



Text Part Number: 78-6137-06

Release Notes for Cisco 4000 Series for Cisco IOS Release 12.0 T

December 13, 1999

These release notes for the Cisco AS4000 series support Cisco IOS Release 12.0 T, up to and including Release 12.0(7)T. These release notes are updated as needed to describe new features, memory requirements, hardware support, software platform deferrals, and changes to the microcode or modem code and related documents.

For a list of software caveats that apply to Release 12.0(7)T, see *Caveats for Cisco IOS Release 12.0 T* that accompanies these release notes. This caveats document is updated for every maintenance release and is located on Cisco Connection Online (CCO) and the Documentation CD-ROM.

Use these release notes with *Cross-Platform Release Notes for Cisco IOS Release 12.0* on CCO and the Documentation CD-ROM.

Contents

These release notes describe the following topics:

- System Requirements, page 2
- New and Changed Information, page 16
- Limitations and Restrictions, page 34
- Important Notes, page 34
- Caveats, page 35
- Related Documentation, page 35
- Service and Support, page 40
- Cisco Connection Online, page 41
- Documentation CD-ROM, page 42

Corporate Headquarters

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

Copyright © 1998–1999
Cisco Systems, Inc.
All rights reserved.

System Requirements

This section describes the system requirements for Release 12.0 T:

- Memory Requirements, page 2
- Hardware Supported, page 3
- Determining the Software Version, page 4
- Upgrading to a New Software Release, page 4
- Feature Set Tables, page 5

Memory Requirements

Table 1 Memory Requirements for the Cisco 4000 Series

Feature Set by Platform		Image Name	Minimum Flash Memory	Minimum DRAM Memory	Runs From	In ¹
Cisco 4000 and Cisco 4000-M	IP	c4000-i-mz	4 MB	16 MB	RAM	
	IP Plus	c4000-is-mz	8 MB	16 MB	RAM	
	IP Plus 40	c4000-is40-mz	8 MB	16 MB	RAM	
	IP Plus IPsec 56	c4000-is56i-mz	8 MB	16 MB	RAM	
	IP Plus IPsec 3DES	c4000-ik2s-mz	8 MB	16 MB	RAM	(2)
	IP/IPX/AT/DEC	c4000-d-mz	8 MB	16 MB	RAM	
	IP/IPX/AT/DEC Plus	c4000-ds-mz	8 MB	16 MB	RAM	
	Enterprise Plus	c4000-js-mz	8 MB	32 MB	RAM	
	Enterprise Plus IPsec 56	c4000-js56i-mz	8 MB	32 MB	RAM	
	Enterprise Plus IPsec 3DES	c4000-jk2s-mz	8 MB	32 MB	RAM	(2)
	Enterprise/SNSAw Plus	c4000-a3js-mz	8 MB	32 MB	RAM	(7)
	Enterprise/SNSAw Plus IPsec 56	c4000-a3js56i-mz	8 MB	32 MB	RAM	(7)
	Enterprise/SNSAw Plus IPsec 3DES	c4000-a3jk2s-mz	8 MB	32 MB	RAM	(7)

Table 1 Memory Requirements for the Cisco 4000 Series (continued)

Feature Set by Platform		Image Name	Minimum Flash Memory	Minimum DRAM Memory	Runs From	In ¹
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 40	c4500-is40-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	(2)
	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	8 MB	32 MB	RAM	
	Enterprise Plus IPsec 56	c4500-js56i-mz	8 MB	32 MB	RAM	
	Enterprise Plus IPsec 3DES	c4500-jk2s-mz	8 MB	32 MB	RAM	(2)
	Enterprise/SNSAw Plus	c4500-a3js-mz	16 MB	32 MB	RAM	(7)
	Enterprise/SNSAw Plus IPsec 56	c4500-a3js56i-mz	16 MB	32 MB	RAM	(7)
Enterprise/SNSAw Plus IPsec 3DES	c4500-a3jk2s-mz	16 MB	32 MB	RAM	(7)	
Cisco 4700-M	DistributedDirector	c4500-w3-mz	16 MB	32 MB	RAM	(7)

¹ This column indicates which maintenance release the image was introduced. For example, (2) indicates the image was introduced in Cisco IOS Release 12.0(2)T, and so forth. If no number is in this column, the image was introduced in the initial release.

Hardware Supported

Cisco IOS Release 12.0 T supports the Cisco 4000 series routers:

- Cisco 4000, Cisco 4000-M
- Cisco 4500, Cisco 4500-M
- Cisco 4700, Cisco 4700-M

Table 2 Supported Interfaces

Interface, Network Module, or Data Rate	Platforms Supported	
LAN Interfaces	ATM Interface	All Cisco 4000 series platforms
	Ethernet	All Cisco 4000 series platforms
	Fast Ethernet	Cisco 4500 and Cisco 4700
	Token Ring	All Cisco 4000 series platforms
	FDDI	All Cisco 4000 series platforms
	Serial	All Cisco 4000 series platforms
	HSSI	Cisco 4500 and Cisco 4700
	ISDN BRI	All Cisco 4000 series platforms
	Channelized E1/T1 ISDN PRI	All Cisco 4000 series platforms

Table 2 Supported Interfaces (continued)

LAN Interfaces (continued)	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	All Cisco 4000 series platforms
	1.544/2.048 Mbps	All Cisco 4000 series platforms
WAN Interfaces and Network Modules	56K/64K DSU/CSU	All Cisco 4000 series platforms
	Channelized E1	All Cisco 4000 series platforms
	Channelized T1	All Cisco 4000 series platforms
	E1-G.703/G.704	All Cisco 4000 series platforms
	EIA/TIA-232	All Cisco 4000 series platforms
	EIA/TIA-449	All Cisco 4000 series platforms
	EIA/TIA-613 (HSSI)	All Cisco 4000 series platforms
	EIA-530	All Cisco 4000 series platforms
	ISDN BRI	All Cisco 4000 series platforms
	ISDN PRI	All Cisco 4000 series platforms
	MultiChannel Interface (Channelized E1/T1)	All Cisco 4000 series platforms
	Serial	All Cisco 4000 series platforms
	V.35	All Cisco 4000 series platforms
X.21	All Cisco 4000 series platforms	

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) 4000 Software (C4000-JS-MZ), Version 12.0(7)T, RELEASE SOFTWARE
```

Upgrading to a New Software Release

For information on upgrading to a new software release, see the product bulletin *Cisco IOS Software Release 12.0 T Upgrade Paths and Packaging Simplification (#819: 1/99)* on CCO at:

Technical Documents: Product Bulletins: Software

Under **Cisco IOS 12.0**, click **Cisco IOS Software Release 12.0 T Upgrade (#819: 1/99)**.

Feature Set Tables

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.

Table 3 Feature Sets Supported by the Cisco 4000 Series

Feature Set		Feature Set Matrix Term	Software Image	Platforms Supported	In ¹
IP Standard Feature Sets	IP	Basic ²	c4000-i-mz	Cisco 4000/4000-M	
			c4500-i-mz	Cisco 4500/4500-M, Cisco 4700/4700-M	
	IP Plus	Plus ³	c4000-is-mz	Cisco 4000/4000-M	
			c4500-is-mz	Cisco 4500/4500-M, Cisco 4700/4700-M	
	IP Plus 40	Plus, Plus 40 ⁴	c4000-is40-mz	Cisco 4000/4000-M	
			c4500-is40-mz	Cisco 4500/4500-M, Cisco 4700/4700-M	
	IP Plus IPsec 56	Plus, Plus IPsec 56 ⁵	c4000-is56i-mz	Cisco 4000, Cisco 4000-M	
			c4500-is56i-mz	Cisco 4500/4500-M, Cisco 4700/4700-M	
	IP Plus IPsec 3DES	Plus, Plus IPsec, 3DES ⁶	c4000-ik2s-mz	Cisco 4000, Cisco 4000-M	(2)
			c4500-ik2s-mz	Cisco 4500/4500-M, Cisco 4700/4700-M	
IP/IPX/Apple Talk/DEC Standard Feature Sets	IP/IPX/AppleTalk/DEC	Basic	c4000-d-mz,	Cisco 4000/4000-M	
			c4500-d-mz	Cisco 4500/4500-M, Cisco 4700/4700-M	
	IP/IPX/AppleTalk/DEC Plus	Plus	c4000-ds-mz	Cisco 4000/4000-M	
			c4500-ds-mz	Cisco 4500/4500-M, Cisco 4700/4700-M	
Enterprise Standard Feature Sets	Enterprise Plus	Plus	c4000-js-mz	Cisco 4000/4000-M	
			c4500-js-mz	Cisco 4500/4500-M, Cisco 4700/4700-M	
	Enterprise Plus IPsec 56	Plus, Plus IPsec 56	c4000-js56i-mz	Cisco 4000/4000-M	
			c4500-js56i-mz	Cisco 4500/4500-M, Cisco 4700/4700-M	
	Enterprise Plus IPsec 3DES	Plus, Plus IPsec 56, 3DES	c4000-jk2s-mz	Cisco 4000/4000-M	(2)
			c4500-jk2s-mz	Cisco 4500/4500-M, Cisco 4700/4700-M	
Enterprise/SNSAw Standard Feature Set	Enterprise/SNSAw Plus	Plus	c4000-a3js-mz	Cisco 4000/4000-M	(7)
			c4500-a3js-mz	Cisco 4500/4500-M, Cisco 4700/4700-M	(7)
	Enterprise/SNSAw Plus IPsec 56	Plus, Plus IPsec 56	c4000-a3js56i-mz	Cisco 4000/4000-M	(7)
			c4500-a3js56i-mz	Cisco 4500/4500-M, Cisco 4700/4700-M	(7)
	Enterprise/SNSAw Plus IPsec 3DES	Plus, Plus IPsec, 3DES	c4000-a3jk2s-mz	Cisco 4000/4000-M	(7)
			c4500-a3jk2s-mz	Cisco 4500/4500-M, Cisco 4700/4700-M	(7)
Distributed-Director Standard Feature Set	DistributedDirector	Distributed-Director	c4500-w3-mz	Cisco 4700-M	(7)

1 This column indicates which maintenance release the image was introduced. For example, (2) indicates the image was introduced in Cisco IOS Release 12.0(2)T. If this column is blank, the image was introduced in the initial release.

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

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

4 This feature set is offered in the encryption feature sets which consist of 40-bit (Plus 40) data encryption feature sets.

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

6 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.

Tables 4 and 5 list the features and feature sets supported by the Cisco IOS Release 12.0 T for the Cisco 4000 and 4000-M.

Tables 6 and 7 list the features and feature sets supported by the Cisco IOS Release 12.0 T for the Cisco 4500, 4500-M, 4700, and 4700-M.

All the 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 4000 and 4000-M—Part 1 of 2

Features	Feature Sets						
	IP	IP Plus	IP Plus 40	IP Plus IPsec 56	IP Plus IPsec 3DES ¹	IP/IPX/AT/DEC	IP/IPX/AT/DEC Plus
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
RIP Enhancements	Yes	Yes	Yes	Yes	Yes	Yes	Yes
IBM Support							
DLSw+ Ethernet Redundancy	Yes	Yes	Yes	Yes	Yes	Yes	Yes
DLSW RSVP	Yes	Yes	Yes	Yes	Yes	No	Yes
IP Routing							
Airline Product Set	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
Multicast Routing Monitor	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Table 4 Feature List by Feature Set for the Cisco 4000 and 4000-M—Part 1 of 2 (continued)

Features	Feature Sets						
	IP	IP Plus	IP Plus 40	IP Plus IPsec 56	IP Plus IPsec 3DES ¹	IP/IPX/AT/DEC	IP/IPX/AT/DEC 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							
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
Process MIB	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Service Assurance Agent (formerly Response Time Reporter)	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
Lane Fast SSRP	No	Yes	Yes	Yes	Yes	No	Yes
Security							
X.25 Closed User Groups	No	Yes	Yes	Yes	Yes	No	Yes
Switching							
Cisco IOS STP Enhancements	No	Yes	Yes	Yes	Yes	No	Yes
MPLS Traffic Engineering	No	No	No	No	No	No	No
SNA Switching Services	No	No	No	No	No	No	No
X.25 Switch Local Acknowledgement	No	Yes	Yes	Yes	Yes	No	Yes

System Requirements

Table 4 Feature List by Feature Set for the Cisco 4000 and 4000-M—Part 1 of 2 (continued)

Features	Feature Sets						
	IP	IP Plus	IP Plus 40	IP Plus IPsec 56	IP Plus IPsec 3DES ¹	IP/IPX/ AT/DEC	IP/IPX/ AT/DEC Plus
WAN Services							
Annex G	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Cisco IOS IEEE 802.1Q	Yes	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
Mobile IP	No	Yes	Yes	Yes	Yes	No	Yes
PPP over Frame Relay	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Time-Based Access List	Yes	Yes	Yes	Yes	Yes	Yes	Yes

¹ This image was introduced in Cisco IOS Release 12.0(2)T.

Table 5 Feature List by Feature Set for the Cisco 4000 and 4000-M—Part 2 of 2

Features	Enterprise Plus	Enterprise Plus IPsec 56	Enterprise Plus IPsec 3DES ¹	Enterprise/ SNASw Plus ²	Enterprise/ SNASw Plus IPsec 56 ²	Enterprise /SNASw Plus IPsec 3DES ²
Connectivity						
Layer 2 Tunnel Protocol (L2TP)	Yes	Yes	Yes	Yes	Yes	Yes
L2TP Dial Out	Yes	Yes	Yes	Yes	Yes	Yes
Multicast Source Discovery Protocol	Yes	Yes	Yes	Yes	Yes	Yes
RIP Enhancements	Yes	Yes	Yes	Yes	Yes	Yes
IBM Support						
DLSw+ Ethernet Redundancy	Yes	Yes	Yes	Yes	Yes	Yes
DLSW RSVP	Yes	Yes	Yes	Yes	Yes	Yes
IP Routing						
Airline Product Set	Yes	Yes	Yes	Yes	Yes	Yes
DNS for X.25	Yes	Yes	Yes	Yes	Yes	Yes
Easy IP Phase 2-DHCP Server	Yes	Yes	Yes	Yes	Yes	Yes
Flow WRED	Yes	Yes	Yes	Yes	Yes	Yes

Table 5 Feature List by Feature Set for the Cisco 4000 and 4000-M—Part 2 of 2 (continued)

Features	Enterprise Plus	Enterprise Plus IPsec 56	Enterprise Plus IPsec 3DES¹	Enterprise/SNASw Plus²	Enterprise/SNASw Plus IPsec 56²	Enterprise/SNASw Plus IPsec 3DES²
Multicast Routing Monitor	Yes	Yes	Yes	Yes	Yes	Yes
OSPF Packet Pacing	Yes	Yes	Yes	Yes	Yes	Yes
PGM Router Assist	Yes	Yes	Yes	Yes	Yes	Yes
WPPC	Yes	Yes	Yes	Yes	Yes	Yes
X.25 Load Balancing	Yes	Yes	Yes	Yes	Yes	Yes
X.25 Remote Failure Detection	Yes	Yes	Yes	Yes	Yes	Yes
Management						
CNS Client for Cisco IOS Software	Yes	Yes	Yes	Yes	Yes	Yes
CNS Client for Cisco IOS (IPsec Policy Agent II)	Yes	Yes	Yes	Yes	Yes	Yes
ISDN MIB RFC 2127	Yes	Yes	Yes	Yes	Yes	Yes
Process MIB	Yes	Yes	Yes	Yes	Yes	Yes
Service Assurance Agent (formerly Response Time Reporter)	Yes	Yes	Yes	Yes	Yes	Yes
SNMPv3	Yes	Yes	Yes	Yes	Yes	Yes
Subnetwork Bandwidth Manager	Yes	Yes	Yes	Yes	Yes	Yes
Quality of Service						
CLI String Search	Yes	Yes	Yes	Yes	Yes	Yes
Lane Fast SSRP	Yes	Yes	Yes	Yes	Yes	Yes
Security						
X.25 Closed User Groups	No	Yes	Yes	Yes	Yes	Yes
Switching						
Cisco IOS STP Enhancements	No	Yes	Yes	Yes	Yes	No
MPLS Traffic Engineering	Yes	Yes	Yes	Yes	Yes	Yes
SNA Switching Services	No	No	No	Yes	Yes	Yes

System Requirements

Table 5 Feature List by Feature Set for the Cisco 4000 and 4000-M—Part 2 of 2 (continued)

Features	Enterprise Plus	Enterprise Plus IPsec 56	Enterprise Plus IPsec 3DES ¹	Enterprise/SNASw Plus ²	Enterprise/SNASw Plus IPsec 56 ²	Enterprise/SNASw Plus IPsec 3DES ²
X.25 Switch Local Acknowledgement	Yes	Yes	Yes	Yes	Yes	Yes
WAN Services						
Annex G	Yes	Yes	Yes	Yes	Yes	Yes
Cisco IOS IEEE 802.1Q	Yes	Yes	Yes	Yes	Yes	Yes
Dynamic Multiple Encapsulation for Dial-in over ISDN	Yes	Yes	Yes	Yes	Yes	Yes
Frame Relay End to End Keepalive	Yes	Yes	Yes	Yes	Yes	Yes
Mobile IP	Yes	Yes	Yes	Yes	Yes	Yes
PPP over Frame Relay	Yes	Yes	Yes	Yes	Yes	Yes
Time-Based Access List	Yes	Yes	Yes	Yes	Yes	Yes

1 This image was introduced in Cisco IOS Release 12.0(2)T.

2 This image was introduced in Cisco IOS Release 12.0(7)T.

Table 6 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 ¹	IP/IPX/AT/DEC	IP/IPX/AT/DEC Plus
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
RIP Enhancements	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Ease of Use							
Interface MIB Implementation for ATM Supinterfaces ²	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

Table 6 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 ¹	IP/IPX/AT/DEC	IP/IPX/AT/DEC Plus
IP/IPX Routing							
Airline Product Set	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 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							
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 (formerly Response Time Reporter)	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
LANE Fast SSRP	No	Yes	Yes	Yes	Yes	No	Yes
MPLS VPN	No	No	No	No	No	No	No

System Requirements

Table 6 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 ¹	IP/IPX/AT/DEC	IP/IPX/AT/DEC Plus
MPLS Class of Service	No	No	No	No	No	No	No
Scalability							
IETF-Compliant PPP over ATM Scalability	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Security							
X.25 Closed User Groups	No	Yes	Yes	Yes	Yes	No	Yes
Switching							
Cisco IOS STP Enhancements	No	Yes	Yes	Yes	Yes	No	Yes
Express RTP and TCP Header Compression	Yes	Yes	Yes	Yes	Yes	No	No
MPLS Traffic Engineering	No	No	No	No	No	Yes	Yes
SNA Switching Services	No	No	No	No	No	No	No
X.25 Switch Local Acknowledgement	No	Yes	Yes	Yes	Yes	No	Yes
WAN Services							
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
Mobile IP	No	Yes	Yes	Yes	Yes	No	Yes
Time-based Access List	Yes	Yes	Yes	Yes	Yes	Yes	Yes

¹ This image was introduced in Cisco IOS Release 12.0(2)T.

² Available on the 4500 only.

Table 7 Feature List by Feature Set for the Cisco 4500/4500-M and 4700/4700-M—Part 2 of 2

Features	Feature Sets						
	Enter- prise Plus	Enter- prise Plus IPsec 56	Enter- prise Plus IPsec 3DES ¹	Enter- prise/ SNASw Plus ²	Enter- prise/ SNASw Plus IPsec 56 ²	Enter- prise/ SNASw Plus IPsec 3DES ²	Distri- buted- Director ²
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
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
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 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 7 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 ¹	Enterprise/ SNASw Plus ²	Enterprise/ SNASw Plus IPsec 56 ²	Enterprise/ SNASw Plus IPsec 3DES ²	Distributed-Director ²
Management							
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 (formerly Response Time Reporter)	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
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
Scalability							
IETF-Compliant PPP over ATM Scalability		Yes	Yes	Yes	Yes	Yes	No
Security							
X.25 Closed User Groups	Yes	Yes	Yes	Yes	Yes	Yes	No
Switching							
Cisco IOS STP Enhancements	Yes	Yes	Yes	Yes	Yes	Yes	No
Express RTP and TCP Header Compression	Yes	Yes	Yes	Yes	Yes	Yes	No
MPLS Traffic Engineering	Yes	Yes	Yes	Yes	Yes	Yes	No

Table 7 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 ¹	Enterprise/ SNASw Plus ²	Enterprise/ SNASw Plus IPsec 56 ²	Enterprise/ SNASw Plus IPsec 3DES ²	Distributed-Director ²
SNA Switching Services	No	No	No	Yes	Yes	Yes	No
X.25 Switch Local Acknowledgement	Yes	Yes	Yes	Yes	Yes	Yes	No
WAN Services							
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 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
Mobile IP	Yes	Yes	Yes	Yes	Yes	Yes	No
Time-Based Access List	Yes	Yes	Yes	Yes	Yes	Yes	Yes

¹ This image was introduced in Cisco IOS Release 12.0(2)T.

² This image was introduced in Cisco IOS Release 12.0(7)T and applies to the 4700-M only.

New and Changed Information

The following sections list new hardware and software features supported by the Cisco 4000 series for Cisco IOS Release 12.0 T.

New Hardware Features in Release 12.0(7)T

There are no new hardware features supported by the Cisco 4000 series in Cisco IOS Release 12.0(7)T.

New Software Features in Release 12.0(7)T

Dynamic Multiple Encapsulations for Dial-In over ISDN

The Dynamic Multiple Encapsulations feature allows incoming calls over ISDN to be assigned an encapsulation type such as Frame Relay, PPP, and X.25 based on calling line identification (CLID) or DNIS. It also allows various encapsulation types and per-user configurations on the same ISDN B channel at different times according to the type of incoming call.

The Dynamic Multiple Encapsulations feature allows per-user configuration for each dial-in caller on any ingress ISDN B channel on which encapsulation can be run independently from other B channels on the same ISDN link. The caller is identified by CLID (caller ID) or DNIS to ensure that only incoming calls with authorization and valid user profiles are accepted. When PPP is used, authentication and profile binding can also be done by PPP name.

In addition, a large set of user profiles can be stored in dialer profiles locally or on a remote AAA server. (For large scale dial-in, storing user-specific configurations on a remote server becomes necessary for enhancing expandability and local memory efficiency.) However, whether stored locally or on a remote AAA server, the user-specific encapsulation and configuration can be applied to individual B channels dynamically and independently.

Dynamic multiple encapsulation is especially important in Europe where ISDN is relatively inexpensive and maximum use of all 30 B channels on the same ISDN link is desirable. Further, the feature removes the need to statically dedicate channels to a particular encapsulation and configuration type, and improves channel usage.

Express RTP and TCP Header Compression

Formerly, 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, compression 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 is increased to 1,000 connections each.

If neither fast switching nor CEF switching is enabled and TCP or RTP header compression is enabled, compression occurs in the process-switched path as before.

Interface MIB Implementation for ATM Subinterfaces

The Interface MIB Implementation for ATM Subinterfaces feature involves the implementation of the Interface MIB (RFC 2233) for ATM subinterfaces. Network managers can now query for the MIB variables on a per-subinterface basis. Because the implementation of this feature is in platform-independent code, this feature is supported on all Cisco ATM interfaces and port adapters where speeds are at or above OC-3.

Low Latency Queueing (CSGdm84810)

The Low Latency Queueing feature brings strict priority queueing to Class-Based Weighted Fair Queueing (CBWFQ). Strict priority 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.

Without Low Latency Queueing, CBWFQ provides weighted fair queueing based on defined classes with no strict priority queue available for real-time traffic. CBWFQ allows you to define traffic classes and then assign characteristics to that class. For example, you can designate the minimum bandwidth delivered to the class during congestion.

For CBWFQ, the weight for a packet belonging to a specific class is derived from the bandwidth you assigned to the class when you configured it. Therefore, the bandwidth assigned to the packets of a class determines the order in which packets are sent. All packets are serviced fairly based on weight; no class of packets may be granted strict priority. This scheme poses problems for voice traffic that is largely intolerant of delay, especially variation in delay. For voice traffic, variations in delay introduce irregularities of transmission manifesting as jitter in the heard conversation.

The Low Latency Queueing feature provides strict priority queueing for CBWFQ, reducing jitter in voice conversations. Configured by the **priority** command, Low Latency Queueing enables use of a single, strict priority queue within CBWFQ at the class level, allowing you to direct traffic belonging to a class to the CBWFQ strict priority queue.

In the event of congestion, when the bandwidth is exceeded, policing is used to drop packets. Voice traffic enqueued to the priority queue is UDP-based and therefore not adaptive to the early packet drop characteristic of Weighted Random Early Detection (WRED).

When congestion occurs, traffic destined for the priority queue is metered to ensure that the bandwidth allocation configured for the class to which the traffic belongs is not exceeded.

MPLS Traffic Engineering

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.

Traffic engineering is essential for service provider and Internet service provider (ISP) backbones that support a high-transmission capacity, and the networks must be resilient to withstand link or node failures.

- Provides an integrated approach to traffic engineering.

With MPLS, traffic engineering capabilities are integrated into Layer 3, which optimizes the routing of IP traffic, given the constraints imposed by backbone capacity and topology.

- Routes traffic flows across a network based on the resources the traffic flow requires and the resources available on the network.

Multicast Source Discovery Protocol

Multicast Source Discovery Protocol (MSDP) connects multiple PIM sparse-mode (SM) domains. MSDP allows multicast sources for a group to be known to all rendezvous points (RPs) in different domains. Each PIM-SM domain uses its own RPs and need not depend on RPs in other domains. An RP runs MSDP over TCP to discover multicast sources in other domains.

An RP in a PIM-SM domain has an MSDP peering relationship with MSDP-enabled routers in another domain. The peering relationship occurs over a TCP connection, where primarily a list of sources sending to multicast groups is exchanged. The TCP connections between RPs are achieved by the underlying routing system. The receiving RP uses the source lists to establish a source path.

The purpose of this topology is to have domains discover multicast sources in other domains. If the multicast sources are of interest to a domain that has receivers, multicast data is delivered over the normal, source-tree building mechanism in PIM-SM.

MSDP is also used to announce sources sending to a group. These announcements must originate at the domain's RP.

MSDP depends heavily on (M)BGP for interdomain operation. You should run MSDP in your domain's RPs that act as sources, sending to global groups for announcement to the Internet.

SNA Switching Services

SNASw provides an easier way than earlier methods to design and implement networks with Systems Network Architecture (SNA) routing requirements. Previously, this network design was accomplished using Advanced Peer-to-Peer Networking (APPN) with full network node (NN) support in the Cisco router. This type of support provided the SNA routing functionality needed, but was inconsistent with the trends in Enterprise networks today. The corporate intranet is replacing the SNA WAN. Enterprises are replacing their traditional SNA network with an IP infrastructure that supports traffic from a variety of clients, using a variety of protocols, requiring access to applications on a variety of platforms, including SNA applications on Enterprise servers.

While SNA routing is still required when multiple servers must be accessed, the number of nodes required to perform this function is decreasing as the IP infrastructure grows and as the amount of native SNA traffic in the network decreases.

SNASw enables an enterprise to develop their IP infrastructure, while meeting SNA routing requirements.

X.25 Closed User Groups

The X.25 specification for Closed User Groups (CUG):

- Provides an application access security service that restricts users who do not have subscribed access to the host location.
- Provides a privacy technique that you can use to create private subnets or virtual networks out of a public data network.

Note Previously, Cisco supported only the ability to specify the CUG value but did not enforce restriction. Cisco currently enforces this security restriction.

X.25 Switch Local Acknowledgment

Cisco offers an X.25 switch function that creates virtual connections (VC) by connecting channels between X.25 class services.

The following X.25 class services are supported:

- X.25, Connection-Mode Network Service (CMNS)
- X.25 over TCP (XOT)
- Switched Virtual Circuits (SVCs) and Permanent Virtual Circuits (PVCs) are both supported and can be switched to each other (converted).

The current Cisco implementation provides end-to-end acknowledgment, which means that flow control or window and packet size acknowledgment is between the originating and terminating data terminal equipment (DTE).

Acknowledgment is not local to the DTE and data communications equipment (DTE), and the overall effect is low throughput.

VPN Tunnel Management (CSCdk51134 and CSCdm52604)

The VPN Tunnel Management feature provides network administrators with two new functions for managing VPN tunnels:

- The ability to set a limit for the maximum number of allowed simultaneous VPN sessions
- The ability to prevent new sessions from being established on a VPN tunnel without disturbing the service of existing sessions (this function is called VPN tunnel soft shutdown)

These functions can be used on either end of a VPN tunnel—the NAS or on the home gateway.

When this feature is enabled, Multichassis Multilink PPP (MMP) Layer 2 Forwarding (L2F) tunnels can still be created and established.

New Hardware Features in Release 12.0(5)T

There are no new hardware features supported by the Cisco 4000 Series in Cisco IOS Release 12.0(5)T.

New Software Features in Release 12.0(5)T

The following new software features are supported by the Cisco 4000 series for Release 12.0(5)T.

Airline Product Set Enhancements

The Airline Product Set Enhancements feature, ALPS phase III, provides support for Mapping of Airline Traffic over Internet Protocol (MATIP). MATIP is an industry standard protocol for transporting airline protocol traffic across a TCP/IP network. This feature enables the end-to-end delivery of ALC and UTS data streams between a Cisco router and the mainframe using TCP/IP. This feature removes the X.25 (AX.25 or EMTOX) requirements for communication with the host reservation system by enabling TCP/IP communication between the router and the airline host reservation system.

ATM LANE Fast Simple Server Redundancy Protocol

To improve the ATM LAN Emulation (LANE) Simple Server Redundancy Protocol (SSRP), Cisco has introduced the ATM LANE Fast Simple Server Redundancy Protocol (FSSRP). FSSRP differs from LANE SSRP in that all configured LANE servers of an emulated LAN (ELAN) are always active. FSSRP-enabled LANE clients have VCs linked to up to four LANE server broadcast-and-unknown servers (BUSs). If a LANE server goes down, the LANE client quickly switches over to a new LANE server and BUS resulting in no data or LE-ARP table entry losses and no extraneous signaling.

DNS-Based X.25 Routing

Managing a large TCP/IP network requires accurate and up-to-date maintenance of IP addresses and X.121 address mapping information on each router database in the network. Currently, this data is managed manually. Because these addresses are constantly being added and removed in the network, the routing table of every router frequently needs to be updated, which is a time-consuming and error-prone task.

X.25 has long operated over an IP network, specifically using Transmission Control Protocol (TCP) as a reliable transport mechanism. This method is known as X.25 over TCP (XOT). However, large networks and financial legacy environments experienced problems with the amount of route configuration that needed to be performed manually because each router switching calls over TCP needed every destination configured. Every destination from the host router needed a static IP route statement, and for larger environments, these destinations could be as much as several thousand per router. Until now, the only way to map X.121 addresses and IP addresses was on a one-to-one basis using the **x25 route x121address xot ipaddress** command.

The solution to this problem was to centralize route configuration that routers could then access for their connectivity needs. This centralization is the function of the DNS-Based X.25 Routing feature, because the DNS server is a database of all domains and addresses on a network.

Frame Relay End-to-End Keepalive

The Frame Relay End-to-End Keepalive feature enables the router to keep track of permanent virtual circuit (PVC) status, independent of the switches in the Frame Relay network. The routers at both ends of a PVC in a Frame Relay network engage in a keepalive session where one router issues keepalive messages and the router at the other end of the PVC connection responds. The time interval for the keepalive is configurable and is enabled on a per-PVC basis. As long as the keepalive-issuing router receives response messages, the PVC status is up. When response messages are not received (because of line failure, a faulty switch in the Frame Relay network, or a router failure), the PVC is down. This mechanism enables bidirectional communication of PVC status to both routers at the ends of a PVC connection.

IP Multicast Multilayer Switching

The IP Multicast Multilayer Switching (MLS) feature provides high-performance, hardware-based, Layer 3 switching of IP multicast traffic for routers connected to Catalyst 5000 series LAN switches.

An IP multicast flow is a unidirectional sequence of packets between a multicast source and the members of a destination multicast group. Flows are based on the IP address of the source device and the destination IP multicast group address.

IP multicast MLS switches IP multicast data packet flows between IP subnets using advanced, application-specific integrated circuit switching hardware, thereby off-loading processor-intensive, multicast packet routing from network routers.

The packet forwarding function is moved onto the connected Layer 3 switch whenever a supported path exists between a source and members of a multicast group. Packets that do not have a supported path to reach their destinations are still forwarded in software by routers. Protocol Independent Multicast is used for route determination.

IPX Multilayer Switching

The IPX Multilayer Switching (IPX MLS) feature provides high-performance, hardware-based, Layer 3 switching for Catalyst 5000 series LAN switches. IPX data packet flows are switched between networks, off-loading processor-intensive packet routing from network routers.

Whenever a partial or complete switched path exists between two hosts, packet forwarding occurs on Layer 3 switches. Packets without such a path are still forwarded by routers to their destinations. Standard routing protocols—such as Routing Information Protocol, Enhanced Interior Gateway Protocol, and NetWare Link Services Protocol—are used for route determination.

IPX MLS also allows you to debug and trace flows in your network. Use MLS explorer packets to identify which switch is handling a particular flow. These packets aid you in path detection and troubleshooting.

Layer 2 Tunneling Protocol Dial-Out

The Layer 2 Tunneling Protocol (L2TP) Dial-Out feature enables L2TP Network Servers (LNSs) to tunnel dial-out VPDN calls using L2TP as the tunneling protocol. This feature enables a centralized network to efficiently and inexpensively establish a virtual point-to-point connection with any number of remote offices.

Using the L2TP Dial-Out feature, Cisco routers can carry both dial-in and dial-out calls in the same L2TP tunnels. Previously, only dial-in VPDN calls were supported.

L2TP dial-out involves two devices: an LNS and an L2TP Access Concentrator (LAC). When the LNS wants to perform L2TP dial-out, it negotiates an L2TP tunnel with the LAC. The LAC then places a PPP call to the client(s) the LNS wants to dial-out to.

Multicast Routing Monitor

The Multicast Routing Monitor (MRM) feature is a management diagnostic tool that provides network fault detection and isolation in a large multicast routing infrastructure. It is designed to notify a network administrator of multicast routing problems in near real time.

MRM has three components that play different roles: the Manager, the Test Sender, and the Test Receiver. The Manager can reside on the same device as the Test Sender or Test Receiver. You can test a multicast environment using test packets (perhaps before an upcoming multicast event) or you can monitor existing IP multicast traffic.

You create a test based on various test parameters, name the test, and start the test. The test runs in the background and the command prompt returns. If the Test Receiver detects an error (such as packet loss or duplicate packets), it sends an error report to the router configured as the Manager. The Manager immediately displays the error report. Also, by entering a certain **show** command, you can see the error reports, if any. You then troubleshoot your multicast environment as normal, perhaps using the **mtrace** command from the source to the Test Receiver. If the **show** command displays no error reports, the Test Receiver is receiving test packets without loss or duplicates from the Test Sender.

Network Director Forwarding Agent

The Network Director Forwarding Agent feature is a Cisco IOS-based packet redirector component of Cisco Network Director, the latest offering in the Cisco family of load balancing solutions. The Network Director Forwarding Agent feature implements two new architectures, the Cisco Applications and Services Architecture and the Cisco-patented Multinode Load Balancing Architecture.

Each Forwarding Agent “learns” the destination of specific connection requests and forwards packets between the appropriate client and chosen destination. When a Forwarding Agent receives a connection request, the request is forwarded to the Services Manager, the LocalDirector-based component of Cisco Network Director. The Services Manager makes the load balancing decision and instructs the Forwarding Agents with the optimal destination. After destination selection, session data is forwarded directly to the destination without further Services Manager participation. There is no limit to the number of Forwarding Agents that can be configured in the Network Director solution.

PGM Router Assist

The PGM Router Assist feature allows Cisco routers to support the optimal operation of Pragmatic General Multicast (PGM). The PGM Reliable Transport Protocol itself is implemented on the hosts of the customer.

PGM is a reliable multicast transport protocol for applications that require 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. It is network-layer independent. The Cisco implementation of the PGM Router Assist feature supports PGM over IP.

Service Assurance Agent

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. The feature allows you to monitor network performance by measuring key Service Level Agreement metrics such as response time, network resources, availability, jitter, connect time, packet loss, and application performance.

With Cisco IOS Release 12.0(5)T, the SA Agent provides new capabilities that enable you to monitor:

- Domain Name Server, DHCP Server, and DLSw peer stack and tunnel performance. Thresholds can be used to trigger additional collection of time delay statistics.
- Network one-way delay variance (jitter) and packet loss.
- Web server response time.

Subnetwork Bandwidth Manager

Resource Reservation Protocol (RSVP) is a signaling mechanism that supports request of specific levels of service such as reserved bandwidth from the network. RSVP and its service class definitions are largely independent of the underlying network technologies. This independence requires that a user define the mapping of RSVP onto subnetwork technologies.

The Subnetwork Bandwidth Manager (SBM) feature answers this requirement for RSVP in relation to IEEE 802-based networks. SBM specifies a signaling method and protocol for LAN-based admission control for RSVP flows. SBM allows RSVP-enabled routers and Layer 2 and Layer 3 devices to support reservation of LAN resources for RSVP-enabled data flows. The SBM signalling method is similar to that of RSVP itself. SBM protocol entities have the following features:

- Reside in Layer 2 or Layer 3 devices.
- Can manage resources on a segment. A segment is a Layer 2 physical segment shared by one or more senders, such as a shared Ethernet or Token Ring wire.
- Can become candidates in a dynamic election process that designates one SBM as the segment manager. The elected candidate is called the Designated Subnetwork Bandwidth Manager (DSBM). The elected DSBM is responsible for exercising admission control over requests for resource reservations on a managed segment.

New Hardware Features in Release 12.0(4)T

There are no new hardware features supported by the Cisco 4000 Series in Cisco IOS Release 12.0(4)T.

New Software Features in Release 12.0(4)T

The following new software features are supported by the Cisco 4000 series for Release 12.0(4)T.

Async over UDP

The Async over UDP feature reads data from low-speed asynchronous ports and transmits it using UDP to clients who might be listening. The clients can be unicast and belong to a multicast group. The incoming data can also be sent out as a broadcast. A sample use might be receiving stock quotes from a source and distributing the quotes in a broadcast or multicast fashion.

CNS Client for Cisco IOS Software

Cisco Directory Services consist of an enhanced UNIX implementation of ActiveDirectory with cache memory support, an SDK with sample applications, and a client for Cisco IOS software. CDS will work with all third party Directory Services such as NDS.

CDS client for Cisco IOS software establishes a Directory Service infrastructure for directory-enabled networks. It will enable many Cisco IOS directory applications to take advantage of Cisco Directory. The client includes the following features:

- EAP/PPP support for RADIUS
- Second release of IPSec Policy Agent
- Second release of Provision Agent

Parse Bookmarks

The Parse Bookmarks feature quickly processes consecutive similar commands, such as **access-lists** and **prefix-lists**—up to five times faster. Parse Bookmarks reduce boot time and load time for large configurations with many similar consecutive commands. This feature is an enhancement to the parsing algorithm; therefore no configuration changes are needed.

Dynamic Multiple Encapsulations for Dial-in over ISDN

The Dynamic Multiple Encapsulations feature allows incoming calls over Integrated Services Digital Network (ISDN) to be assigned an encapsulation type such as Point-to-Point Protocol (PPP), X.25, and ISDN Link Access Procedure, Balanced-Terminal Adapter (LAPB-TA) based on calling line identification (CLID) or Dialed Number Identification Service (DNIS). It also allows various encapsulation types as well as per-user configurations on the same ISDN B channel at different times according to the type of incoming call.

The Dynamic Multiple Encapsulations feature allows per-user configuration for each dial-in caller on any ingress ISDN B channel on which encapsulation can be run independently from other B channels on the same ISDN link. The caller is identified by CLID or DNIS to make sure that only incoming calls with authorization and valid user profiles are accepted. If the protocol is PPP, authentication and profile binding can also be done by PPP name.

Dynamic multiple encapsulations are especially important in Europe where ISDN is relatively inexpensive, and it is desirable to allow maximum use of all B channels on the same ISDN link, especially for large scale dial-in. Further, the feature removes the need to statically dedicate channels to a particular encapsulation and configuration type, and improves channel usage.

Although the Dynamic Multiple Encapsulations feature enhances large scale dial-in functionality, the feature also works well in smaller scale dial-in situations and for modem calls.

New Hardware Features in Release 12.0(3)T

There are no new hardware features supported by the Cisco 4000 series in Cisco IOS Release 12.0(3)T

New Software Features in Release 12.0(3)T

The following new software features are supported by the Cisco 4000 Series in Cisco IOS Release 12.0(3)T.

Annex-G (X.25 over Frame Relay)

Annex G (X.25 over Frame Relay) facilitates the migration from an X.25 backbone to a Frame Relay backbone by permitting encapsulation of CCITT X.25/X.75 traffic within a Frame Relay connection. Annex G was developed to accommodate the many Cisco customers in Europe, where X.25 is still a popular protocol. With Annex G, the process of transporting X.25 over Frame Relay has been simplified, by allowing direct X.25 encapsulation over a Frame Relay network.

This simple process is largely achieved using X.25 profiles (similar to dialer profiles), which were created to streamline the configuration of X.25 on a per DLCI basis. X.25 profiles can contain any existing X.25 command and, once created and named, can be simultaneously associated with more than one Annex G DLCI connection, just using the profile name.

DistributedDirector

Cisco DistributedDirector provides dynamic, transparent, and scalable Internet traffic load distribution between multiple topologically dispersed servers. DistributedDirector is the only global Internet service scaling solution that utilizes Cisco IOS software and leverages routing table information in the network infrastructure to make “network intelligent” load distribution decisions.

Using routing table intelligence in the network infrastructure, DistributedDirector transparently redirects end user service requests to the closest responsive server, as determined by client-to-server topological proximity and/or client-to-server response times, resulting in increased access performance seen by the end user and reduced transmission costs.

For Cisco IOS Release 12.0(3)T, the functionality of DistributedDirector from Release 11.1 IA is migrated to Release 12.0 T. Cisco DistributedDirector is only available as a special hardware/software bundle on the Cisco 2501, 2502, and the 4700-M platforms.

DLSw+ Enhancements

This feature is composed of three major components and enhancements:

- DLSw+ Enhanced Load Balancing

In a network with multiple capable paths, the DLSw+ Load Balancing Enhancements feature improves traffic load balancing between peers by distributing new circuits based on existing loads and the desired ratio.

For each capable peer (peers that have the lowest or equal cost specified), the DLSw+ Load Balancing feature calculates the difference between the desired and the actual ratio of circuits being used on a peer. It detects the path that is underloaded in comparison to the other capable peers and assigns new circuits to that path until the desired ratio is achieved.

- DLSw+ Peer Clusters

The DLSw+ Peer Clusters feature reduces the explorer packet replication that typically occurs in a large DLSw+ Peer Group design, where there are multiple routers connected to the same LAN.

The DLSw+ Peer Clusters feature associates DLSw+ peers (that are connected to the same LAN) into logical groups. Once the multiple peers are defined in the same peer group cluster, the DLSw+ Border Peer recognizes that it does not have to forward explorers to more than one member within the same peer group cluster.

- DLSw+ RSVP Bandwidth Reservation

The DLSw+ RSVP Bandwidth Reservation feature allows DLSw+ to reserve network bandwidth for the DLSw+ TCP connection between DLSw+ peers.

Although it has been possible in the past to reserve bandwidth for a particular existing DLSw+ peer connection through the RSVP CLI support in Cisco IOS software, the CLI required prior knowledge of the TCP ports for which the reservation was being made. Because DLSw+ uses one well-known port and one randomly assigned port, the reservation could not be made until after the peer connection was active.

The DLSw+ RSVP feature permits new DLSw+ peer connections to automatically request bandwidth reservations upon connection, thereby removing the need for user intervention after the peer is connected. This feature assures the reservation will survive a network or device failure and that the DLSw+ traffic carried over a TCP connection is not affected by congestion.

Flow-Based WRED

This feature provides a mechanism to penalize the flows that do not respond to Weighted Random Early Detection (WRED) drops. This feature is provided as an extension to the existing WRED functionality and can be turned on after WRED is turned on.

Flow-WRED ensures that no single flow can unfairly dominate the buffer resources at the output interface queue. With WRED alone, this can occur in the presence of traffic sources that do not back off during congestion. Flow-WRED maintains minimal information about the buffer occupancy per flow. Whenever a flow exceeds its share of the output interface buffer resource the packets of the flow are penalized by increasing the probability of their drop (by WRED).

Large Scale Dialout

Large scale dialout eliminates the need to configure dialer maps on every network access server (NAS) for every destination. Instead, you create remote site profiles containing outgoing call attributes (telephone number, service type, maximum number of links, and so on) on an authentication, authorization, and accounting (AAA) server. The profile is downloaded by the NAS when packet traffic requires a call to be placed to a remote site. Large scale dialout also takes advantage of features previously only available for incoming calls, such as dialer and virtual profiles, Multichassis Multilink PPP (MMP) support, and the ability to use an AAA server to store dialout attributes. MMP allows NASes to be stacked together and appear as a single NAS chassis so that if one NAS fails, another NAS in the stack can accept calls. Additionally, large scale dialout addresses congestion management by seeking an uncongested, alternative NAS when the designated primary NAS experiences port congestion.

Policy Routing Infrastructure

Full support of IP Policy Based Routing is used in conjunction with Cisco Express Forwarding and NetFlow. As CEF gradually obsoletes fast switching, policy routing must be integrated with CEF to meet customer performance requirements. When both policy routing and flow are enabled, redundant processing is avoided, performance is optimized, and a scalable set of services is delivered.

Process MIB

The addition of the CISCO-PROCESS-MIB and changes to the CISCO-MEMORY-POOL-MIB allow the retrieval of additional CPU and memory statistics and their reporting by SNMP.

The CISCO-PROCESS-MIB:

- Provides CPU 5-second, 1-minute, and 5-minute statistics.
- Provides CPU utilization and memory allocation/deallocation statistics for each process on each CPU listed in the CISCO-PROCESS-MIB.
- Is enabled when the first SNMP command is configured. The background statistics collection for VIP cards and the master CPU occurs even if the SNMP subsystem is not initialized.

Response Time Reporter Enhancements

The Response Time Reporter (RTR) feature allows you to monitor network performance, network resources, and applications by measuring response times and availability. RTR statistics can be used to perform troubleshooting, problem notifications and pre-problem analysis. The RTR enhancements extend IP support, such as Type of Service, and allow you to measure various types of IP traffic, such as UDP, TCP, and HTTP.

SNMP v3

Simple Network Management Protocol version 3 (SNMPv3) addresses issues related to the large scale deployment of SNMP for configuration, accounting, and fault management. Currently, SNMP is predominantly used for monitoring and performance management. The primary goal of SNMPv3 is to define a secure version of the SNMP protocol. SNMPv3 also facilitates remote configuration of the SNMP entities, which make remote administration of SNMP entities a much simpler task. SNMPv3 builds on top of SNMPv1 and SNMPv2 to provide a secure environment for the management of systems and networks.

SNMPv3 provides an identification strategy for SNMP devices to facilitate communication only between known SNMP strategy. Each SNMP device has an identifier called the SNMP EngineID, which is a copy of SNMP. Each SNMP message contains an SNMP EngineID. SNMP communication is possible only if an SNMP entity knows the identity of its peer SNMP device.

SNMPv3 also contains a security model or security strategy that exists between an SNMP user and the SNMP group to which the user belongs. A security model may define the security policy within an administrative domain or a intranet. The SNMPv3 protocol consists of the specification for the User-Based Security Model (USM).

Definition of security goals where the goals of message authentication service includes the following protection strategies:

- Modification of Information or protection against some unauthorized SNMP entity altering in-transit SNMP messages generated on behalf of an authorized principal
- Masquerade or protection against attempting management operations not authorized for some principal by assuming the identity of another principal that has the appropriate authorizations
- Message Stream Modification or protection against messages getting maliciously reordered, delayed, or replayed in order to effect unauthorized management operations
- Disclosure or protection against eavesdropping on the exchanges between SNMP engines. Three different types of communication mechanisms are available for this protection strategy:
 - Communication without authentication and privacy (NoAuthNoPriv)
 - Communication with authentication and without privacy (AuthNoPriv)
 - Communication with authentication and privacy (AuthPriv)

Time-Based Access Lists

Time-based access lists (ACLs) are widely used for implementing security policy throughout the network infrastructure. Access lists are used to define application packets that trigger connections to a service. Implementing time-of-day policy on ACLs adds flexibility in the filtering of packets.

Web Cache Communications Protocol Version 2 (WCCPv2)

The Web Cache Communications Protocol enables Cisco IOS routing platforms to transparently redirect content requests (for example, web requests) from clients to a locally connected Cisco Cache Engine (or Cache Cluster) instead of the intended origin server. When a Cache Engine receives such a request, it attempts to service it from its own local cache if the requested information is present. If not, the Cache Engine issues its own request to the originally requested origin server to get the required information. When the Cache Engine retrieves the requested information, it forwards it to the requesting client and caches it to fulfill future requests, thus maximizing download performance and significantly reducing WAN transmission costs.

WCCPv2 provides enhancements to WCCPv1, including:

- Multihome router support enables multiple co-located, WCCP-enabled routers to share a cache cluster.
- Improved security enables MD5 digital signature authentication (RFC 1321) to be used in Cache Engine/WCCP router communications.
- Redirection of non-port 80 traffic enables WCCP-enabled routers to transparently redirect traffic based on any TCP port (for example, FTP and NNTP traffic), in addition to HTTP traffic. Cache Engine-side support for non-port 80 traffic will be provided in the future.
- Content bypass support—When a Cache Engine rejects a request and sends it back to the WCCP-enabled router, the router knows not to redirect the request to the Cache Engine again.
- Flexible content distribution within a cache cluster—Various hashing parameters can be used to determine content distribution within a cache cluster.

X.25 Load Balancing

As the number of users accessing the same host has grown, competition for these application resources has become a problem. Internet service providers (ISPs) have had to increase the number of users they could support by increasing the number of X.25 lines to the host.

In order to support a large number of virtual circuits (VCs) to a particular destination, configuration of more than one serial interface to that destination was needed. When a serial interface is configured to support X.25, there is a fixed number of VCs available for use.

Using a facility called “hunt-group” (the method for X.25 load balancing), a switch is able to view a pool of X.25 lines going to the same host as one address and assign VCs on an “idle logical channel” basis. With this feature, X.25 calls can be load balanced among all configured outgoing interfaces to fully use and balance all managed lines. The benefits include, the choice of two load-balancing distribution methods (rotary or vc-count) and improved performance of serial lines.

New Features in Release 12.0(2)T

The following new features are supported by the Cisco 4000 series in Cisco IOS Release 12.0(2)T.

Four New Feature Sets

The following four new feature sets have been created for the Cisco 4000 series in Release 12.0(2)T that support IPsec Triple DES encryption:

- IP Plus IPsec 3DES—c4000-ik2s-mz, c4500-ik2s-mz
- Enterprise Plus IPsec 3DES—c4000-jk2s-mz, c4500-jk2s-mz
- Enterprise/APPN Plus IPsec 3DES—c4000-ajk2s-mz, c4500-ajk2s-mz
- Enterprise/APPN/DB Conn 3DES—c4500-aejk2s-mz (not supported on the Cisco 4000 or Cisco 4000-M)

Triple DES (3DES) is a strong form of encryption that allows sensitive information to be transmitted over unsecure networks. Triple DES (3DES) enables customers, particularly in the finance industry, to utilize network layer encryption. IPsec supports the Triple DES encryption algorithm (168-bit) in addition to 56-bit encryption.

New Features in Release 12.0(1)T

The following new features are supported by the Cisco 4000 Series in Cisco IOS Release 12.0(1)T.

Cisco IOS IEEE 802.1Q Support

Cisco IOS IEEE 802.1Q provides support for IEEE 802.1Q encapsulation for Virtual LANs (VLANs). Use this feature for VLANs consisting of IEEE 802.1Q compliant switches.

Mobile IP

Mobile IP:

- Provides you the freedom to roam beyond your home subnet while consistently maintaining your home IP address.
- Enables transparent routing of IP datagrams to mobile users during their movement, so that data sessions can be initiated to them while they roam.
- Enables sessions to be maintained in spite of physical movement between points of attachment to the Internet or other networks.

Cisco's implementation of Mobile IP is fully compliant with the Internet Engineering Task Force's (IETF's) proposed standard defined in RFC 2002.

Easy IP Phase 2-DHCP Server

With the introduction of Easy IP Phase 2, Cisco IOS software also supports Intelligent DHCP Relay functionality. A DHCP Relay Agent is any host that forwards DHCP packets between clients and servers and enables the client and server to reside on separate subnets. If the Cisco IOS DHCP server cannot satisfy a DHCP request from its own database, it forwards the DHCP request to one or more secondary DHCP servers defined by the network administrator by using standard Cisco IOS ip helper-address functionality.

OSPF Packet Pacing

In former OSPF implementation for sending update packets, some update packets got lost when the link was slow, a neighboring router did not receive the updates fast enough, or the router was out of buffer space. For example, packets were dropped if either of these topologies existed:

- A fast router was connected to a slower router over a point-to-point link.
- During flooding, several neighbors dumped updates to a single router at the same time.

OSPF update packets are now automatically paced by a delay of 33 milliseconds. Pacing is also added between retransmissions to increase efficiency and minimize lost retransmissions.

OSPF update and retransmission packets are sent more efficiently. You can also display the LSAs waiting to be sent out an interface.

RIP Enhancements

Triggered extensions to IP RIP increase efficiency of RIP on point-to-point serial interfaces.

Routers are used on connection-oriented networks to allow connectivity to many remote destinations. Circuits on the WAN are established on demand and are relinquished when the traffic subsides. Depending on the application, the connection between any two sites for user data can be short and relatively infrequent.

There were two problems using RIP to connect to a WAN:

- Periodic broadcasting by RIP generally prevented WAN circuits from being closed.
- Even on fixed point-to-point links, the overhead of periodic RIP transmissions could seriously interrupt normal data transfer because of the quantity of information that hit the line every 30 seconds.

To overcome these limitations, triggered extensions to RIP cause RIP to send information on the WAN only when there has been an update to the routing database. Periodic update packets are suppressed over the interface on which this feature is enabled.

ISDN MIB RFC 2127

The new Integrated Services Digital Network (ISDN) Management Information Base (MIB) RFC 2127 has been designed to provide useful information in accordance with the IETF's new standard for the management of ISDN interfaces. RFC 2127 provides information on the physical Basic Rate interfaces, control and statistical information for B (bearer) and D (signaling) channels, terminal endpoints, and directory numbers.

The ISDN MIB RFC 2127 controls all aspects of ISDN interfaces. It consists of five groups:

- ISDN Physical Interface Group
- B (Bearer) Channel Group
- D (Signaling) Channel Group
- Terminal Endpoint Group
- Directory Number Group (optional)

The ISDN MIB RFC 2127 enables you to use any commercial SNMP network management application to support ISDN call processing in Cisco IOS software. You can integrate management of dial access products by using ISDN with your existing network management systems.

Layer 2 Tunneling Protocol (L2TP)

Layer 2 Tunneling Protocol (L2TP) is an emerging Internet Engineering Task Force (IETF) standard that combines the best features of two existing tunneling protocols: Cisco's Layer 2 Forwarding (L2F) and Microsoft's Point-to-Point Tunneling Protocol (PPTP). L2TP is an extension to the Point-to-Point Protocol (PPP), which is an important component for Access Virtual Private Networks (VPNs). Access VPNs allow remote users to connect to their corporate intranets or extranets, thus improving flexibility and reducing costs.

Traditional dial-up networking services only supported registered IP addresses, which limited the types of applications that could be implemented over Virtual Private Networks (VPNs). L2TP supports multiple protocols and unregistered and privately administered IP addresses over the Internet. L2TP allows you to use the existing access infrastructure, such as the Internet, modems, access servers, and ISDN terminal adaptors (TAs).

You can initiate L2TP wherever PPTP or L2F is currently deployed. You can operate it as a client initiated tunnel, such as PPTP, or a network access server (NAS) initiated tunnel, such as L2F.

PPP over Frame Relay

The PPP over Frame Relay feature allows a router to establish end-to-end Point-to-Point Protocol (PPP) sessions over Frame Relay. IP datagrams are transported over the PPP link by using RFC 1973 compliant Frame Relay framing. This feature is useful for remote users running PPP to access their Frame Relay corporate networks.

PPP over Frame Relay provides the following benefits:

- Allows end-to-end PPP sessions over Frame Relay
- Supports the 90i IDSL Channel Unit that supports both Frame Relay and Point-to-Point Protocol (PPP) on an ISDN DSL

IETF-Compliant PPP over ATM Scalability (Cisco 4500/4500-M and Cisco 4700/4700-M only)

Point-to-Point Protocol (PPP) over Asynchronous Transfer Mode (ATM) is now available on an ATM CES port adapter in the Cisco 4500/4500-M and Cisco 4700/4700-M.

In previous releases of PPP over ATM, permanent virtual circuits (PVCs) for PPP over ATM were configured on point-to-point subinterfaces. The previous version of PPP over ATM supported only the Frame Forwarding data encapsulation (aal5ciscopp).

In this release, PPP over ATM:

- No longer requires two interfaces: a virtual access interface and ATM subinterface
- Allows you to configure multiple PVCs for PPP over ATM on multipoint subinterfaces
- Provides a significant increase in the number of PPP over ATM sessions per router
- Supports virtual circuit (VC) multiplexed encapsulation

- Complies with the Internet Engineering Task Force (IETF) draft on multiplexed encapsulation titled PPP over AAL5
- Provides support for IETF-compliant PPP over ATM and significantly increases the maximum number of PPP over ATM sessions running on a router

Note The IETF PPP over ATM feature does not currently support LLC encapsulated PPP over ATM Adaptation Layer 5 (AAL5).

The maximum number of PPP over ATM sessions supported on a platform depends on available system resources, such as memory and CPU speed.

ATM PVC Trap Support (Cisco 4500/4500-M and Cisco 4700/4700-M only)

The ATM PVC Trap Support feature:

- Provides Simple Network Management Protocol (SNMP) notification for permanent virtual circuit (PVC) failures
- Provides SNMP access to PVC status tables
- Enables an agent to send the required PVC traps for this notification
- Provides support for these PVC status tables: atmCurrentlyFailingPVCTable and atmInterfaceExtTable

Normally, a management station is not notified when an ATM PVC goes down.

CLI String Search

The Command Line Interface (CLI) String Search feature allows you to search or filter any **show** or **more** command's output. This is useful when you need to sort through large amounts of output, or if you want to exclude output that you do not need to see. CLI String Search also allows you to search and filter at --More-- paging prompts.

With the search function, you can begin unfiltered output at the first line that contains a regular expression that you specify. You can specify a maximum of one filter per command to either include or exclude output lines that contain the specified regular expression.

A regular expression is any word, phrase, number, and so on that appears in **show** or **more** command output.

Cisco IOS STP Enhancements

Cisco IOS Spanning Tree Protocol enhancements broaden the original Cisco IOS STP implementation with increased port identification capability, improved path cost determination, and support for a new VLAN bridge spanning-tree protocol.

Limitations and Restrictions

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 8.

Table 8 **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

Important Notes

Last Maintenance Release of Cisco IOS Release 12.0 T

Cisco IOS Release 12.0(6)T has been renamed 12.0(7)T to align this release with the 12.0(7) mainline release. The closed caveats for Release 12.0(7)T are identical to the caveats closed in the 12.0(7) mainline release. There was no change in the feature content of the renamed release--the features in 12.0(6)T are the same as 12.0(7)T. Release 12.0(7)T is the last maintenance release of the 12.0 T release train.

Customers needing closure of caveats for the 12.0 T features should migrate to the 12.1 mainline release, which has the complete feature content of Release 12.0 T and will eventually reach General Deployment (GD). Release 12.0 T is a super set of the 12.0 mainline release, so all caveats closed in the 12.0 mainline are also closed in 12.0 T.

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.

For information on caveats in Cisco IOS Release 12.0 T, see *Caveats for Cisco IOS Release 12.0 T*.

All caveats in Release 12.0 are also in Release 12.0 T.

For information about caveats in Cisco IOS Release 12.0, see *Caveats for Cisco IOS Release 12.0*, 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 the 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, except for feature modules, which are available online on CCO and the Documentation CD-ROM.

Use these release notes with these documents:

- Release-Specific Documents, page 35
- Platform-Specific Documents, page 36
- Feature Modules, page 36
- Cisco IOS Software Documentation Set, page 37

Release-Specific Documents

The following documents are specific to Release 12.0 T and are located on CCO and the Documentation CD-ROM:

- *Cross-Platform Release Notes for Cisco IOS Release 12.0 T*

On CCO at:

Technical Documents: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 12.0:

On the Documentation CD-ROM at:

Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 12.0: Release Notes: Cross-Platform Release Notes for Cisco IOS Release 12.0 T

- Product bulletins, field notices, and other release-specific documents on CCO at:

Technical Documents

- *Caveats for Cisco IOS Release 12.0 T*

See *Caveats for Cisco IOS Release 12.0 T*, which contain caveats applicable to all platforms for all maintenance releases of Release 12.0 and Release 12.0 T.

On CCO at:

Technical Documents: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 12.0: Caveats: Caveats for Cisco IOS Release 12.0 T

On the Documentation CD-ROM at:

Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS 12.0: Caveats: Caveats for Cisco IOS Release 12.0 T

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 - 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 12.0 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 12.0: New Feature Documentation

On the Documentation CD-ROM:

Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 12.0: New Feature Documentation: New Features in Release 12.0 T

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. These documents 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 12.0: Configuration Guides and Command References

On the Documentation CD-ROM:

Cisco Products Documentation: Cisco IOS Software Configuration: Cisco IOS Release 12.0: Configuration Guides and Command References

Release 12.0 Documentation Set

Table 9 describes the contents of the Cisco IOS Release 12.0 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 12.0

On the Documentation CD-ROM at:

Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 12.0

Table 9 Cisco IOS Software Release 12.0 Documentation Set

Books	Chapter Topics
<ul style="list-style-type: none"> • <i>Configuration Fundamentals Configuration Guide</i> • <i>Configuration Fundamentals Command Reference</i> 	Configuration Fundamentals Overview Cisco IOS User Interfaces File Management System Management
<ul style="list-style-type: none"> • <i>Bridging and IBM Networking Configuration Guide</i> • <i>Bridging and IBM Networking Command Reference</i> 	Transparent Bridging Source-Route Bridging Token Ring Inter-Switch Link Remote Source-Route Bridging DLSw+ STUN and BSTUN LLC2 and SDLC IBM Network Media Translation DSPU and SNA Service Point SNA Frame Relay Access Support APPN Cisco Database Connection NCIA Client/Server Topologies Cisco Mainframe Channel Connection Airline Product Set
<ul style="list-style-type: none"> • <i>Dial Solutions Configuration Guide</i> • <i>Dial Solutions Command Reference</i> 	X.25 over ISDN Appletalk Remote Access Asynchronous Callback, DDR, PPP, SLIP Bandwidth Allocation Control Protocol ISDN Basic Rate Service ISDN Caller ID Callback PPP Callback for DDR Channelized E1 & T1 Dial Backup for Dialer Profiles Dial Backup Using Dialer Watch Dial Backup for Serial Lines Peer-to-Peer DDR with Dialer Profiles DialOut Dial-In Terminal Services Dial-on-Demand Routing (DDR) Dial Backup Dial-Out Modem Pooling Large-Scale Dial Solutions Cost-Control Solutions Virtual Private Dialup Networks Dial Business Solutions and Examples
<ul style="list-style-type: none"> • <i>Cisco IOS Interface Configuration Guide</i> • <i>Cisco IOS Interface Command Reference</i> 	Interface Configuration Overview LAN Interfaces Logical Interfaces Serial Interfaces
<ul style="list-style-type: none"> • <i>Network Protocols Configuration Guide, Part 1</i> • <i>Network Protocols Command Reference, Part 1</i> 	IP Overview IP Addressing and Services IP Routing Protocols
<ul style="list-style-type: none"> • <i>Network Protocols Configuration Guide, Part 2</i> • <i>Network Protocols Command Reference, Part 2</i> 	AppleTalk Novell IPX

Table 9 Cisco IOS Software Release 12.0 Documentation Set (continued)

Books	Chapter Topics
<ul style="list-style-type: none"> • <i>Network Protocols Configuration Guide, Part 3</i> • <i>Network Protocols Command Reference, Part 3</i> 	Network Protocols Overview Apollo Domain Banyan VINES DECnet ISO CLNS XNS
<ul style="list-style-type: none"> • <i>Security Configuration Guide</i> • <i>Security Command Reference</i> 	AAA Security Services Security Server Protocols Traffic Filtering and Firewalls IP Security and Encryption Passwords and Privileges Neighbor Router Authentication 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> 	Switching Services Switching Paths for IP Networks Virtual LAN (VLAN) Switching and Routing
<ul style="list-style-type: none"> • <i>Wide-Area Networking Configuration Guide</i> • <i>Wide-Area Networking Command Reference</i> 	Wide-Area Network Overview ATM Frame Relay SMDS X.25 and LAPB
<ul style="list-style-type: none"> • <i>Voice, Video, and Home Applications Configuration Guide</i> • <i>Voice, Video, and Home Applications Command Reference</i> 	Voice over IP Voice over Frame Relay Voice over ATM Voice over HDLC Frame Relay-ATM Internetworking Synchronized Clocks Video Support Universal Broadband Features
<ul style="list-style-type: none"> • <i>Quality of Service Solutions Configuration Guide</i> • <i>Quality of Service Solutions Command Reference</i> 	Policy-Based Routing QoS Policy Propagation via BGP Committed Access Rate Weighted Fair Queueing Custom Queueing Priority Queueing Weighted Random Early Detection Scheduling Signaling RSVP Packet Drop Frame Relay Traffic Shaping Link Fragmentation RTP Header Compression
<ul style="list-style-type: none"> • <i>Cisco IOS Software Command Summary</i> • <i>Dial Solutions Quick Configuration Guide</i> • <i>System Error Messages</i> • <i>Debug Command Reference</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**.

Service and Support

For service and support for a product purchased from a reseller, contact the reseller, who offers a wide variety of Cisco service and support programs described in “Service and Support” of *Cisco Information Packet* shipped with your product.

Note If you purchased your product from a reseller, you can access CCO as a guest. CCO is Cisco Systems’ primary real-time support channel. Your reseller offers programs that include direct access to CCO services.

For service and support for a product purchased directly from Cisco, use CCO.

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/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: **Products & Technologies: Products: Technical Tips**.

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*.

Cisco Connection Online

Cisco Connection Online (CCO) is Cisco Systems' primary, real-time support channel. Maintenance customers and partners can self-register on CCO to obtain additional information and services.

Available 24 hours a day, 7 days a week, CCO provides a wealth of standard and value-added services to Cisco's customers and business partners. CCO services include product information, product documentation, software updates, release notes, technical tips, the Bug Navigator, configuration notes, brochures, descriptions of service offerings, and download access to public and authorized files.

CCO serves a wide variety of users through two interfaces that are updated and enhanced simultaneously: a character-based version and a multimedia version that resides on the World Wide Web (WWW). The character-based CCO supports Zmodem, Kermit, Xmodem, FTP, and Internet e-mail, and it is excellent for quick access to information over lower bandwidths. The WWW version of CCO provides richly formatted documents with photographs, figures, graphics, and video, as well as hyperlinks to related information.

You can access CCO in the following ways:

- WWW: <http://www.cisco.com>
- WWW: <http://www-europe.cisco.com>
- WWW: <http://www-china.cisco.com>
- Telnet: cco.cisco.com
- Modem: From North America, 408 526-8070; from Europe, 33 1 64 46 40 82. Use the following terminal settings: VT100 emulation; databits: 8; parity: none; stop bits: 1; and connection rates up to 28.8 kbps.

For a copy of CCO's Frequently Asked Questions (FAQ), contact cco-help@cisco.com. For additional information, contact cco-team@cisco.com.

Note If you are a network administrator and need personal technical assistance with a Cisco product that is under warranty or covered by a maintenance contract, contact Cisco's Technical Assistance Center (TAC) at 800 553-2447, 408 526-7209, or tac@cisco.com. To obtain general information about Cisco Systems, Cisco products, or upgrades, contact 800 553-6387, 408 526-7208, or cs-rep@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, a member of the Cisco Connection Family, is updated monthly. Therefore, it might be more current than printed documentation. To order additional copies of the Documentation CD-ROM, contact your local sales representative or call customer service. The CD-ROM package is available as a single package or as an annual subscription. You can also access Cisco documentation on the World Wide Web at <http://www.cisco.com>, <http://www-china.cisco.com>, or <http://www-europe.cisco.com>.

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

This document is to be used in conjunction with the documents listed in the "Related Documentation" section on page 35.

Access Registrar, AccessPath, Any to Any, AtmDirector, Browse with Me, CCDA, CCDE, CCDP, CCIE, CCNA, CCNP, CCSI, CD-PAC, the Cisco logo, Cisco Certified Internetwork Expert logo, *CiscoLink*, the Cisco Management Connection logo, the Cisco NetWorks logo, the Cisco Powered Network logo, Cisco Systems Capital, the Cisco Systems Capital logo, Cisco Systems Networking Academy, the Cisco Systems Networking Academy logo, the Cisco Technologies logo, ConnectWay, Fast Step, FireRunner, Follow Me Browsing, FormShare, GigaStack, IGX, Intelligence in the Optical Core, Internet Quotient, IP/VC, Kernel Proxy, MGX, MultiPath Data, MultiPath Voice, Natural Network Viewer, NetSonar, Network Registrar, the Networkers logo, *Packet*, PIX, Point and Click Internetworking, Policy Builder, Precept, ScriptShare, Secure Script, ServiceWay, Shop with Me, SlideCast, SMARTnet, SVX, *The Cell*, TrafficDirector, TransPath, ViewRunner, Virtual Loop Carrier System, Virtual Service Node, Virtual Voice Line, VisionWay, VlanDirector, Voice LAN, WaRP, Wavelength Router, Wavelength Router Protocol, WebViewer, Workgroup Director, and Workgroup Stack are trademarks; Changing the Way We Work, Live, Play, and Learn, Empowering the Internet Generation, The Internet Economy, and The New Internet Economy are service marks; and ASIST, BPX, Catalyst, Cisco, Cisco IOS, the Cisco IOS logo, Cisco Systems, the Cisco Systems logo, the Cisco Systems Cisco Press logo, Enterprise/Solver, EtherChannel, EtherSwitch, FastHub, FastLink, FastPAD, FastSwitch, GeoTel, IOS, IP/TV, IPX, LightStream, LightSwitch, MICA, NetRanger, Post-Routing, Pre-Routing, Registrar, StrataView Plus, Stratm, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. or its affiliates in the U.S. and certain other countries. All other trademarks mentioned in this document are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any of its resellers. (9912R)

Copyright © 1998–1999 Cisco Systems, Inc.
All rights reserved.