	32 MB	RAM
	IP Plus IPsec 3DES	c4500-ik2s-mz	8 MB	32 MB	RAM
	IP Plus/SNASw Plus	c4500-a3is-mz	8 MB	32 MB	RAM
	IP/IPX/AT/DEC	c4500-d-mz	8 MB	32 MB	RAM
	IP/IPX/AT/DEC Plus	c4500-ds-mz	8 MB	32 MB	RAM
	Enterprise Plus	c4500-js-mz	16 MB	32 MB	RAM
	Enterprise Plus IPsec 56	c4500-js56i-mz	16 MB	32 MB	RAM
	Enterprise Plus IPsec 3DES	c4500-jk2s-mz	16 MB	32 MB	RAM
	Enterprise/SNASw Plus	c4500-a3js-mz	16 MB	32 MB	RAM
	Enterprise/SNASw Plus IPsec 56	c4500-a3js56i-mz	16 MB	32 MB	RAM
	Enterprise/SNASw Plus IPsec 3DES	c4500-a3jk2s-mz	16 MB	32 MB	RAM
Cisco 4700-M	DistributedDirector	c4500-w3-mz	16 MB	32 MB	RAM

Hardware Supported

Cisco IOS Release 12.1(5)T supports the Cisco 4000 series routers:

- Cisco 4500, Cisco 4500-M
- Cisco 4700, Cisco 4700-M


Note

Because of memory limitations, Cisco 4000 and 4000-M routers are not supported by Cisco IOS Release 12.1T. These platforms will continue to be supported by Cisco IOS Release 12.1 and earlier releases.

Table 2 lists the interfaces supported by the Cisco 4000 series.

Table 2 Supported Interfaces

Interface, Network Module, or Data Rate		Platforms Supported
LAN Interfaces	ATM Interface	Cisco 4500 and Cisco 4700
	Ethernet	Cisco 4500 and Cisco 4700
	Fast Ethernet	Cisco 4500 and Cisco 4700
	Token Ring	Cisco 4500 and Cisco 4700
	FDDI	Cisco 4500 and Cisco 4700
	Serial	Cisco 4500 and Cisco 4700
	HSSI	Cisco 4500 and Cisco 4700
	ISDN BRI	Cisco 4500 and Cisco 4700
	Channelized E1/T1 ISDN PRI	Cisco 4500 and Cisco 4700
	ATM OC-3c	Cisco 4500 and Cisco 4700
	ATM DS-3	Cisco 4500 and Cisco 4700
	ATM E3	Cisco 4500 and Cisco 4700
WAN Data Rates	48/56/64 kbps	Cisco 4500 and Cisco 4700
	1.544/2.048 Mbps	Cisco 4500 and Cisco 4700

Table 2 Supported Interfaces (continued)

Interface, Network Module, or Data Rate	Platforms Supported	
WAN Interfaces and Network Modules	56K/64K DSU/CSU	Cisco 4500 and Cisco 4700
	Channelized E1	Cisco 4500 and Cisco 4700
	Channelized T1	Cisco 4500 and Cisco 4700
	E1-G.703/G.704	Cisco 4500 and Cisco 4700
	EIA/TIA-232	Cisco 4500 and Cisco 4700
	EIA/TIA-449	Cisco 4500 and Cisco 4700
	EIA/TIA-613 (HSSI)	Cisco 4500 and Cisco 4700
	EIA-530	Cisco 4500 and Cisco 4700
	ISDN BRI	Cisco 4500 and Cisco 4700
	ISDN PRI	Cisco 4500 and Cisco 4700
	MultiChannel Interface (Channelized E1/T1)	Cisco 4500 and Cisco 4700
	Serial	Cisco 4500 and Cisco 4700
	V.35	Cisco 4500 and Cisco 4700
	X.21	Cisco 4500 and Cisco 4700

Determining the Software Version

To determine the version of Cisco IOS software running on your Cisco 4000 series router, log in to the router and use the **show version EXEC** command:

```
router>#show version
Cisco Internetwork Operating System Software
IOS (tm) 4500 Software (C4500-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 the product bulletin *Cisco IOS Upgrade Ordering Instructions* on CCO at:

Technical Documents: Product Bulletins: Software: General System Software Bulletins

Feature Set Tables

Cisco IOS software is packaged in feature sets consisting of software images—depending on the platform, as listed in Table 3. Each feature set contains a specific set of Cisco IOS features.

Table 3 Feature Sets Supported by the Cisco 4000 Series

Feature Set	Feature Set Matrix Term	Software Image	Platforms Supported
IP Standard Feature Sets	IP	Basic ¹	c4500-i-mz Cisco 4500/4500-M, Cisco 4700/4700-M
	IP Plus	Plus ²	c4500-is-mz Cisco 4500/4500-M, Cisco 4700/4700-M
	IP Plus IPsec 56	Plus, Plus IPsec 56 ³	c4500-is56i-mz Cisco 4500/4500-M, Cisco 4700/4700-M
	IP Plus IPsec 3DES	Plus, Plus IPsec, 3DES ⁴	c4500-ik2s-mz Cisco 4500/4500-M, Cisco 4700/4700-M
IP/IPX/Apple Talk/DEC Standard Feature Sets	IP/IPX/AppleTalk/DEC	Basic	c4500-d-mz Cisco 4500/4500-M, Cisco 4700/4700-M
	IP/IPX/AppleTalk/DEC Plus	Plus	c4500-ds-mz Cisco 4500/4500-M, Cisco 4700/4700-M
Enterprise Standard Feature Sets	Enterprise Plus	Plus	c4500-js-mz Cisco 4500/4500-M, Cisco 4700/4700-M
	Enterprise Plus IPsec 56	Plus, Plus IPsec 56	c4500-js56i-mz Cisco 4500/4500-M, Cisco 4700/4700-M
	Enterprise Plus IPsec 3DES	Plus, Plus IPsec 56, 3DES	c4500-jk2s-mz Cisco 4500/4500-M, Cisco 4700/4700-M
Enterprise/SNASw Standard Feature Set	IP Plus/SNASw Plus	Plus	c4500-a3is Cisco 4500/4500-M, Cisco 4700/4700-M
	Enterprise/SNASw Plus	Plus	c4500-a3js-mz Cisco 4500/4500-M, Cisco 4700/4700-M
	Enterprise/SNASw Plus IPsec 56	Plus, Plus IPsec 56	c4500-a3js56i-mz Cisco 4500/4500-M, Cisco 4700/4700-M
	Enterprise/SNASw Plus IPsec 3DES	Plus, Plus IPsec, 3DES	c4500-a3jk2s-mz Cisco 4500/4500-M, Cisco 4700/4700-M
Distributed-Director Standard Feature Set	DistributedDirector	Distributed-Director	c4500-w3-mz Cisco 4700-M

1. This feature set is offered in the basic feature set.

2. This feature set is offered in the Plus feature set.

3. This feature set is offered in the encryption feature sets which consist of IPsec 56-bit (Plus IPsec 56) data encryption feature sets.

4. This feature set is offered in the encryption feature sets which consist of Triple DES (3DES) Encryption data encryption feature sets.

**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.

Table 4 and Table 5 list the features and feature sets images supported by Cisco IOS Release 12.1(5)T for the Cisco 4500, 4500-M, 4700, and 4700-M.

All tables use the following conventions to identify features:

- Yes—The feature is supported in the feature set.
- No—The feature is not supported in the feature set.

**Note**

This feature set table only contains a selected list of features. This table is not cumulative—nor does it list all the features in each image.

Table 4 Feature List by Feature Set for the Cisco 4500/4500-M and 4700/4700-M—Part 1 of 2

Features	Feature Sets							
	IP	IP Plus	IP Plus 40	IP Plus IPsec 56	IP Plus IPsec 3DES	IP/IPX/AT/DEC	IP/IPX/AT/DEC Plus	IP Plus/SNASw Plus
Features in Release 12.1(5)T								
AutoInstall Using DHCP for LAN Interfaces	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Class Based Ethernet CoS Matching and Marking (802.1p & ISL CoS)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Class Based Policer for the DiffServ AF PHB	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Class Based QoS MIB	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Closed User Group Selection Facility Suppress Option	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
DistributedDirector Enhancements for Cisco IOS Release 12.1(5)T	No	No	No	No	No	No	No	No
DiffServ Compliant WRED	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
IGMP Version 3	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Inter-Autonomous Systems MPLS VPN Support	No	No	No	No	No	No	No	No
NAT - Enhanced H.225/H.245 Forwarding Engine	No	No	No	No	No	No	No	No

Table 4 Feature List by Feature Set for the Cisco 4500/4500-M and 4700/4700-M—Part 1 of 2 (continued)

Features	Feature Sets							
	IP	IP Plus	IP Plus 40	IP Plus IPsec 56	IP Plus IPsec 3DES	IP/IPX/AT/DEC	IP/IPX/AT/DEC Plus	IP Plus/SNASw Plus
NAT - Support for NetMeeting (Internet Locator Service - ILS)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
NAT - Support of H.323 v2 Call Signaling (FastConnect)	No	No	No	No	No	No	No	No
NAT - Support of IP Phone to Cisco Call Manager	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
NTP MIB	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Parser Cache	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
PIM Dense Mode State Refresh	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
PPPoE Over IEEE 802.1Q VLANs	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
PPPoE RADIUS Port Identification	No	Yes	Yes	Yes	Yes	No	No	Yes
SDLC SNRM Timer and Window Size	No	Yes	Yes	Yes	Yes	No	No	Yes
Connectivity								
Layer 2 Tunnel Protocol (L2TP)	No	Yes	Yes	Yes	Yes	No	Yes	
L2TP Dial Out	No	Yes	Yes	Yes	Yes	No	Yes	
Multicast Source Discovery Protocol	Yes	Yes	Yes	Yes	Yes	Yes	Yes	
OS_IFSS	Yes	Yes	Yes	Yes	Yes	Yes	Yes	
PPP over Ethernet	No	Yes	Yes	Yes	Yes	No	No	
RIP Enhancements	Yes	Yes	Yes	Yes	Yes	Yes	Yes	
Ease of Use								
Interface MIB Implementation for ATM Subinterfaces ¹	No	Yes	Yes	Yes	Yes	No	Yes	
IBM Support								
DLSw+ Ethernet Redundancy	No	Yes	Yes	Yes	Yes	No	Yes	
DLSW RSVP	No	Yes	Yes	Yes	Yes	No	Yes	
IP/IPX Routing								
Airline Product Set	Yes	Yes	Yes	Yes	Yes	Yes	Yes	
Bidirectional PIM	Yes	Yes	Yes	Yes	Yes	Yes	Yes	
DNS for X.25	Yes	Yes	Yes	Yes	Yes	Yes	Yes	
Easy IP Phase 2-DHCP Server	Yes	Yes	Yes	Yes	Yes	Yes	Yes	
Flow WRED	Yes	Yes	Yes	Yes	Yes	Yes	Yes	
IPX Multilayer Switching	Yes	Yes	Yes	Yes	Yes	Yes	Yes	
Multilayer Switching for IP Multicast	No	Yes	Yes	Yes	Yes	Yes	Yes	
Multicast Routing Monitor	Yes	Yes	Yes	Yes	Yes	Yes	Yes	
OSPF Flooding Reduction	Yes	Yes	Yes	Yes	Yes	Yes	Yes	

Table 4 Feature List by Feature Set for the Cisco 4500/4500-M and 4700/4700-M—Part 1 of 2 (continued)

Features	Feature Sets							
	IP	IP Plus	IP Plus 40	IP Plus IPsec 56	IP Plus IPsec 3DES	IP/IPX/AT/DEC	IP/IPX/AT/DEC Plus	IP Plus/SNASw Plus
OSPF Packet Pacing	Yes	Yes	Yes	Yes	Yes	Yes	Yes	
PGM Router Assist	Yes	Yes	Yes	Yes	Yes	Yes	Yes	
WCCP	Yes	Yes	Yes	Yes	Yes	Yes	Yes	
X.25 Load Balancing	Yes	Yes	Yes	Yes	Yes	Yes	Yes	
X.25 Remote Failure Detection	Yes	Yes	Yes	Yes	Yes	Yes	Yes	
Management								
SNMP Support for IOS vLAN Subinterfaces	No	Yes	Yes	Yes	Yes	Yes	Yes	
Event MIB	Yes	Yes	Yes	Yes	Yes	Yes	Yes	
CNS Client for Cisco IOS Software	No	No	No	Yes	Yes	No	No	
CNS Client for Cisco IOS (IPsec Policy Agent II)	No	No	No	No	No	No	No	
ISDN MIB RFC 2127	Yes	Yes	Yes	Yes	Yes	Yes	Yes	
Network Director Forwarding Agent	No	Yes	Yes	Yes	Yes	No	Yes	
Process MIB	Yes	Yes	Yes	Yes	Yes	Yes	Yes	
Service Assurance Agent	Yes	Yes	Yes	Yes	Yes	Yes	Yes	
SNMPv3	Yes	Yes	Yes	Yes	Yes	Yes	Yes	
Subnetwork Bandwidth Manager	Yes	Yes	Yes	Yes	Yes	Yes	Yes	
Quality of Service								
CLI String Search	Yes	Yes	Yes	Yes	Yes	Yes	Yes	
COPS for RSVP	Yes	Yes	Yes	Yes	Yes	Yes	Yes	
LANE Fast SSRP	No	Yes	Yes	Yes	Yes	No	Yes	
MPLS VPN	No	No	No	No	No	No	No	
MPLS Class of Service	No	No	No	No	No	No	No	
Express Resource Transport Protocol and TCP Header Compression	Yes	Yes	Yes	Yes	Yes	Yes	Yes	
Reliability								
Pragmatic General Multicast	No	No	No	No	No	No	No	
Scalability								
IETF-Compliant PPP over ATM Scalability	Yes	Yes	Yes	Yes	Yes	Yes	Yes	
Security								
Secure Shell Version 1 Integrated Client	No	No	No	Yes	Yes	No	No	
X.25 Closed User Groups	No	Yes	Yes	Yes	Yes	No	Yes	

Table 4 Feature List by Feature Set for the Cisco 4500/4500-M and 4700/4700-M—Part 1 of 2 (continued)

Features	Feature Sets							
	IP	IP Plus	IP Plus 40	IP Plus IPsec 56	IP Plus IPsec 3DES	IP/IPX/AT/DEC	IP/IPX/AT/DEC Plus	IP Plus/SNASw Plus
Switching								
Bridging between IEEE 802.1Q vLANs	No	No	No	No	No	No	No	
CEF Support for IP Routing between IEEE 802.1Q vLANs	No	Yes	Yes	Yes	Yes	Yes	Yes	
Cisco IOS STP Enhancements	No	Yes	Yes	Yes	Yes	No	Yes	
MPLS Traffic Engineering	No	No	No	No	No	Yes	Yes	
SNA Switching Services	No	No	No	No	No	No	No	
X.25 Switch Local Acknowledgment	No	Yes	Yes	Yes	Yes	No	Yes	
Voice								
PPP over ATM SVC	Yes	Yes	Yes	Yes	Yes	Yes	Yes	
WAN Services								
Frame Relay ELMI Address Registration	Yes	Yes	Yes	Yes	Yes	Yes	Yes	
Annex G (X.25 over Frame Relay)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	
ATM LANE FSSR Protocol	No	Yes	Yes	Yes	Yes	No	Yes	
ATM PVC Trap Support	Yes	Yes	Yes	Yes	Yes	Yes	Yes	
Cisco IOS IEEE 802.1Q	No	Yes	Yes	Yes	Yes	Yes	Yes	
Dynamic Multiple Encapsulation for Dial-in over ISDN	Yes	Yes	Yes	Yes	Yes	Yes	Yes	
Frame Relay End-to-End Keepalive	Yes	Yes	Yes	Yes	Yes	Yes	Yes	
Frame Relay Switching Enhancements: Shaping and Policing	Yes	Yes	Yes	Yes	Yes	Yes	Yes	
Mobile IP	No	Yes	Yes	Yes	Yes	No	Yes	
Time-based Access List	Yes	Yes	Yes	Yes	Yes	Yes	Yes	

1. Available on the Cisco 4500 only.

Table 5 Feature List by Feature Set for the Cisco 4500/4500-M and 4700/4700-M—Part 2 of 2

Features	Feature Sets						
	Enterprise Plus	Enterprise Plus IPsec 56	Enterprise Plus IPsec 3DES	Enterprise/SNASw Plus	Enterprise/SNASw Plus IPsec 56	Enterprise/SNASw Plus IPsec 3DES	Distributed-Director
New Features in Release 12.1(5)T							
Autoinstall Using DHCP for LAN Interfaces	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Class Based Ethernet CoS Matching and Marking (802.1p & ISL CoS)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Class Based Policer for the DiffServ AF PHB	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Class Based QoS MIB	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Closed User Group Selection Facility Suppress Option	Yes	Yes	Yes	Yes	Yes	Yes	Yes
DistributedDirector Enhancements for Cisco IOS Release 12.1(5)T	No	No	No	No	No	No	Yes
DiffServ Compliant WRED	Yes	Yes	Yes	Yes	Yes	Yes	Yes
IGMP Version 3	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Inter-Autonomous Systems MPLS VPN Support	Yes	Yes	Yes	Yes	Yes	Yes	No
NAT - Enhanced H.225/H.245 Forwarding Engine	Yes	Yes	Yes	Yes	Yes	Yes	No
NAT - Support for NetMeeting (Internet Locator Service - ILS)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
NAT - Support of H.323 v2 Call Signaling (FastConnect)	Yes	Yes	Yes	Yes	Yes	Yes	No
NAT - Support of IP Phone to Cisco Call Manager	Yes	Yes	Yes	Yes	Yes	Yes	Yes
NTP MIB	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Parser Cache	Yes	Yes	Yes	Yes	Yes	Yes	Yes
PIM Dense Mode State Refresh	Yes	Yes	Yes	Yes	Yes	Yes	Yes
PPP Over Fast Ethernet 802.1Q VLANs	Yes	Yes	Yes	Yes	Yes	Yes	No
PPPoE RADIUS Port Identification	Yes	Yes	Yes	Yes	Yes	Yes	No
SDLC SNRM Timer and Window Size	Yes	Yes	Yes	Yes	Yes	Yes	No

Table 5 Feature List by Feature Set for the Cisco 4500/4500-M and 4700/4700-M—Part 2 of 2 (continued)

Features	Feature Sets						
	Enterprise Plus	Enterprise Plus IPsec 56	Enterprise Plus IPsec 3DES	Enterprise/SNASw Plus	Enterprise/SNASw Plus IPsec 56	Enterprise/SNASw Plus IPsec 3DES	Distributed-Director
Connectivity							
Layer 2 Tunnel Protocol (L2TP)	Yes	Yes	Yes	Yes	Yes	Yes	No
L2TP Dial Out	Yes	Yes	Yes	Yes	Yes	Yes	No
Multicast Source Discovery Protocol	Yes	Yes	Yes	Yes	Yes	Yes	No
OS_IFSS	Yes	Yes	Yes	Yes	Yes	Yes	Yes
PPP over Ethernet	Yes	Yes	Yes	Yes	Yes	Yes	No
RIP Enhancements	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Ease of Use							
Interface MIB Implementation for ATM Supinterfaces	Yes	Yes	Yes	Yes	Yes	Yes	Yes
IBM Support							
DLSw+ Ethernet Redundancy	Yes	Yes	Yes	Yes	Yes	Yes	No
DLSW RSVP	Yes	Yes	Yes	Yes	Yes	Yes	Yes
IP/IPX Routing							
Airline Product Set	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Bidirectional PIM	Yes	Yes	Yes	Yes	Yes	Yes	Yes
DNS for X.25	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Easy IP Phase 2-DHCP Server	Yes	Yes	Yes	Yes	Yes	Yes	No
Flow WRED	Yes	Yes	Yes	Yes	Yes	Yes	Yes
IPX Multilayer Switching	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Multilayer Switching for IP Multicast	Yes	Yes	Yes	Yes	Yes	Yes	No
Multicast Routing Monitor	Yes	Yes	Yes	Yes	Yes	Yes	Yes
OSPF Flooding Reduction	Yes	Yes	Yes	Yes	Yes	Yes	Yes
OSPF Packet Pacing	Yes	Yes	No	Yes	Yes	Yes	Yes
Policy Routing Infrastructure	Yes	Yes	Yes	Yes	Yes	Yes	Yes
PGM Router Assist	Yes	Yes	Yes	Yes	Yes	Yes	Yes
WCCPv2 Support	Yes	Yes	Yes	Yes	Yes	Yes	Yes
X.25 Load Balancing	Yes	Yes	Yes	Yes	Yes	Yes	Yes
X.25 Failure Remote Detection	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Table 5 Feature List by Feature Set for the Cisco 4500/4500-M and 4700/4700-M—Part 2 of 2 (continued)

Features	Feature Sets						
	Enterprise Plus	Enterprise Plus IPsec 56	Enterprise Plus IPsec 3DES	Enterprise/SNASw Plus	Enterprise/SNASw Plus IPsec 56	Enterprise/SNASw Plus IPsec 3DES	Distributed-Director
Management							
SNMP Support for IOS vLAN Subinterfaces	Yes	Yes	Yes	Yes	Yes	Yes	No
Individual SNMP Trap Support	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Event MIB	Yes	Yes	Yes	Yes	Yes	Yes	Yes
CNS Client for Cisco IOS Software	Yes	Yes	Yes	Yes	Yes	Yes	No
CNS Client for Cisco IOS (IPsec Policy Agent II)	Yes	Yes	Yes	Yes	Yes	Yes	No
ISDN MIB RFC 2127	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Network Director Forwarding Agent	Yes	Yes	Yes	Yes	Yes	Yes	No
Process MIB	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Service Assurance Agent	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SNMPv3	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Subnetwork Bandwidth Manager	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Quality of Service							
CLI String Search	Yes	Yes	Yes	Yes	Yes	Yes	Yes
COPS for RSVP	Yes	Yes	Yes	Yes	Yes	Yes	Yes
LANE Fast SSRP	Yes	Yes	Yes	Yes	Yes	Yes	No
MPLS VPN	Yes	Yes	Yes	Yes	Yes	Yes	No
MPLS Class of Service	Yes	Yes	Yes	Yes	Yes	Yes	No
Express Resource Transport Protocol and TCP Header Compression	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Reliability							
Pragmatic General Multicast	Yes	Yes	Yes	Yes	Yes	Yes	No
Scalability							
IETF-Compliant PPP over ATM Scalability		Yes	Yes	Yes	Yes	Yes	No

Table 5 Feature List by Feature Set for the Cisco 4500/4500-M and 4700/4700-M—Part 2 of 2 (continued)

Features	Feature Sets						
	Enterprise Plus	Enterprise Plus IPsec 56	Enterprise Plus IPsec 3DES	Enterprise/SNASw Plus	Enterprise/SNASw Plus IPsec 56	Enterprise/SNASw Plus IPsec 3DES	Distributed-Director
Security							
Secure Shell Version 1 Integrated Client	No	Yes	Yes	No	Yes	Yes	No
AAA Server Group Deadtimer	Yes	Yes	Yes	Yes	Yes	Yes	Yes
X.25 Closed User Groups	Yes	Yes	Yes	Yes	Yes	Yes	No
Switching							
CEF Support for IP Routing between IEEE 802.1Q vLANs	Yes	Yes	Yes	Yes	Yes	Yes	No
Bridging between IEEE 802.1Q vLANs	Yes	Yes	Yes	Yes	Yes	Yes	No
Cisco IOS STP Enhancements	Yes	Yes	Yes	Yes	Yes	Yes	No
MPLS Traffic Engineering	Yes	Yes	Yes	Yes	Yes	Yes	No
SNA Switching Services	No	No	No	Yes	Yes	Yes	No
X.25 Switch Local Acknowledgement	Yes	Yes	Yes	Yes	Yes	Yes	No
Voice							
PPP over ATM SVC	Yes	Yes	Yes	Yes	Yes	Yes	Yes
WAN Services							
Frame Relay ELMI Address Registration	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Annex G	Yes	Yes	Yes	Yes	Yes	Yes	Yes
ATM LANE FSSR Protocol	Yes	Yes	Yes	Yes	Yes	Yes	No
ATM PVC Trap Support	Yes	Yes	Yes	Yes	Yes	Yes	No
Cisco IOS IEEE 802.1Q	Yes	Yes	Yes	Yes	Yes	Yes	No
Dynamic Encapsulation for Dial-in over ISDN	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Frame Relay Switching Enhancements: Shaping and Policing	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Frame Relay End to End Keepalive	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Mobile IP	Yes	Yes	Yes	Yes	Yes	Yes	No
Time-Based Access List	Yes	Yes	Yes	Yes	Yes	Yes	Yes

New and Changed Information

The following sections list the new hardware and software features supported by the Cisco 4000 series for Cisco IOS Release 12.1 T.

New Hardware Features in Release 12.1(5)T

There are no new hardware features supported by the Cisco 4000 series in Cisco IOS Release 12.1(5)T.

New Hardware Features in Release 12.1(3)T

There are no new hardware features supported by the Cisco 4000 series in Cisco IOS Release 12.1(3)T.

New Hardware Features in Release 12.1(2)T

There are no new hardware features supported by the Cisco 4000 series in Cisco IOS Release 12.1(2)T.

New Software Features in Release 12.1(5)T.

The following new software features are supported by the Cisco 4000 series for Cisco IOS Release 12.1(5)T.

AutoInstall Using DHCP for LAN Interfaces

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 which 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 LAN 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 allows 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 allows for the uploading of configuration files using unicast TFTP.

Class Based Ethernet CoS Matching and Marking (802.1p & ISL CoS)

The Class-Based Ethernet CoS Matching and Marking (802.1p & ISL CoS) feature (which is also called Class-Based Marking or QoS Packet Marking in some Cisco documentation) has been enhanced for the Cisco 3640 routers to include the ability to mark and match Class of Service values and to set the ATM cell lose priority (CLP) bit value on packets.

Associating a packet with a local CoS value enables users to associate a Layer 2 Class of Service (CoS) value with a packet. The value can then be used to classify packets based on user-defined requirements. Layer 2 to Layer 3 mapping can also be configured by matching on the CoS value, since switches already have the capability to match and set CoS values. If a packet that needs to be marked to differentiate user-defined QoS services is leaving a router and entering a switch, the router should set the CoS value of the packet, since the switch can process the Layer 2 CoS header marking.

Changing the CLP bit setting in the ATM header of a cell provides a method of controlling the discarding of cells in congested ATM environments. 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 users had the ability to change the CLP bit setting in the ATM header, the CLP bit was automatically set to 0 on packets leaving Cisco routers that were converted into ATM cells for ATM networks. The CLP bit on packets leaving Cisco routers for ATM networks can now be set to 1.

For additional information on Class-Based Packet Marking, including information on the new enhancements, see the *Class-Based Packet Marking* feature module on CCO and the Documentation CD-ROM.

Class Based Policer for the DiffServ AF PHB

The Class-Based Policer for the DiffServ AF PHB is based on RFC 2697 - "A Single Rate Three Color Marker". The packet stream is metered and packets are marked either "conform", "exceed", or "violate". Marking is based on a Committed Information Rate (CIR) and two associated burst sizes, a Committed Burst Size (CBS) and an Excess Burst Size (EBS). A packet is marked "conform" if it doesn't exceed the CBS, "exceed" if it exceeds the CBS, but not the EBS, and "violate" otherwise.

Class-Based QoS MIB

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

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).

DistributedDirector Enhancements for Cisco IOS Release 12.1(5)T

The DistributedDirector Enhancements for Cisco IOS Release 12.1(5)T feature sends event information to the IOS syslog.

DiffServ Compliant WRED

This 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). This feature enables customers to 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.

IGMP Version 3

Internet Group Management Protocol (IGMP) is a protocol used by IPv4 systems to report IP multicast group memberships to neighboring multicast routers. On networks with hosts directly attached, IGMP Version 3 (IGMPv3) 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 source(s) 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, IGMPv3 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(3)T, hosts must explicitly include sources when joining a multicast group (this is known as “channel subscription”). IGMPv3 is the industry-designated standard protocol for hosts to signal channel subscriptions in SSM. In deployment cases where IGMPv3 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 v3lite. Both of these features were introduced with SSM in Cisco IOS Release 12.1(3)T.

Inter-Autonomous Systems MPLS VPN Support

The Inter-Autonomous Systems for MPLS VPN feature module explains how to provide MPLS VPN services that can span multiple autonomous systems (ASs) and VPN service providers. 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 IPv4 network layer reachability information (NLRI) in the form of VPN-IPv4 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-IPv4 prefixes throughout each VPN and each autonomous system.

Configuring an IP over CLNS tunnel (CTunnel) allows you to telnet to a remote router that has only CLNS connectivity. Other management facilities can also be used, such as SNMP, TFTP, and so on, which otherwise would not be available over a CLNS network.

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

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 for NetMeeting Directory (Internet Locator Service—ILS)

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.

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

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

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.

NTP MIB

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 Connection Online at <http://www.cisco.com/public/mibs/v2/>).

Parser Cache

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

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 Over IEEE 802.1Q VLANs

The PPPoE Over IEEE 802.1Q VLANs feature adds support for running PPP over ethernet over IEEE 802.1Q virtual local area networks (VLANs). IEEE 802.1Q is used to interconnect a VLAN-capable router with another VLAN-capable device. The packets on the 802.1Q link contain a standard (fast) Ethernet frame and the VLAN information associated with that frame. PPPoE Radius Port Identification.

PPPoE RADIUS Port Identification

This feature adds RADIUS port identification information when using point to point protocol over Ethernet (PPPoE) over ATM, Ethernet, and 802.1Q VLANs.

SDLC SNRM Timer and Window Size

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.

New Software Features in Release 12.1(3)T

The following new software features are supported by the Cisco 4000 series for Cisco IOS Release 12.1(3)T.

Bridging between IEEE 802.1Q vLANs

This feature supports integrated routing and bridging, transparent bridging, and PVST+ between vLANs (virtual LANs) with IEEE 802.1Q encapsulation features. It 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)—connectivity for multiple VLANs using a Bridge-Group Virtual Interface (BVI) to associate a bridge group.
- Transparent bridging (TB)—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—support for Dot1q trunks to map multiple spanning trees to a single spanning tree.

CEF Support for IP Routing between IEEE 802.1Q vLANs

The CEF Support for IP Routing between IEEE 802.1Q vLANs feature provides the support needed for a CEF feature module.

Event MIB

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 Management Information Base (MIB) objects on a local or remote system using SNMP and initiate simple actions whenever a trigger condition is met (for example, an SNMP trap can be generated when an object is modified). By allowing notifications based on events, the Network Management System (NMS) does not need to constantly poll managed devices to find out if something has changed. When combined with the Expression MIB support introduced in Cisco IOS Release 12.0(5)T, Event MIB support in Cisco IOS software provides a flexible and efficient way to monitor complex conditions on network devices.

PPP Over ATM SVC

PPP over ATM SVC implements standards-based PPP over ATM AAL5.

Frame Relay ELMI Address Registration (CSCdp36027)

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, NMS could detect only the topology of routers or the topology of switches. This new 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.

Secure Shell Version 1 Integrated Client

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 allows for a secure communication over an insecure network.

The SSH client in Cisco IOS will work with publicly and commercially available SSH servers. The SSH client supports DES, 3DES, and password authentication.

HSRP Support for ICMP Redirect Messages (CSCdp37610)

The HSRP (Hot Standby Router Protocol) Support for ICMP Redirect Message feature enables ICMP redirects on interfaces configured with HSRP. This functionality works by filtering outgoing ICMP redirect messages through HSRP, where the next-hop IP address may be changed to an HSRP virtual IP address.

Individual SNMP Trap Support (CSCdp97172)

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.

SNMP Support for IOS vLAN Subinterfaces (CSCdk25367)

This enhancement provides sparse table support for fastethernet subinterfaces similar to what is currently provided for frame-relay subinterfaces.

New Software Features in Release 12.1(2)T

The following new software features are supported by the Cisco 4000 series for Cisco IOS Release 12.1(2)T.

AAA Server Group Deadtimer

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

With the introduction of this feature, deadtime 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

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 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.

COPS for RSVP

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 videoconferencing 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

In so doing, COPS for RSVP supports the following crucial RSVP features:

- Admission control—The RSVP reservation is accepted or rejected based on *end-to-end* available network resources.
- Bandwidth guarantee—The RSVP reservation, if accepted, will guarantee that those reserved resources will continue to be available while the reservation is in place.
- Media-independent reservation—An end-to-end RSVP reservation can span arbitrary lower layer media types.
- Data classification—While a reservation is in place, data packets belonging to that RSVP flow are separated from other packets and forwarded as part of the reserved flow.
- Data policing—Data packets belonging to an RSVP flow that exceed the reserved bandwidth size are marked with a lower packet precedence.

Frame Relay Switching Enhancements

You can now configure frame relay (FR) traffic shaping on switched PVCs. By applying traffic shaping to switched PVCs you enable a router to be used as a FR port concentrator in front of an FR switch. The FR switch will shape the concentrated traffic before sending it into the FR network.

OSPF Flooding Reduction

The explosive growth of the Internet has placed the focus on the scalability of Interior Gateway Protocols such as OSPF. 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 sec. Some implementations have tried to improve the flooding by reducing the frequency to refresh from 30 min to around 50 min or so. 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 Do Not Age (DNA) LSAs.

New Hardware Features in Release 12.1(1)T

There are no new hardware features supported by the Cisco 4000 series in Cisco IOS Release 12.1(1)T.

New Software Features in Release 12.1(1)T

The following new software features are supported by the Cisco 4000 series for Cisco IOS Release 12.1(1)T.

Express RTP and TCP Header Compression

Before Cisco IOS Release 12.0(7)T, if compression of TCP or Real-Time Transport Protocol (RTP) headers was enabled, 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 process to be switched. This procedure slowed down transmission of the packet, and therefore some users preferred to fast switch uncompressed TCP and RTP packets.

Now, if TCP or RTP header compression is enabled, it occurs by default in the fast-switched path or the Cisco Express Forwarding-switched (CEF-switched) path, depending on which switching method is enabled on the interface. Furthermore, the number of TCP and RTP header compression connections was increased to 1000 connections each.

If neither fast switching nor CEF switching is enabled, then if TCP or RTP header compression is enabled, it will occur in the process-switched path as before.

PPP over Ethernet for ATM

The Point-to-Point Protocol over Ethernet (PPPoE) for 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 done 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.

Pragmatic General Multicast

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 can detect unrecoverable data packet loss. PGM is intended 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” part of the *Cisco IOS IP and IP Routing Configuration Guide* for information about the PGM Router Assist feature.

Service Assurance Agent

The Service Assurance (SA) Agent is an both an enhancement to and a new name for the Response Time Reporter (RTR) feature that was introduced in Cisco IOS Release 11.2. The feature allows you to 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. This feature enables you to perform troubleshooting, problem analysis, and notification based on the statistics collected by the SA Agent.

The SA Agent Enhancements 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 that enable you to:

- 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.

Important Notes

This section contains important information about the use of your Cisco IOS Release 12.1(5)T software.

CSCdr91706 and Cisco 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 Cisco 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 Cisco 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.

This section contains important information about use of your Cisco IOS Release 12.1(5)T software.

The last maintenance release of the Cisco IOS Release 12.0T release train is 12.0(7)T. The migration path for customers needing bug fixes for Cisco IOS Release 12.0 T features is 12.1 Mainline. Cisco IOS Release 12.1 Mainline has the complete feature content of 12.0T and this release will eventually reach General Deployment (GD).

Cisco IOS Release 12.1 T begins with the same set of features as the Cisco IOS Release 12.1 mainline but will continue to add features.

Limitations and Restrictions

Deprecated MIBs

Old Cisco Management Information Bases (MIBs) will be replaced in a future release. OLD-CISCO-* MIBs are currently migrated 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 6.

Table 6 *Deprecated and Replacement MIBs*

Deprecated MIB	Replacement
OLD-CISCO-APPLETALK-MIB	RFC1243-MIB
OLD-CISCO-CHASSIS-MIB	ENTITY-MIB
OLD-CISCO-CPUK-MIB	In Development
OLD-CISCO-DECNET-MIB	In Development
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	In Development
OLD-CISCO-MEMORY-MIB	CISCO-MEMORY-POOL-MIB
OLD-CISCO-NOVELL-MIB	NOVELL-IPX-MIB
OLD-CISCO-SYS-MIB	(Compilation of other OLD* MIBS)
OLD-CISCO-SYSTEM-MIB	CISCO-CONFIG-COPY-MIB
OLD-CISCO-TCP-MIB	CISCO-TCP-MIB
OLD-CISCO-TS-MIB	In Development
OLD-CISCO-VINES-MIB	CISCO-VINES-MIB
OLD-CISCO-XNS-MIB	In Development

Caveats

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

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

All caveats in Cisco IOS 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 CCO and the Documentation CD-ROM.



Note

If you have an account with CCO, you can use Bug Navigator II to find caveats of any severity for any release. You can reach Bug Navigator II on CCO at: **Software Center: Cisco IOS Software: Cisco Bug Toolkit: Cisco Bugtool Navigator II** or at <http://www.cisco.com/support/bugtools>.

Related Documentation

The following sections describe the documentation available for Cisco 4000 series 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.

Use these release notes with these documents:

- Release-Specific Documents, page 26
- Platform-Specific Documents, page 27
- Feature Modules, page 27
- Cisco IOS Software Documentation Set, page 28

Release-Specific Documents

The following documents are specific to Release 12.1(5)T and are located on CCO and the Documentation CD-ROM:

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

On CCO 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 for Cisco IOS Release 12.1

- Product bulletins, field notices, and other release-specific documents on CCO 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 Release 12.1 and Release 12.1 T.

On CCO at:

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

On the Documentation CD-ROM at:

Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS 12.1: Caveats: Caveats for Cisco IOS Release 12.1



Note

If you have an account with CCO, you can use Bug Navigator II to find caveats of any severity for any release. You can reach Bug Navigator II on CCO at: **Software Center: Cisco IOS Software: Cisco Bug Toolkit: Cisco Bugtool Navigator II** or at <http://www.cisco.com/support/bugtools>.

Platform-Specific Documents

These documents are available for the Cisco 4000 series on CCO and the Documentation CD-ROM:

- Cisco 4000 Series hardware installation and maintenance documents
- *Cisco 4000 Series Configuration Notes*
- *Cisco 4000 Series Regulatory Compliance and Safety Information*
- *Redundant Power Systems*
- *Release Notes for Cisco 4000 Series Routers*

On CCO at:

Technical Documents: Documentation Home Page: Cisco Product Documentation: Access Servers and Access Routers: Modular Access Routers: Cisco 4000 Series Routers

On the Documentation CD-ROM at:

Cisco Product Documentation: Access Servers and Access Routers: Modular Access Routers: Cisco 4000 Series Routers

Feature Modules

Feature modules describe new features supported by Release 12.1(3)T and are an update 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 on CCO or the documentation CD-ROM. The feature module information is incorporated in the next printing of the Cisco IOS documentation set.

On CCO:

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

On the Documentation CD-ROM:

Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 12.1: New Feature Documentation: New Features in Release 12.1

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 ordered 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, and Cisco IOS software functionality and contain comprehensive configuration examples. Chapters in a command reference provide complete command syntax information. You can use each configuration guide in conjunction with its corresponding command reference.

On CCO and the Documentation CD-ROM, two master hot-linked documents provide information for the Cisco IOS software documentation set.

On CCO 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:

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

Release 12.1 Documentation Set

Table 7 describes the contents of the Cisco IOS Release 12.1 software documentation set, which is available in electronic form, and also in printed form upon request.



Note

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

On CCO 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 7 Cisco IOS Release 12.1 Documentation Set

Books	Major Topics
<ul style="list-style-type: none"> • <i>Cisco IOS Configuration Fundamentals Configuration Guide</i> • <i>Cisco IOS Configuration Fundamentals Command Reference</i> 	Configuration Fundamentals Overview Cisco IOS User Interfaces Configuration Files File Management System Management
<ul style="list-style-type: none"> • <i>Cisco IOS Bridging and IBM Networking Configuration Guide</i> • <i>Cisco IOS Bridging and IBM Networking Command Reference, Volume I</i> • <i>Cisco IOS Bridging and IBM Networking Command Reference, Volume II</i> 	Transparent Bridging Source-Route Bridging Token Ring Inter-Switch Link Remote Source-Route Bridging DLSw+ Serial Tunnel and Block Serial Tunnel Commands LLC2 and SDLC Commands IBM Network Media Translation Commands SNA Frame Relay Access Support Commands NCIA Client/Server Commands Airline Product Set Commands
<ul style="list-style-type: none"> • <i>Cisco IOS Dial Services Configuration Guide: Terminal Services</i> • <i>Cisco IOS Dial Services Configuration Guide: Network Services</i> • <i>Cisco IOS Dial Services Command Reference</i> 	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 Dial Access Scenarios
<ul style="list-style-type: none"> • <i>Cisco IOS Interface Configuration Guide</i> • <i>Cisco IOS Interface Command Reference</i> 	Interface Configuration Overview Configuring LAN Interfaces Configuring Serial Interfaces Configuring Logical Interfaces
<ul style="list-style-type: none"> • <i>Cisco IOS IP and IP Routing Configuration Guide</i> • <i>Cisco IOS IP and IP Routing Command Reference</i> 	IP Overview IP Addressing and Services IP Routing Protocols IP Multicast
<ul style="list-style-type: none"> • <i>Cisco IOS AppleTalk and Novell IPX Configuration Guide</i> • <i>Cisco IOS AppleTalk and Novell IPX Command Reference</i> 	AppleTalk and Novell IPX Overview Configuring AppleTalk Configuring Novell IPX

Table 7 Cisco IOS Release 12.1 Documentation Set (continued)

Books	Major Topics
<ul style="list-style-type: none"> • <i>Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS, and XNS Configuration Guide</i> • <i>Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS, and XNS Command Reference</i> 	<ul style="list-style-type: none"> Overview Configuring Apollo Domain Configuring Banyan VINES Configuring DECnet Configuring ISO CLNS Configuring XNS
<ul style="list-style-type: none"> • <i>Cisco IOS Multiservice Applications Configuration Guide</i> • <i>Cisco IOS Multiservice Applications Command Reference</i> 	<ul style="list-style-type: none"> Multiservice Applications Overview Voice Video Broadband
<ul style="list-style-type: none"> • <i>Cisco IOS Quality of Service Solutions Configuration Guide</i> • <i>Cisco IOS Quality of Service Solutions Command Reference</i> 	<ul style="list-style-type: none"> 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"> • <i>Cisco IOS Security Configuration Guide</i> • <i>Cisco IOS Security Command Reference</i> 	<ul style="list-style-type: none"> Security Overview Authentication, Authorization, and Accounting (AAA) Security Server Protocols Traffic Filtering and Firewalls IP Security and Encryption Configuring Passwords and Privileges Neighbor Router Authentication: Configuring IP Security Options
<ul style="list-style-type: none"> • <i>Cisco IOS Switching Services Configuration Guide</i> • <i>Cisco IOS Switching Services Command Reference</i> 	<ul style="list-style-type: none"> Cisco IOS Switching Services Overview Cisco IOS Switching Paths Cisco Express Forwarding NetFlow Switching MPLS Switching Multilayer Switching Multicast Distributed Switching Virtual LANs

Table 7 Cisco IOS Release 12.1 Documentation Set (continued)

Books	Major Topics
<ul style="list-style-type: none"> • <i>Cisco IOS Wide-Area Networking Configuration Guide</i> • <i>Cisco IOS Wide-Area Networking Command Reference</i> 	Introduction: Wide-Area Networking Overview Configuring ATM Configuring Frame Relay Configuring Frame Relay-ATM Interworking Configuring SMDS Configuring X.25 and LAPB
<ul style="list-style-type: none"> • <i>Cisco IOS Software Command Summary</i> • <i>Cisco IOS Dial Services Quick Configuration Guide</i> • <i>Cisco IOS Configuration Guide Master Index</i> • <i>Cisco IOS Command Reference Master Index</i> • <i>Cisco IOS New Features Index</i> • <i>Cisco IOS Debug Command Reference</i> • <i>Cisco IOS System Error Messages</i> 	

**Note**

Cisco Management Information Base (MIB) User Quick Reference is no longer published. For the latest list of MIBs supported by Cisco, see *Cisco Network Management Toolkit* on Cisco Connection Online. From CCO, click on the following path: **Software Center: Network Mgmt Products: Cisco Network Management Toolkit: Cisco MIB.**

Obtaining Documentation

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at <http://www.cisco.com>. Translated documentation can be accessed at http://www.cisco.com/public/countries_languages.shtm.

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. Therefore, it is probably more current than printed documentation. The CD-ROM package is available as a single unit or as an annual subscription.

Ordering Documentation

Registered CCO users can order the Documentation CD-ROM and other Cisco Product documentation through our online Subscription Services at <http://www.cisco.com/cgi-bin/subcat/kaojump.cgi>.

Nonregistered CCO users can order documentation through a local account representative by calling Cisco's corporate headquarters (California, USA) at 408 526-4000 or, in North America, call 800 553-NETS (6387).

Obtaining Technical Assistance

Cisco provides Cisco Connection Online (CCO) as a starting point for all technical assistance. Warranty or maintenance contract customers can use the Technical Assistance Center. All customers can submit technical feedback on Cisco documentation using the Web, e-mail, a self-addressed stamped response card included in many printed docs, or by sending mail to Cisco.

Cisco Connection Online

Cisco continues to revolutionize how business is done on the Internet. Cisco Connection Online 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.

CCO's broad range of features and services helps customers and partners to streamline business processes and improve productivity. Through CCO, you will find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online support services, 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 CCO to obtain additional personalized information and services. Registered users may order products, check on the status of an order and view benefits specific to their relationships with Cisco.

You can access CCO in the following ways:

- WWW: www.cisco.com
- Telnet: [cco.cisco.com](telnet://cco.cisco.com)
- Modem using standard connection rates and the following terminal settings: VT100 emulation; 8 data bits; no parity; and 1 stop bit.
 - From North America, call 408 526-8070
 - From Europe, call 33 1 64 46 40 82

You can e-mail questions about using CCO to cco-team@cisco.com.

Technical Assistance Center

The Cisco Technical Assistance Center (TAC) is available to warranty or maintenance contract customers who need technical assistance with a Cisco product that is under warranty or covered by a maintenance contract.

To display the TAC web site that includes links to technical support information and software upgrades and for requesting TAC support, use www.cisco.com/techsupport.

To contact the TAC by e-mail, use one of the following:

Language	E-mail Address
English	tac@cisco.com
Hanzi (Chinese)	chinese-tac@cisco.com
Kanji (Japanese)	japan-tac@cisco.com
Hangul (Korean)	korea-tac@cisco.com
Spanish	tac@cisco.com
Thai	thai-tac@cisco.com

In North America, TAC can be reached at 800 553-2447 or 408 526-7209. For other telephone numbers and TAC e-mail addresses worldwide, consult the following web site:
<http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml>.

Software Configuration Tips on the Cisco Technical Assistance Center Home Page

If you have a CCO login account, you can access the following URL, which contains links and tips on configuring your Cisco products:

http://www.cisco.com/kobayashi/technotes/serv_tips.shtml

This URL is subject to change without notice. If it changes, point your Web browser to CCO and click on this path: **Technical Assistance Center: Technical Tips**. (You must have a CCO account to access this link.)

The following sections are provided from the Technical Tips page:

- Access Dial Cookbook—Contains common configurations or recipes for configuring various access routes and dial technologies.
- Field Notices—Notifies you of any critical issues regarding Cisco products and includes problem descriptions, safety or security issues, and hardware defects.
- Frequently Asked Questions—Describes the most frequently asked technical questions about Cisco hardware and software.
- Hardware—Provides technical tips related to specific hardware platforms.
- Hot Tips—Describes popular tips and hints gathered from the Cisco Technical Assistance Center (TAC). Most of these documents are available from the TAC Fax-on-demand service. To reach Fax-on-demand and receive documents at your fax machine from the United States, call 888 50-CISCO (888 502-4726). From other areas, call 650 596-4408.
- Internetworking Features—Lists tips on using and deploying Cisco IOS software features and services.
- Sample Configurations—Provides actual configuration examples that are complete with topology and annotations.

- Software Products—Contains Cisco IOS Software Bulletins, Cisco TCP/IP Suite 100, General Cisco IOS, Internet/Intranet Applications and Software, Network Management, Network Protection Software Tips, and WAN Switching Products and Software.
- Special Collections—Lists other helpful documents, including *Case Studies*, *References & Request for Comments (RFCs)*, and *Security Advisories*.

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.

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 and value your comments.

This document is to be used with the documents listed in the “Related Documentation” section on page 26.

Access Registrar, AccessPath, Are You Ready, ATM Director, Browse with Me, CCDA, CCDE, CCDP, 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.