Release Notes for the Cisco 1700 Series for Cisco IOS Release 12.0 T

December 13, 1999

These release notes for Cisco 1700 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 the software caveats that apply to Release 12.0(7)T, see the *Caveats for Cisco IOS Release 12.0 T* document that accompanies these release notes. The 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* R*elease Notes for Cisco IOS Release 12.0* on CCO and the Documentation CD-ROM.

Contents

These release notes describe the following topics:

Cisco Systems

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

System Requirements

This section describes the system requirements for Release 12.0 T:

- Memory Requirements, page 2
- Hardware Supported, page 4
- Determining the Software Version, page 6
- Upgrading to a New Software Release, page 6
- Feature Set Tables, page 6

Memory Requirements

Table 1 Memory Requirements for the Cisco 1700 Series

Platform	Feature Sets	Image Name	Software Image	Required Flash Memory	Required DRAM Memory	Runs from
Cisco 1720 Router	IP Feature Sets	IP	c1700-y-mz	4 MB	16 MB	RAM
		IP Plus	c1700-sy-mz	4 MB	16 MB	RAM
		IP Plus 40	c1700-sy40-mz	4 MB	16 MB	RAM
		IP Plus 56	c1700-sy56-mz	4 MB	20 MB	RAM
		IP Plus IPSEC 56[1]	c1700-sy56i-mz	4 MB	20 MB	RAM
		IP/IPX	c1700-ny-mz	4 MB	16 MB	RAM
		IP/IPX/AT/IBM	c1700-bnr2y-mz	4 MB	20 MB	RAM
		IP/IPX/AT/IBM Plus	c1700-bnr2sy-mz	8 MB	24 MB	RAM
		IP/Firewall	c1700-oy-mz	8[2] MB	16 MB	RAM
		IP/Firewall Plus IPSEC 56	c1700-osy56i-mz	8[2] MB	20 MB	RAM
		IP/IPX/Firewall Plus	c1700-nosy-mz	8[2] MB	20 MB	RAM
		IP/IPX/AT/IBM/Firewall Plus IPSEC 56	c1700-bnor2sy56i-mz	8 MB	24 MB	RAM
		IP Plus IPSEC 3DES	c1700-k2sy-mz	8 MB	20 MB	RAM
		IP/Firewall Plus IPSEC 3DES	c1700-k2osy-mz	4 MB	20 MB	RAM
		IP/IPX/AT/IBM/Firewall Plus IPSEC 3DES	c1700-bk2nor2sy-mz	8 MB	24 MB	RAM

Table 1 Memory Requirements for the Cisco 1700 Series (continued)

Platform	Feature Sets	Image Name	Software Image	Required Flash Memory	Required DRAM Memory	Runs from
Cisco 1750 Router	IP Feature Sets	IP	c1700-y-mz	4 MB	16 MB	RAM
		IP Plus	c1700-sy-mz	4 MB	16 MB	RAM
		IP Plus 40	c1700-sy40-mz	4 MB	20 MB	RAM
		IP Plus 56	c1700-sy56-mz	8 MB	20 MB	RAM
		IP Plus IPSEC 56	c1700-sy56i-mz	8 MB	20 MB	RAM
		IP Plus IPSEC 3DES	c1700-k2sy-mz	8 MB	20 MB	RAM
		IP/FW	c1700-oy-mz	4 MB	16 MB	RAM
		IP/IPX/FW Plus	c1700-nosy-mz	8 MB	20 MB	RAM
		IP/FW Plus IPSEC 56	c1700-osy56i-mz	8 MB	24 MB	RAM
		IP/FW Plus IPSEC 3DES	c1700-k2osy-mz	8 MB	24 MB	RAM
		IP/IPX	c1700-ny-mz	4 MB	16 MB	RAM
		IP/IPX/AT/IBM	c1700-bnr2y-mz	8 MB	20 MB	RAM
		IP/IPX/AT/IBM Plus	c1700-bnr2sy-mz	8 MB	24 MB	RAM
		IP/IPX/AT/IBM/FW Plus IPSEC 56	c1700-bnor2sy56i-mz	8 MB	32 MB	RAM
		IP/IPX/AT/IBM/FW Plus IPSEC 3DES	c1700-bk2nor2sy-mz	8 MB	32 MB	RAM
		IP/Voice Plus	c1700-sv3y-mz	8 MB	24 MB	RAM
		IP/Voice Plus 40	c1700-sv3y40-mz	8 MB	24 MB	RAM
		IP/Voice Plus 56	c1700-sv3y56-mz	8 MB	24 MB	RAM
		IP/Voice Plus IPSEC 56	c1700-sv3y56i-mz	8 MB	24 MB	RAM
		IP/Voice Plus IPSEC 3DES	c1700-k2sv3y-mz	8 MB	24 MB	RAM
		IP/FW/Voice Plus	c1700-osv3y-mz	8 MB	24 MB	RAM
		IP/FW/Voice Plus IPSEC 56	c1700-osv3y56i-mz	8 MB	24 MB	RAM
		IP/FW/Voice Plus 3DES	c1700-k2osv3y-mz	8 MB	32 MB	RAM
		IP/IPX/FW/Voice Plus	c1700-nosv3y-mz	8 MB	24 MB	RAM
		IP/IPX/AT/IBM/FW/Voice Plus IPSEC 56	c1700-bnor2sv3y56i-mz	8 MB	32 MB	RAM
		IP/IPX/AT/IBM/FW/Voice Plus 3DES	c1700-bk2nor2sv3y-mz	8 MB	32 MB	RAM

[1] This image was not available until release 12.0(3)T.

[2] 4 MB in Release 12.0(4)T and earlier releases.

Hardware Supported

Cisco IOS Release 12.0 T supports the Cisco 1700 series:

- Cisco 1720—Runs data images only. Introduced in Release 12.0(1)T.
- Cisco 1750—Runs data and data-plus-voice images. Introduced in Release 12.0(7)T.

For detailed descriptions of the new hardware features, see the “New and Changed Information” section on page 16.

Cisco 1720

The 1720 router provides Internet and intranet access and includes the following:

- Support for virtual private networking
- Modular architecture
- Network device integration

The Cisco 1720 router has the following hardware components:

- One autosensing 10/100 Fast Ethernet port
- Two WAN interface card slots
- One auxiliary (AUX) port (up to 115.2 kbps asynchronous serial)
- One console port
- RISC Processor for high performance encryption
- One internal expansion slot for support of future hardware-assisted services such as encryption (up to T1/E1) and compression
- DRAM memory: 16 MB default, expandable to 48 MB
- Flash memory: 4 MB default, expandable to 16 MB
- Desktop form factor

The Cisco 1720 router supports any combination of one or two of the following WAN interface cards, which are shared with the Cisco 1600, 2600, and 3600 routers:

- WIC-1T: One port high speed serial (sync/async)
- WIC-2T: Two port high speed serial (sync/async)
- WIC-2A/S: Two port low speed serial (sync/async) (up to 128 kbps)
- WIC-1B-S/T: One port ISDN BRI S/T
- WIC-1B-U: One port ISDN BRI U
- WIC-1DSU-56K4: One port integrated 56/64 kbps 4-wire DSU/CSU
- WIC-1DSU-T1: One port integrated T1 / Fractional T1 DSU/CSU

Cisco 1750

The voice-and-data capable Cisco 1750 router provides global Internet and company intranet access and includes the following:

- Voice-over-IP (VoIP) voice-and-data functionality; the router can carry voice traffic (for example, telephone calls and faxes) over an IP network
- Support for virtual private networking
- Modular architecture
- Network device integration

The Cisco 1750 router has the following hardware components:

- One autosensing 10/100 Fast Ethernet port, which operates in full- or half-duplex mode (with manual override available)
- One Voice interface card slot—Supports a single voice interface card (Table 4) with two ports per card
- Two WAN interface card slots for either WAN interface cards (WICs) or voice interface cards (VICs)
- Synchronous serial interfaces on serial WAN interface cards
- Asynchronous serial interfaces on serial WAN interface cards
- ISDN WAN interface cards—ISDN dialup and ISDN leased line (IDSL) at 144 kbps; encapsulation over ISDN leased line: Frame Relay and PPP
- One auxiliary (AUX) port (up to 115.2 kbps asynchronous serial)
- One console port
- One internal expansion slot—Supports future hardware-assisted services such as encryption (up to T1/E1) and compression processor
- RISC Processor—Motorola MPC860T PowerQUICC at 48 MHz
- One security slot that supports Kensington or similar lockdown equipment
- DRAM memory: 16 MB default, expandable to 48 MB
- Flash memory: 4 MB default, expandable to 16 MB
- Desktop form factor

The Cisco 1750 router also supports any combination of one or two of the following WAN interface cards, which are shared with the Cisco 1600, 1720, 2600, and 3600 routers:

- WIC-1T: One port high speed serial (sync/async)(T1/E1)
- WIC-2T: Two port high speed serial (sync/async) (T1/E1)
- WIC-2A/S: Two port low speed serial (sync/async) (up to 128 kbps)
- WIC-1B-S/T: One port ISDN BRI S/T
- WIC-1B-U: One port ISDN BRI U with integrated NT1
- WIC-1DSU-56K4: One port integrated 56/64 kbps 4-wire DSU/CSU
- WIC-1DSU-T1: One port integrated T1 / Fractional T1 DSU/CSU

The Cisco 1750 router supports any combination of one or two of the following voice interface cards, which are shared with the Cisco 2600 and 3600 routers:

- VIC-2FXS: Two port Foreign Exchange Station (FXS) voice/fax interface card for voice/fax network module
- VIC-2FXO: Two port Foreign Exchange Office (FXO) voice/fax interface card for voice/fax network module
- VIC-2FXO-EU: Two port FXO voice/fax interface card for Europe
- VIC-2E/M: Two port Ear & Mouth (E&M) voice/fax interface card for voice/fax network module

Determining the Software Version

To determine the version of Cisco IOS software running on your Cisco 1700 series router, log in to the router and enter the **show version** EXEC command:

```
router> show version
Cisco Internetwork Operating System Software
IOS (tm) 1700 Software (C1700-oy-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

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

Release 12.0 T supports the same feature sets as Release 12.0, but Release 12.0 T can include new features supported by the Cisco 1700 series.

Table 2 Feature Sets Supported by the Cisco 1700 Series

Feature Sets	Image Name	Feature Set Matrix Terms	Software Image	Platforms	In[1]
IP Feature Sets	IP	Basic[2]	c1700-y-mz	Cisco 1720	
				Cisco 1750	(7)
	IP Plus	Plus[3]	c1700-sy-mz	Cisco 1720	
				Cisco 1750	(7)
	IP Plus 40	Plus 40[4]	c1700-sy40-mz	Cisco 1720	
				Cisco 1750	(7)
	IP Plus 56	Plus 56[5]	c1700-sy56-mz	Cisco 1720	
				Cisco 1750	(7)
	IP Plus IPSEC 56	Plus, IPSec 56[6]	c1700-sy56i-mz	Cisco 1720	(3)
				Cisco 1750	(7)
	IP/IPX	Basic	c1700-ny-mz	Cisco 1720	
				Cisco 1750	(7)
	IP/IPX/AT/IBM	Basic	c1700-bnr2y-mz	Cisco 1720	
				Cisco 1750	(7)
	IP/IPX/AT/IBM Plus	Plus	c1700-bnr2sy-mz	Cisco 1720	
				Cisco 1750	(7)
	IP/Firewall	Basic	c1700-oy-mz	Cisco 1720	
				Cisco 1750	(7)
	IP/Firewall Plus IPSEC 56	Plus, IPSec 56	c1700-osy56i-mz	Cisco 1720	
				Cisco 1750	(7)
	IP/IPX/Firewall Plus	Plus	c1700-nosy-mz	Cisco 1720	
				Cisco 1750	(7)
	IP/IPX/AT/IBM/Firewall Plus IPSEC 56	Plus, IPSec 56	c1700-bnor2sy56i-mz	Cisco 1720	
				Cisco 1750	(7)
	IP Plus IPSEC 3DES	Plus, IPSec, 3DES[7]	c1700-k2sy-mz	Cisco 1720	
				Cisco 1750	(7)
	IP/Firewall Plus IPSEC 3DES	Plus, IPSec, 3DES	c1700-k2osy-mz	Cisco 1720	
				Cisco 1750	(7)
	IP/IPX/AT/IBM/Firewall Plus IPSEC 3DES	Plus, IPSec, 3DES	c1700-bk2nor2sy-mz	Cisco 1720	
				Cisco 1750	(7)

Table 2 Feature Sets Supported by the Cisco 1700 Series (continued)

Feature Sets	Image Name	Feature Set Matrix Terms	Software Image	Platforms	In[1]
IP/Voice Feature Sets	IP/Voice Plus	Plus, Voice[8]	c1700-sv3y-mz	Cisco 1750	(7)
	IP/Voice Plus 40	Plus 40, Voice	c1700-sv3y40-mz	Cisco 1750	(7)
	IP/Voice Plus 56	Plus 56, Voice	c1700-sv3y56-mz	Cisco 1750	(7)
	IP/Voice Plus IPSEC 56	Plus, Voice, IPSec 56	c1700-sv3y56i-mz	Cisco 1750	(7)
	IP/Voice Plus IPSEC 3DES	Plus, Voice, IPSec, 3DES	c1700-k2sv3y-mz	Cisco 1750	(7)
	IP/FW/Voice Plus	Plus, FW, Voice	c1700-osv3y-mz	Cisco 1750	(7)
	IP/FW/Voice Plus IPSEC 56	Plus, FW, Voice, IPSEC 56	c1700-osv3y56i-mz	Cisco 1750	(7)
	IP/FW/Voice Plus 3DES	Plus, FW, Voice, 3DES	c1700-k2osv3y-mz	Cisco 1750	(7)
	IP/IPX/FW/Voice Plus	Plus, IPX, FW, Voice	c1700-nosv3y-mz	Cisco 1750	(7)
	IP/IPX/AT/IBM/FW/Voice Plus IPSEC 56	Plus, IPX, AT, IBM, FW, Voice, IPSEC 56	c1700-bnor2sv3y56i-mz	Cisco 1750	(7)
	IP/IPX/AT/IBM/FW/Voice Plus 3DES	Plus, IPX, AT, IBM, FW, Voice, 3DES	c1700-bk2nor2sv3y-mz	Cisco 1750	(7)

[1] The number in the “In” column indicates the Cisco IOS release in which the feature was introduced. For example, (3) means a feature was introduced in Release 12.0(3)T. If a cell in this column is empty, the feature was included in the initial base 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 56-bit (Plus 56) data encryption feature sets.

[6] This feature set is offered in the encryption feature sets, which consist of IPSec 56-bit (Plus IPSec 56) data encryption feature sets.

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

[8] This set of features is provided in the Voice feature set.

⚠ **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 may require an export license. Customer orders may be denied or subject to delay due to United States government regulations. When applicable, the purchaser or the user must obtain local import and use authorizations for all encryption strengths. Contact your sales representative or distributor for more information, or send an e-mail to export@cisco.com.

Table 3 and Table 4 list the features and feature sets supported by the Cisco 1720 router in Cisco IOS Release 12.0 T, and Table 5 through Table 8 list the features and feature sets supported by the Cisco 1750 router in Cisco IOS Release 12.0 T. All the tables use the following conventions:

- Yes—The feature is supported in the software image.
- No—The feature is not supported in the software image.
- In—The number in the “In” column indicates the Cisco IOS release in which the feature was introduced. For example, (7) means a feature was introduced in Release 12.0(7)T. If a cell in this column is empty, the feature was included in the initial base release.

Note These feature set tables only contain a selected list of features. These tables are not cumulative— nor do they list all the features in each image.

Table 3 Feature List by Feature Set for the Cisco 1720 Router, Part 1

		Feature Sets						
Features	**In**	**IP**	**IP Plus**	**IP Plus 40**	**IP Plus 56**	**IP Plus IPSEC 56**	**IP/FW**	**IP/FW Plus IPSec 56**
Connectivity								
L2TP Dial-Out		Yes	Yes	Yes	Yes	Yes	No	Yes
IBM Support								
Bridging Code Rework		Yes	Yes	Yes	Yes	Yes	Yes	Yes
DSLw+ Ethernet Redundancy		No	No	No	No	No	No	No
IP Routing								
IP Type of Service and Precedence for GRE Tunnels		Yes	Yes	Yes	Yes	Yes	Yes	No
OSPF Point to Multipoint		Yes	No	No	No	No	Yes	No
Management								
Cisco IOS File System		Yes	Yes	Yes	Yes	Yes	Yes	Yes
Entity MIB		Yes	Yes	Yes	Yes	Yes	Yes	Yes
Expression MIB		Yes	Yes	Yes	Yes	Yes	Yes	Yes
Conditionally Triggered Debugging		Yes	Yes	Yes	Yes	Yes	Yes	Yes
Process MIB		Yes	Yes	Yes	Yes	Yes	Yes	Yes
Miscellaneous								
Multicast Source Discovery Protocol	(7)	TBD	TBD	TBD	TBD	TBD	TBD	TBD
X.25 Closed User Groups	(7)	TBD	TBD	TBD	TBD	TBD	TBD	TBD
X.25 Switch Local Acknowledgment	(7)	TBD	TBD	TBD	TBD	TBD	TBD	TBD
VPN Tunnel Management	(7)	TBD	TBD	TBD	TBD	TBD	TBD	TBD

Table 3 Feature List by Feature Set for the Cisco 1720 Router, Part 1 (continued)

		Feature Sets						
Features	**In**	**IP**	**IP Plus**	**IP Plus 40**	**IP Plus 56**	**IP Plus IPSEC 56**	**IP/FW**	**IP/FW Plus IPSec 56**
Multimedia								
Protocol-Independent Multicasts Version 2		Yes	Yes	Yes	Yes	Yes	Yes	Yes
Switching								
WCCPv2		No	Yes	Yes	Yes	Yes	No	Yes
WAN Services								
Always On/Direct ISDN		Yes	Yes	Yes	Yes	Yes	Yes	Yes
Dialer Watch		Yes	Yes	Yes	Yes	Yes	Yes	Yes
DLSw+ Enhancements		No	No	No	No	No	No	No
DLSw+ RSVP		No	No	No	No	No	No	No
MPPC-MS PPP Compression		Yes	Yes	Yes	Yes	Yes	Yes	Yes
MS Callback		Yes	Yes	Yes	Yes	Yes	Yes	Yes
VPDN MIB Feature		No	Yes	Yes	Yes	Yes	No	Yes

Table 4 Feature List by Feature Set for the Cisco 1720 Router, Part 2

		Feature Sets							
Features	**In**	**IP/IPX**	**IP/IPX/ FW Plus**	**IP/IPX/ AT/IBM**	**IP/IPX/ AT/IBM Plus**	**IP/IPX/ AT/IBM/ FW Plus IPSec 56**	**IP Plus IPSec 3DES**	**IP/FW Plus IPSec 3DES**	**IP/IPX/ AT/IBM/ FW Plus IPSec 3DES**
Connectivity									
L2TP Dial-Out		No	Yes	No	Yes	Yes	Yes	Yes	Yes
IBM Support									
Bridging Code Rework		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
DSLw+ Ethernet Redundancy		No	No	Yes	Yes	Yes	No	No	Yes
IP Routing									
IP Type of Service and Precedence for GRE Tunnels		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
OSPF Point to Multipoint		Yes	No	Yes	No	No	No	No	No
Management									
Cisco IOS File System		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Entity MIB		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Expression MIB		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Table 4 Feature List by Feature Set for the Cisco 1720 Router, Part 2 (continued)

		Feature Sets							
Features	**In**	**IP/IPX**	**IP/IPX/ FW Plus**	**IP/IPX/ AT/IBM**	**IP/IPX/ AT/IBM Plus**	**IP/IPX/ AT/IBM/ FW Plus IPSec 56**	**IP Plus IPSec 3DES**	**IP/FW Plus IPSec 3DES**	**IP/IPX/ AT/IBM/ FW Plus IPSec 3DES**
Conditionally Triggered Debugging		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Process MIB		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Miscellaneous									
Multicast Source Discovery Protocol	(7)	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD
X.25 Closed User Groups	(7)	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD
X.25 Switch Local Acknowledgment	(7)	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD
VPN Tunnel Management	(7)	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD
Multimedia									
Protocol-Independent Multicasts Version 2		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Switching									
WCCPv2		No	Yes	No	Yes	Yes	Yes	Yes	Yes
WAN Services									
Always On/Direct ISDN		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Dialer Watch		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
DLSw+ Enhancements		No	No	Yes	Yes	Yes	No	No	Yes
DLSw+ RSVP		No	No	No	Yes	Yes	No	No	Yes
MPPC-MS PPP Compression		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
MS Callback		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
VPDN MIB Feature		No	Yes	No	Yes	Yes	Yes	Yes	Yes

Table 5 Feature List by Feature Set for the Cisco 1750 Router, Part 1

	Feature Sets					
Features	IP	IP Plus	IP Plus 40	IP Plus 56	IP Plus IPSEC 56	IP Plus IPSec 3DES	IP/FW
Connectivity							
L2TP Dial-Out	Yes	Yes	Yes	Yes	Yes	Yes	No
IBM Support							
Bridging Code Rework	Yes	Yes	Yes	Yes	Yes	Yes	Yes
DSLw+ Ethernet Redundancy	No	No	No	No	No	No	No
IP Routing							
IP Type of Service and Precedence for GRE Tunnels	Yes	Yes	Yes	Yes	Yes	Yes	Yes
OSPF Point to Multipoint	Yes	No	No	No	No	No	Yes
Management							
Cisco IOS File System	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Entity MIB	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Expression MIB	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Conditionally Triggered Debugging	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Process MIB	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Multimedia							
Protocol-Independent Multicasts Version 2	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Switching							
WCCPv2	No	Yes	Yes	Yes	Yes	Yes	No
Voice Services							
Voice over IP	No	No	No	No	No	No	No
WAN Services							
Always On/Direct ISDN	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Dialer Watch	Yes	Yes	Yes	Yes	Yes	Yes	Yes
DLSw+ Enhancements	No	No	No	No	No	No	No
DLSw+ RSVP	No	No	No	No	No	No	No
MPPC-MS PPP Compression	Yes	Yes	Yes	Yes	Yes	Yes	Yes
MS Callback	Yes	Yes	Yes	Yes	Yes	Yes	Yes
VPDN MIB Feature	No	Yes	Yes	Yes	Yes	Yes	No

Table 6 Feature List by Feature Set for the Cisco 1750 Router, Part 2

				Feature Sets				
Features	**IP/IPX/ FW Plus**	**IP/FW Plus IPSec 56**	**IP/FW Plus IPSec 3DES**	**IP/IPX**	**IP/IPX/ AT/IBM**	**IP/IPX/ AT/IBM Plus**	**IP/IPX/ AT/IBM/ FW Plus IPSec 56**	**IP/IPX/ AT/IBM/ FW Plus IPSec 3DES**
Connectivity								
L2TP Dial-Out	Yes	Yes	Yes	No	No	Yes	Yes	Yes
IBM Support								
Bridging Code Rework	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
DSLw+ Ethernet Redundancy	No	No	No	No	Yes	Yes	Yes	Yes
IP Routing								
IP Type of Service and Precedence for GRE Tunnels	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes
OSPF Point to Multipoint	No	No	No	Yes	Yes	No	No	No
Management								
Cisco IOS File System	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Entity MIB	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Expression MIB	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Conditionally Triggered Debugging	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Process MIB	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Multimedia								
Protocol-Independent Multicasts Version 2	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Switching								
WCCPv2	Yes	Yes	Yes	No	No	Yes	Yes	Yes
Voice Services								
Voice over IP	No	No	No	No	No	No	No	No
WAN Services								
Always On/Direct ISDN	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Dialer Watch	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
DLSw+ Enhancements	No	No	No	No	Yes	Yes	Yes	Yes
DLSw+ RSVP	No	No	No	No	No	Yes	Yes	Yes
MPPC-MS PPP Compression	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
MS Callback	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
VPDN MIB Feature	Yes	Yes	Yes	No	No	Yes	Yes	Yes

Table 7 Feature List by Feature Set for the Cisco 1750 Router, Part 3

Features	Feature Sets					
	IP/Voice Plus	**IP/Voice Plus 40**	**IP/Voice Plus 56**	**IP/Voice Plus IPSEC 56**	**IP/Voice Plus IPSEC 3DES**	**IP/FW/Voice Plus**
Connectivity						
L2TP Dial-Out	Yes	Yes	Yes	Yes	Yes	Yes
IBM Support						
Bridging Code Rework	Yes	Yes	Yes	Yes	Yes	Yes
DSLw+ Ethernet Redundancy	No	No	No	No	No	No
IP Routing						
IP Type of Service and Precedence for GRE Tunnels	Yes	Yes	Yes	Yes	Yes	No
OSPF Point to Multipoint	No	No	No	No	No	No
Management						
Cisco IOS File System	Yes	Yes	Yes	Yes	Yes	Yes
Entity MIB	Yes	Yes	Yes	Yes	Yes	Yes
Expression MIB	Yes	Yes	Yes	Yes	Yes	Yes
Conditionally Triggered Debugging	Yes	Yes	Yes	Yes	Yes	Yes
Process MIB	Yes	Yes	Yes	Yes	Yes	Yes
Multimedia						
Protocol-Independent Multicasts Version 2	Yes	Yes	Yes	Yes	Yes	Yes
Switching						
WCCPv2	Yes	Yes	Yes	Yes	Yes	Yes
Voice Services						
Voice over IP	Yes	Yes	Yes	Yes	Yes	Yes
WAN Services						
Always On/Direct ISDN	Yes	Yes	Yes	Yes	Yes	Yes
Dialer Watch	Yes	Yes	Yes	Yes	Yes	Yes
DLSw+ Enhancements	No	No	No	No	No	No
DLSw+ RSVP	No	No	No	No	No	No
MPPC-MS PPP Compression	Yes	Yes	Yes	Yes	Yes	Yes
MS Callback	Yes	Yes	Yes	Yes	Yes	Yes
VPDN MIB Feature	Yes	Yes	Yes	Yes	Yes	Yes

Table 8 Feature List by Feature Set for the Cisco 1750 Router, Part 4

Features	Feature Sets				
	IP/FW/Voice Plus IPSEC 56	IP/FW/Voice Plus 3DES	IP/IPX/FW/ Voice Plus	IP/IPX/AT/IBM/FW/Voice Plus IPSEC 56	IP/IPX/AT/IBM/ FW/Voice Plus 3DES
Connectivity					
L2TP Dial-Out	Yes	Yes	Yes	Yes	Yes
IBM Support					
Bridging Code Rework	Yes	Yes	Yes	Yes	Yes
DSLw+ Ethernet Redundancy	No	No	No	Yes	Yes
IP Routing					
IP Type of Service and Precedence for GRE Tunnels	No	Yes	Yes	Yes	Yes
OSPF Point to Multipoint	No	No	No	No	No
Management					
Cisco IOS File System	Yes	Yes	Yes	Yes	Yes
Entity MIB	Yes	Yes	Yes	Yes	Yes
Expression MIB	Yes	Yes	Yes	Yes	Yes
Conditionally Triggered Debugging	Yes	Yes	Yes	Yes	Yes
Process MIB	Yes	Yes	Yes	Yes	Yes
Multimedia					
Protocol-Independent Multicasts Version 2	Yes	Yes	Yes	Yes	Yes
Switching					
WCCPv2	Yes	Yes	Yes	Yes	Yes
Voice Services					
Voice over IP	Yes	Yes	Yes	Yes	Yes
WAN Services					
Always On/Direct ISDN	Yes	Yes	Yes	Yes	Yes
Dialer Watch	Yes	Yes	Yes	Yes	Yes
DLSw+ Enhancements	No	No	No	Yes	Yes
DLSw+ RSVP	No	No	No	Yes	Yes
MPPC-MS PPP Compression	Yes	Yes	Yes	Yes	Yes
MS Callback	Yes	Yes	Yes	Yes	Yes
VPDN MIB Feature	Yes	Yes	Yes	Yes	Yes

New and Changed Information

The following sections list the new hardware and software features supported by the Cisco 1700 series for Release 12.0 T:

New Hardware Features in Release 12.0(7)T

The following new hardware enhancements are supported by the Cisco 1700 series for Release 12.0(7)T and later releases:

Support for the Cisco 1750 Router

Cisco IOS Release 12.0 T now includes support for the Cisco 1750 router. The Cisco 1750 router is a voice-and-data capable router that provides VoIP functionality and can carry voice traffic (for example, telephone calls and faxes) over an IP network. Cisco voice support is implemented using voice packet technology.

New Software Features in Release 12.0(7)T

The following new software enhancements are supported by the Cisco 1720 in Release 12.0(7)T and later releases.

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.

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—Cisco 1720 Only

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 Network Access Server (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 Software Features in Release 12.0(5)T

The following new software enhancements are supported by the Cisco 1720 in Release 12.0(5)T and later releases.

DLSw+ Ethernet Redundancy

The DLSw+ Ethernet Redundancy feature provides redundancy in an Ethernet environment. It enables DLSw+ to support parallel paths between two points in an Ethernet environment, ensuring resiliency in the case of a router failure and providing load balancing for traffic load.

DLSw+ could provide redundancy prior to this feature in a Token Ring environment or via backup peers. When an end station on an Ethernet LAN had multiple active paths into a DLSw+ network, problems occurred.

Redundancy is not possible in an Ethernet environment because, unlike Token Ring, it does not have a RIF field in its packet. The RIF notifies a router of the path a packet has traveled by tracking each ring number and bridge it travels along a path. If a bridge notices that the next ring matches a ring already in the RIF, then the frame is not copied on to that ring. The RIF prevents unreliable local reachability information, circuit contention, and undetected looping explorers.

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.

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.

No New Features in Release 12.0(4)T

There are no new features supported by the Cisco 1700 series in Cisco IOS Release 12.0(4)T.

New Software Features in Release 12.0(3)T

The following new software enhancements are supported by the Cisco 1720 in Release 12.0(3)T and later releases.

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 has developed to accommodate the many Cisco customers in Europe, where X.25 still is 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.

CDP Additions for Cisco IOS

The Cisco Discovery Protocol (CDP) is a media-independent device discovery protocol that runs on all cisco manufactured equipment, including routers, bridges, access servers, and switches. Each device sends periodic messages to a multicast address. Each device listens to the periodic messages sent by others in order to learn about neighboring devices and determine when their interfaces to the media go up or down. With CDP, network management applications can learn the device type and the SNMP agent address of neighboring devices. This process enables applications to send SNMP queries to neighboring devices.

CDP runs on all media that support Subnetwork Access Protocol (SNAP), including local-area network (LAN), Frame Relay, and Asynchronous Transfer Mode (ATM) media. CDP runs over the data link layer only. Therefore, two systems that support different network-layer protocols can learn about each other.

Each device configured for CDP sends periodic messages to a multicast address. Each device advertises at least one address at which it can receive SNMP messages. The advertisements also contain time-to-live, or holdtime, information, which indicates the time a receiving device should hold CDP information before discarding it.

Additions for Cisco Discovery Protocol (CDP) include the following:

- New SYSLOG output for instances of mismatching native VLAN IDs (IEEE 802.1Q) on connecting ports and port duplex state values on connecting devices.
- **The command cdp advertise-v2** and new output from the command **show cdp**.

The benefits include, transparent support of X.25 encapsulation over the Frame Relay network; direct X.25 configurations on a per DLCI basis; multiple Annex G DLCIs can use the same X.25 profile; multiple logical X.25 SVCs per Annex G link, and the fact that Cisco routers already contain the functionality necessary to perform the framing and frame removal required by Annex G.

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 hog all 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 it's share of the output interface buffer resource the packets of the flow are penalized by increasing the probability of their drop (by WRED).

Multilink Inverse Multiplexer

The Multilink Point to Point Protocol (MLP) Inverse Multiplexer feature allows you to combine multiple T1/E1 lines in a Versatile Interface Processor (VIP) T1/E1 interface into a bundle that has the combined bandwidth of the multiple T1/E1 lines. This is done by using a VIP MLP link. You choose the number of bundles and the number of T1/E1 lines in each bundle. This allows you to increase the bandwidth of you network links beyond that of a single T1/E1 line without having to purchase a T3 line.

NetFlow Policy Routing

IP policy routing now works with Cisco Express Forwarding (CEF), Distributed CEF (DCEF), NetFlow, and NetFlow with flow acceleration. IP policy routing was formerly supported only in fast-switching and process-switching. Now that policy routing is integrated into CEF, policy routing can be deployed on a wide scale and on high-speed interfaces.

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. In addition, this MIB provides CPU utilization and memory allocation/deallocation statistics for each process on each CPU listed in the CISCO-PROCESS-MIB.

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.

SLIP-PPP Banner and Banner Tokens

The SLIP-PPP Banner section of this feature enables you to configure the banner that is displayed when making a SLIP connection. This improves compatibility with non-Cisco SLIP dial-up software.

The Banner Tokens section of this feature introduces the use of tokens to all existing banner commands. Tokens allow you to display current information from the configuration, such as the router’s hostname, IP address, encapsulation type, and MTU size.

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 can 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 re-ordered, 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. They are:
  - Communication without authentication and privacy (NoAuthNoPriv)
  - Communication with authentication and without privacy (AuthNoPriv)
  - Communication with authentication and privacy (AuthPriv)

X.25 Load Balancing

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

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 Software Features in Release 12.0(2)T

The following new software enhancement is supported by the Cisco 1720 router in Release 12.0(2)T and later releases.

Cisco IOS DHCP Server

With the introduction of Cisco IOS Easy IP Phase 2, Cisco IOS software supports Cisco IOS Dynamic Host Control Protocol (DHCP) Server functionality. DHCP is a protocol that enables you to automatically assign reusable IP addresses to clients. Cisco IOS DHCP server is a full DHCP server implementation that assigns and manages IP addresses from specified address pools within the router to DHCP hosts.

Also, Cisco IOS Easy IP Phase 2 supports DHCP Relay Agent functionality. A DHCP relay agent is any host that forwards DHCP packets between clients and servers with the goal of automatically assigning an IP address and address parameters to a client requesting an address. A DHCP relay agent 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 can forward the DHCP request to one or more secondary DHCP servers defined by the network administrator.

New Software Features in Release 12.0(1)T

The following new software enhancements are supported by the Cisco 1720 router in Release 12.0(1)T and later releases.

OSPF Packet Pacing

The former OSPF implementation for sending update packets needed to be more efficient. Some update packets were getting lost in cases where the link was slow, a neighbor could not receive the updates fast enough, or the router was out of buffer space. For example, packets might be 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. Also, you can display the LSAs waiting to be sent out an interface.

Time-Based Access Lists

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

Currently, IP and IPX extended access lists are the only functions that can use time ranges. The time range allows the network administrator to define when the permit or deny statements in the access list are in effect. Prior to this feature, access list statements were always in effect once they were applied. Both named or numbered access lists can reference a time range.

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 potential 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 could be short and relatively infrequent.

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

- Periodic broadcasting by RIP generally prevented WAN circuits form 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 hits 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.

Cisco IOS Firewall Feature Set Platform Support

The Cisco IOS Firewall feature set is now available on Cisco 2600 and 3600 series products. The Cisco IOS Firewall feature set extends the security technology currently available in Cisco IOS software to provide firewall specific capabilities:

- Context-based Access Control (CBAC)
- Java blocking
- Denial-of-service detection and prevention
- Real-time alerts and audit trails

The Cisco IOS Firewall feature set adds advanced filtering capabilities to existing security functionality in Cisco routers. Some existing Cisco IOS security features include packet filtering via access control lists (ACLs), Network Address Translation (NAT), network-layer encryption, and TACACS+ authentication.

IOS STP Enhancements

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

Layer Two Tunneling Protocol (L2TP)

Layer Two 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 Two 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 mobile users to connect to their corporate intranets or extranets, thus improving flexibility and reducing costs.

Traditional dial-up networking services only supported registered IP address, 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. This allows the existing access infrastructure, such as the Internet, modems, access servers, and ISDN terminal adaptors (TAs), to be used.

L2TP can be initiated wherever PPTP or L2F is currently deployed and can be operated as a client initiated tunnel, such as PPTP, or a network access server (NAS) initiated tunnel, such as L2F.

Important Notes

The following sections contain important notes about Cisco IOS Release 12.0 that can apply to the Cisco 1700 series. (Also, see the "Caveats" section on page 31.)

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 12.1mainline 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.

Using the boot flash Command

Booting a Cisco 1700 series router with the commands **boot flash** or **boot system flash** results in unpredictable behavior. To work around this problem, be sure to enter a colon (:) following both commands (for example, **boot flash:** or **boot system flash:**).

Fan Operation in Cisco 1720 Router

Be advised that the fans in the Cisco 1720 router stay off until needed.

Flash defaults to Flash:1 on Multipartition Flash

When using a multipartition flash card, the various flash partitions are referred to as "flash:1:", "flash:2:", etc. If you specify only "flash" in a multipartition flash, the parser assumes "flash:1:." For example, if you enter **show flash all** the parser defaults to "show flash:1: all" and only the flash information for the first partition displays. To see information for all flash partitions, enter **show flash ?**. This will list all of the valid partitions. Then enter **show flash:xx: all** on each valid partition.

Traffic Shaping

On the ATM25 interface of the C1400 there are two types of traffic shaping: hardware-based and software-based. Hardware-based traffic shaping is provided by the ATM SAR chip and is enabled on a per-pvc basis by one of the following IOS PVC configuration commands:

```
ubr     <peak-cell-rate>
ubr+    <peak-cell-rate> <minimum-guaranteed-cell-rate>
vbr-nrt <peak-cell-rate> <sustainable-cell-rate> <maximum-burst-size>
```

The SAR chip has “rate counters” that control the rate at which the current buffer up for segmentation is going to be transmitted. Ideally, the SAR chip could be programmed with values for all of the above command parameters. Unfortunately, it only has the rate counters, which specify a divisor of the basic line rate of 25 Mbps and which really sets the maximum transmission rate (peak-cell-rate) for the channel. Note that with the “ubr” and “ubr+” commands, the rate counter for the PVC is obtained from the <peak-cell-rate> parameter. With the “vbr-nrt” command, the rate counter is obtained from the <sustainable-cell-rate> parameter. While the <minimum-guaranteed-cell-rate> parameter in the “ubr+” command and the <peak-cell-rate> parameter in the “vbr-nrt” command can be specified by the user, they are ignored by the ATM25 driver.

Software-based traffic shaping is enabled on a per-interface basis via the “traffic-shape” interface configuration command. For performance reasons, and since for ATM interfaces you most likely want to do shaping on a per-pvc basis, the ATM driver does not support software-based traffic shaping while fastswitching. However, if fast-switching is disabled and the “traffic-shape” interface configuration command is enabled, then software traffic shaping will occur. (See CSCdk28377 for more information).

Deferral of Cisco 1720 Images Prior to Release 12.0(4)T

The Cisco 1720 router experiences “WatchDog Timeout” Errors when trying to get a stack trace. This problem affects all Cisco IOS images prior to Release 12.0(4)T, making it difficult to debug potential problems. To work around this, Cisco recommends you upgrade your router to Release 12.0(4)T or higher.

Cisco IOS Syslog Failure

Certain versions of Cisco IOS software may fail or hang when they receive invalid User Datagram Protocol (UDP) packets sent to their syslog ports (port 514). At least one commonly used Internet scanning tool generates packets that cause such problems. This fact has been published on public Internet mailing lists, which are widely read both by security professionals and by security crackers. This information should be considered in the public domain.

Attackers can cause Cisco IOS devices to repeatedly fail and reload, resulting in a completely disabled Cisco IOS device that needs to be reconfigured by its administrator. Some Cisco IOS devices have been observed to hang instead of failing when attacked. These devices do not recover until they are manually restarted by reset or power cycling. An administrator must personally visit an attacked, hung device to restart it, even if the attacker is no longer actively sending any traffic. Some devices have failed without providing stack traces; some devices may indicate that they were “restarted by power-on,” even when that is not the case.

Assume that any potential attacker is likely to know that existence of this problem and the ways to exploit it. An attacker can use tools available to the public on the Internet and does not need to write any software to exploit the vulnerability. Minimal skill is required and no special equipment is required.

Despite Cisco specifically inviting such reports, Cisco has received no actual reports of malicious exploitation of this problem.

This vulnerability notice was posted on Cisco's World Wide Web site:

http://www.cisco.com/warp/public/770/iossyslog-pub.shtml

This information was also sent to the following e-mail and USENET news recipients:

- cust-security-announce@cisco.com
- bugtraq@netspace.org
- first-teams@first.org (includes CERT/CC)
- first-info@first.org
- cisco@spot.colorado.edu
- comp.dcom.sys.cisco
- nanog@merit.edu

Affected Devices and Software Versions

Vulnerable devices and software versions are specified in Table 9, *Affected and Repaired Software Versions*. Affected versions include Releases 11.3 AA, 11.3 DB, and all 12.0 versions (including 12.0 mainline, 12.0 S, 12.0 T, and any other regular released version whose number starts with 12.0), up to the repaired releases listed in Table 9. Cisco is correcting the problem in certain special releases and will correct it in future maintenance and interim releases. See Table 9, *Affected and Repaired Software Versions* for details. Cisco intends to provide fixes for all affected IOS variants.

No particular configuration is needed to make a Cisco IOS device vulnerable. It is possible to filter out attack traffic by using access lists. See the "Workarounds" section on page 28 for techniques. However, except at Internet firewalls, the appropriate filters are not common in customer configurations. Carefully evaluate your configuration before assuming that any filtering you have protects you against this attack.

The most commonly used or asked-about products are listed below. If you are unsure whether your device is running Cisco IOS software, log in to the device and issue the **show version** command. Cisco IOS software will identify itself simply as "IOS" or "Internetwork Operating System Software". Other Cisco devices will not have the **show version** command, or they will identify themselves differently in their output. The most common Cisco devices that run Cisco IOS software include the following:

- Cisco routers in the AGS/MGS/CGS/AGS+, IGS, RSM, 800, uBR900, 1000, 2500, 2600, 3000, 3600, 3800, 4000, 4500, 4700, AS5200, AS5300, AS5800, 6400, 7000, 7200 (including the uBR7200), 7500, and 12000 series
- Most recent versions of the LS1010 ATM switch
- Some versions of the Catalyst 2900XL LAN switch
- Cisco DistributedDirector

Affected software versions, which are relatively new, are not necessarily available on every device listed above. If you are not running Cisco IOS software, you are not affected by this problem.

The following Cisco devices are *not* affected:

- 700 dialup routers (750, 760, and 770 series)
- Catalyst 1900, 2800, 2900, 3000, and 5000 LAN switches are not affected, except for some versions of the Catalyst 2900XL. However, optional router modules running Cisco IOS software in switch backplanes, such as the RSM module for the Catalyst 5000 and 5500, are affected.
- WAN switching products in the IGX and BPX lines

- MGX (formerly known as the AXIS shelf)
- Host-based software
- Cisco PIX Firewall
- Cisco LocalDirector
- Cisco Cache Engine

This vulnerability has been assigned Cisco bug ID CSCdk77426.

Solution

Cisco offers free software updates to correct this vulnerability for all affected customers—regardless of their contract status. However, because this vulnerability information has been disseminated by third parties, Cisco has released this notice before updates are available for all software versions. Table 9 gives Cisco's projected fix dates.

Make sure your hardware has adequate RAM to support the new software before installing it. The amount of RAM is seldom a problem when you upgrade within a major release (say, from 11.2[11]P to 11.2[17]P), but it is often a factor when you upgrade between major releases (say, from 11.2 P to 11.3 T).

Because fixes will be available for all affected releases, this vulnerability will rarely, if ever, require an upgrade to a new major release. Cisco recommends very careful planning for any upgrade between major releases. Make certain no known bugs will prevent the new software from working properly in your environment.

Further upgrade planning assistance is available on Cisco's World Wide Web site at:

http://www.cisco.com

If you have service contracts you can obtain new software through your regular update channels (generally through Cisco's World Wide Web site). You can upgrade to any software release, but you must remain within the boundaries of the feature sets you have purchased.

If you do not have service contracts, you can upgrade to obtain only the bug fixes; free upgrades are restricted to the minimum upgrade required to resolve the defects. In general, you will be restricted to upgrading within a single row of Table 9, except when no upgrade within the same row is available in a timely manner. Obtain updates by contacting one of the following Cisco Technical Assistance Centers (TACs):

- +1 800 553 2447 (toll-free from within North America)
- +1 408 526 7209 (toll call from anywhere in the world)
- tac@cisco.com

Give the URL of this notice (http://www.cisco.com/warp/public/770/iossyslog-pub.shtml) as evidence for a free update. Non-contract customers must request free updates through the TAC. Please do not contact either "psirt@cisco.com" or "security-alert@cisco.com" for software updates.

Workarounds

You can work around this vulnerability by preventing any affected Cisco IOS device from receiving or processing UDP datagrams addressed to its port 514. This can be done either by using packet filtering on surrounding devices, or by using input access list filtering on the affected IOS device itself.

If you use an input access list, apply that list to all interfaces to which attackers may be able to send datagrams. Interfaces include not only physical LAN and WAN interfaces but also virtual subinterfaces of those physical interfaces, as well as virtual interfaces and interface templates corresponding to GRE, L2TP, L2F, and other tunneling protocols.

The input access list must block traffic destined for UDP port 514 at any of the Cisco IOS device's own IP addresses, as well as at any broadcast or multicast addresses on which the Cisco IOS device may be listening. Be sure to block both old-style "all-zeros" broadcasts and new-style "all-ones" broadcasts. It is not necessary to block traffic being forwarded to other hosts—only traffic actually addressed to the Cisco IOS device is of interest.

No single input access list works in all configurations. Know the effect of your access list in your specific configuration before activating it.

The following example shows a possible access list for a three-interface router, along with the configuration commands needed to apply the list. The example assumes input filtering is not needed, other than as a workaround for this problem:

```
! Deny all multicasts, and all unspecified-net broadcasts, to port 514
access-list 101 deny udp any 224.0.0.0 31.255.255.255 eq 514
! Deny old-style unspecified-net broadcasts
access-list 101 deny udp any host 0.0.0.0 eq 514
! Deny network-specific broadcasts. This example assumes that all of
! the local interfaces are on the class B network 172.16.0.0, subnetted
! everywhere with mask 255.255.255.0. This will differ from network
! to network. Note that we block both new-style and old-style broadcasts.
access-list 101 deny udp any 172.16.0.255 0.0.255.0 eq 514
access-list 101 deny udp any 172.16.0.0   0.0.255.0 eq 514
! Deny packets sent to the addresses of our own network interfaces.
access-list 101 deny udp any host 172.16.1.1 eq 514
access-list 101 deny udp any host 172.16.2.1 eq 514
access-list 101 deny udp any host 172.16.3.3 eq 514
! Permit all other traffic (default would be to deny)
access-list 101 permit ip any any

! Apply the access list to the input side of each interface
interface ethernet 0
ip address 172.16.1.1 255.255.255.0
ip access-group 101 in

interface ethernet 2
ip address 172.16.2.1 255.255.255.0
ip access-group 101 in

interface ethernet 3
ip address 172.16.3.3 255.255.255.0
ip access-group 101 in
```

Listing all possible addresses—especially all possible broadcast addresses—to which attack packets may be sent is complicated. If you do not need to forward any legitimate syslog traffic received on an interface, you can block all syslog traffic arriving on that interface. Remember that blocking will affect traffic routed through the Cisco IOS device as well as traffic destined to the device; if the IOS device is expected to forward syslog packets, you will have to do the detailed filtering. Because input access lists impact system performance, install them with caution—especially on systems running very near their capacity.

Software Versions and Fixes

Many Cisco software images have been or will be specially reissued to correct this vulnerability. For example, regular released Cisco IOS version 12.0(2) is vulnerable, as are interim versions 12.0(2.1) through 12.0(2.3). The first fixed interim version of Release12.0 mainline software is Release12.0(2.4). However, a special release, 12.0(2a), contains only the fix for this vulnerability and does not include any other bug fixes from later 12.0 interim releases.

If you are running Release 12.0(2) and want to fix this problem without risking possible instability presented by installing the 12.0(2.4) interim release, you can upgrade to Release 12.0(2a). Release 12.0(2a) is a “code branch” from the Release 12.0(2) base, which will merge back into the Release 12.0 mainline at Release 12.0(2.4).

Special releases, like 12.0(2a), are one-time, spot fixes, and they will not be maintained. Thus, the upgrade path from Release 12.0(2a) is to Release 12.0(3).

Table 9 specifies information about affected and repaired software versions.

Note All dates within this table are subject to change.

Table 9 Affected and Repaired Software Versions

Cisco IOS Major Release	Description	Special Fix[1]	First Fixed Interim Release[2]	Fixed Maintenance Release[3]
Unaffected Releases				
11.2 and earlier releases—all variants	Unaffected early releases (no syslog server)	Unaffected	Unaffected	Unaffected
11.3, 11.3 T, 11.3 DA, 11.3 MA, 11.3 NA, 11.3 WA, 11.3(2)XA	11.3 releases without syslog servers	Unaffected	Unaffected	Unaffected
Releases Based on 11.3				
11.3 AA	11.3 early deployment for AS58xx	11.3(7)AA2, 8-JAN-1999[4]	11.3(7.2)AA	11.3(8)AA, 15-FEB-1999
11.3 DB	11.3 for Cisco NRP routing blade in Cisco 6400 xDSL DSLAM			11.3(7)DB2, 18-JAN-1999
Releases Based on 12.0				
12.0	12.0 Mainline	12.0(2a), 8-JAN-1999	12.0(2.4)	12.0(3), 1-FEB-1999
12.0 T	12.0 new technology early deployment	12.0(2a)T1, 11-JAN-1999	12.0(2.4)T	12.0(3)T, 15-FEB-1999
12.0 S	ISP support; 7200, RSP, GSR		12.0(2.3)S, 27-DEC-1998	12.0(2)S[5], 18-JAN-1999
12.0 DB	12.0 for Cisco 6400 universal access concentrator node switch processor (lab use)			12.0(2)DB, 18-JAN-1999

Table 9 Affected and Repaired Software Versions (continued)

Cisco IOS Major Release	Description	Special Fix[1]	First Fixed Interim Release[2]	Fixed Maintenance Release[3]
12.0(1)W	12.0 for Catalyst 8500 and LS1010	12.0(1)W5(5a) and 12.0(1a)W5(5b) (LS1010 platform only)	12.0(1)W5(5.15)	12.0(1)W5(6) (platform support for Catalyst 8540M will be in 12.0(1)W5(7))
12.0(0.6)W5	One-time early deployment for CH-OC-12 module in Catalyst 8500 series switches	Unaffected; one-time release	Unaffected	Unaffected; To upgrade use 12.0(1)W5 releases.
12.0(1)XA3	Short-life release; merged to 12/0T at 12.0(2)T	Obsolete	Merged	Upgrade to 12.0(2a)T1 or to 12.0(3)T.
12.0(1)XB	Short-life release for Cisco 800 series; merged to 12.0 T and 12.0 (3)T	12.0(1)XB1	Merged	Upgrade to 12.0(3)T.
12.0(2)XC	Short-life release for new features in Cisco 2600, Cisco 3600, uBR7200, uBR900 series; merged to 12.0 T at 12.0(3)T	12.0(2)XC1, 7-JAN-1999	Merged	Upgrade to 12.0(3)T
12.0(2)XD	Short-life release for ISDN voice features; merged to 12.0 T at 12.0(3)T	12.0(2)XD1, 18-JAN-1999	Merged	Upgrade to 12.0(3)T
12.0(1)XE	Short-life release	12.0(2)XE, 18-JAN-1999	Merged	Upgrade to 12.0(3)T

[1] A special fix is a one-time release that provides the most stable immediate upgrade path.

[2] Interim releases are tested less rigorously than regular maintenance releases; interim releases can contain serious bugs.

[3] Fixed maintenance releases are on a long-term upgrade path. Other long-term upgrade paths also exist.

[4] All dates in this table are estimates and are subject to change.

[5] This entry is not a misprint. The 12.0(2.3)S interim release is available before the 12.0(2)S regular release.

Caveats

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

This section only contains open and resolved caveats for the current Cisco IOS maintenance release.

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

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

For information on caveats in Cisco IOS Release 12.0 T, see *Caveats for Cisco IOS Release 12.0 T,* 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 IOS BugToolkit: Cisco Bug Navigator II**, or at http://www.cisco.com/support/bugtools

Caveats for Release 12.0(7)T

This section describes possibly unexpected behavior by Release12.0(7)T, specific to the Cisco 1700 series routers. Only severity 1 and 2 caveats are included.

CSCdm55698

Cisco 1720 or 1750 routers may reload periodically in some application environments. This will disrupt routing for 2 to 4 minutes when the unit is rebooted. The susceptible environment typically uses 100BaseT and high speed WAN ports, or ISDN connections. A limited cases have also been reported, but not reproduced, in 10BaseT and other less stressful environments.

To work around this problem, run the Ethernet at 10BaseT. If problems persist, contact TAC.

CSCdp18521

Under maximal operating conditions (such as the heavy on-and-off-hook cycling of one or more directly connected telephones or heavy voice traffic), while debug messages are turned on and routed to the console), voice Digital Signal Processors (DSPs) on the Packet Voice DSP Modules (PVDM) module can become unresponsive and drop all calls. To work around this problem, reboot the router.

CSCdp60086

The **frame-relay tunnel** subcommand is not available on the Cisco 1600, 1700, and 800 series platforms. This subcommand is only available in IOS images corresponding to Enterprise feature sets:

```
router(config-if)# frame-relay route 19 interface ?
    Serial Serial
    Tunnel Tunnel interface
```

CSCdp62429

It is possible for Cisco 1700 series routers to fail to boot Cisco IOS Release 12.0(7)T. There is a workaround for this problem.

The circumstances can only arise if one of the following is true:

- The router has 16 MB of DRAM and is configured with **memory-size iomem 10**
- The router has 32 MB of DRAM and is configured with **memory-size iomem 5**

If one of the above is true, then while loading Cisco IOS Release 12.0(7)T, it is possible that you will see one of several error messages indicating that the router does not have enough memory. In fact, the router has enough memory, but the relative quantities of process vs. I/O memory need to be reconfigured.

To avoid the problem, one must ensure:

- A router with 16 MB of DRAM must have at least **memory-size iomem 15**
- A router with 32 MB of DRAM must have at least **memory-size iomem 10**

Cisco IOS Release 12.0(7)T images will not boot if a router has less than 1.7 MB of I/O memory configured. The amount of I/O memory configured can be seen with the **show version** command as the quantity after the "/" in the memory size report. Since it is configured as a percentage of main memory, a problem occurs, for example, if a user has configured **memory-size iomem 10** on a router with 16 MB of memory. This command will be allowed, and will work with older images, but the new Cisco IOS Release 12.0(7)T will not boot.

To work around the problem, you need to boot the old image, so that you will have access to the console so that you can reconfigure the router to an increased I/O memory percentage.

From rommon (either send a break within 60 seconds after image decompression, or you might already be there after the image fails to boot):

```
confreg 0x0
reset
```

[Now follow instructions for disaster recovery on pages B-5 and B-6 of the *Cisco 1700 Router Software Configuration Guide* involving the **tftpdnld** command.]

```
confreg 0x2102
reset
```

Now the router should boot with the old image. The next step is to change the configuration to increase the I/O memory percentage. Use 15% if you have 16 MB of DRAM, or 10% if you have 32 MB of DRAM. For example, if you have 16 MB of DRAM:

```
enable
conf t
memory-size iomem 15
<Ctrl-Z>
wr mem
reload
```

The router will reboot and you should verify with the **show version** that you have more than 1.7 MB of I/O memory (the quantity after the "/" in the memory size report). In this example, it will show 2.4 MB of memory (15% of 16 MB).

You can then proceed with **copy tftp flash** and upgrade to Cisco IOS Release 12.0(7)T.

Future Cisco IOS Releases will automatically reconfigure the amount of I/O memory in the router, so that this problem will not occur.

Related Documentation

The following sections describe the documentation available for the Cisco 1700 series. 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 34
- Platform-Specific Documents, page 35
- Feature Modules, page 36
- Cisco IOS Software Documentation Set, page 36

Release-Specific Documents

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

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

  On CCO at:

  Technical Documents: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 12.0: Release Notes: Cross-Platform Release Notes

  On the Documentation CD-ROM at:

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

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

  Service & Support: Technical Documents

- *Caveats for Cisco IOS Release* 12.0 T

  This document contains caveats applicable to all platforms for all maintenance releases of Release 12.0 T.

  On CCO at:

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

  On the Documentation CD-ROM at:

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

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 IOS BugToolkit: Cisco Bug Navigator II**, or at http://www.cisco.com/support/bugtools

Platform-Specific Documents

Cisco 1720

These documents are available for the Cisco 1720 router on CCO and the Documentation CD-ROM:

- *Installing Your Cisco 1720*
- *Cisco 1720 Router Hardware Installation Guide*
- *Cisco 1700 Router Software Configuration Guide*
- *Regulatory Compliance and Safety Information*
- Configuration Notes
- Release Notes for the Cisco 1720 Router
- *WAN Interface Cards Hardware Installation Guide*

On CCO at:

Technical Documents: Documentation Home Page: Access Servers and Access Routers: Modular Access Routers: Cisco 1720 Router

On the Documentation CD-ROM at:

Cisco Product Documentation: Access Servers and Access Routers: Modular Access Routers: Cisco 1720 Router

Cisco 1750

These documents are available for the Cisco 1750 router on CCO and the Documentation CD-ROM:

- *Cisco 1750 Router Hardware Installation Guide*
- Safety Information for Cisco 1600 and 1700 Routers
- *Cisco 1750 Router Voice over IP Configuration Guide*
- *Voice-over-IP Quick Start Guide*
- Release Notes for the Cisco 1750 Router

On CCO at:

Technical Documents: Documentation Home Page: Access Servers and Access Routers: Modular Access Routers: Cisco 1750 Router

On the Documentation CD-ROM at:

Cisco Product Documentation: Access Servers and Access Routers: Modular Access Routers: Cisco 1750 Router

Feature Modules

Feature modules describe new features supported by Release 12.0 T and are updates to the Cisco IOS documentation set. A feature module consists of a brief overview of the feature, benefits, configuration tasks, and a command reference. As updates, the feature modules are available online only. Feature module information is incorporated in the next printing of the Cisco IOS documentation set.

On CCO at:

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

On the Documentation CD-ROM at:

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

Cisco IOS Software Documentation Set

The Cisco IOS software documentation set consists of the Cisco IOS configuration guides, Cisco IOS command references, and several other supporting documents that are shipped with your order in electronic form on the Documentation CD-ROM—unless you specifically 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, Cisco IOS software functionality, and contain comprehensive configuration examples. Chapters in a command reference provide complete command syntax information. Use each configuration guide with its corresponding command reference.

On 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 at:

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

Release 12.0 Documentation Set

Table 10 describes the contents of the Cisco IOS Release 12.0 software documentation set, which is available in electronic form and 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 hard-copy documents were printed.

On CCO at:

Service & Support: 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 10 Cisco IOS Software Release 12.0 Documentation Set

Books	Chapter Topics
• *Configuration Fundamentals Configuration Guide* • *Configuration Fundamentals Command Reference*	Configuration Fundamentals Overview Cisco IOS User Interfaces File Management System Management
• *Bridging and IBM Networking Configuration Guide* • *Bridging and IBM Networking Command Reference*	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

Table 10 Cisco IOS Software Release 12.0 Documentation Set (continued)

Books	Chapter Topics
• *Dial Solutions Configuration Guide* • *Dial Solutions Command Reference*	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
• *Cisco IOS Interface Configuration Guide* • *Cisco IOS Interface Command Reference*	Interface Configuration Overview LAN Interfaces Logical Interfaces Serial Interfaces
• *Network Protocols Configuration Guide, Part 1* • *Network Protocols Command Reference, Part 1*	IP Overview IP Addressing and Services IP Routing Protocols
• *Network Protocols Configuration Guide, Part 2* • *Network Protocols Command Reference, Part 2*	AppleTalk Novell IPX
• *Network Protocols Configuration Guide, Part 3* • *Network Protocols Command Reference, Part 3*	Network Protocols Overview Apollo Domain Banyan VINES DECnet ISO CLNS XNS
• *Security Configuration Guide* • *Security Command Reference*	AAA Security Services Security Server Protocols Traffic Filtering and Firewalls IP Security and Encryption Passwords and Privileges Neighbor Router Authentication IP Security Options
• *Cisco IOS Switching Services Configuration Guide* • *Cisco IOS Switching Services Command Reference*	Switching Services Switching Paths for IP Networks Virtual LAN (VLAN) Switching and Routing

Table 10 Cisco IOS Software Release 12.0 Documentation Set (continued)

Books	Chapter Topics
• *Wide-Area Networking Configuration Guide* • *Wide-Area Networking Command Reference*	Wide-Area Network Overview ATM Frame Relay SMDS X.25 and LAPB
• *Voice, Video, and Home Applications Configuration Guide* • *Voice, Video, and Home Applications Command Reference*	Voice over IP Voice over Frame Relay Voice over ATM Voice over HDLC Frame Relay-ATM Internetworking Synchronized Clocks Video Support Universal Broadband Features
• *Quality of Service Solutions Configuration Guide* • *Quality of Service Solutions Command Reference*	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
• *Cisco IOS Software Command Summary* • *Dial Solutions Quick Configuration Guide* • *System Error Messages* • *Debug Command Reference*	

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: **Service & Support: 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* that 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 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 reach 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 package that 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 34.