Release Notes for the Cisco 1750 Router for Cisco IOS Release 12.0(5)XQ

December 1, 1999

Cisco IOS Release 12.0(5)XQ

Text Part Number 78-7143-02

These release notes describe new features and significant software components for the Cisco 1750 router that supports Cisco IOS Release 12.0 T, up to and including Release 12.0(5)XQ. These release notes are updated as needed to describe new memory requirements, new features, new hardware support, software platform deferrals, microcode or modem code changes, related document changes, and any other important changes. Use these release notes with the C*ross-Platform Release Notes for Cisco IOS Release 12.0 T* located on CCO and the Documentation CD-ROM.

For a list of the software caveats that apply to Release 12.0(5)XQ, refer to 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.

Contents

These release notes discuss the following topics:

CISCO SYSTEMS

System Requirements

This section describes the system requirements for Release 12.0(5)XQ and includes the following sections:

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

Memory Requirements

This section describes the memory requirements for the Cisco IOS feature sets supported by Cisco IOS Release 12.0(5)XQ on the Cisco 1750 router.

Table 1   *Memory Requirements for the Cisco 1750 Routers*

Feature Sets	Image Name	Software Image	Required Flash Memory	Required DRAM Memory	Runs from
IP Feature Sets	IP	c1700-y-mz	4MB	16MB	RAM
	IP Plus	c1700-sy-mz	4MB	16MB	RAM
	IP Plus 40	c1700-sy40-mz	4MB	20MB	RAM
	IP Plus 56	c1700-sy56-mz	8MB	20MB	RAM
	IP Plus IPSEC 56	c1700-sy56i-mz	8MB	20MB	RAM
	IP Plus IPSEC 3DES	c1700-k2sy-mz	8MB	20MB	RAM
	IP/FW	c1700-oy-mz	4MB	16MB	RAM
	IP/IPX/FW Plus	c1700-nosy-mz	8MB	20MB	RAM
	IP/FW Plus IPSEC 56	c1700-osy56i-mz	8MB	24MB	RAM
	IP/FW Plus IPSEC 3DES	c1700-k2osy-mz	8MB	24MB	RAM
	IP/IPX	c1700-ny-mz	4MB	16MB	RAM
	IP/IPX/AT/IBM	c1700-bnr2y-mz	8MB	20MB	RAM
	IP/IPX/AT/IBM Plus	c1700-bnr2sy-mz	8MB	24MB	RAM
	IP/IPX/AT/IBM/FW Plus IPSEC 56	c1700-bnor2sy56i-mz	8MB	32MB	RAM
	IP/IPX/AT/IBM/FW Plus IPSEC 3DES	c1700-bk2nor2sy-mz	8MB	32MB	RAM
	IP/Voice Plus	c1700-sv3y-mz.120-5.XQ	8 MB	24 MB	RAM
	IP/Voice Plus 40	c1700-sv3y40-mz.120-5.XQ	8 MB	24 MB	RAM
	IP/Voice Plus 56	c1700-sv3y56-mz.120-5.XQ	8 MB	24 MB	RAM
	IP/Voice Plus IPSEC 56	c1700-sv3y56i-mz.120-5.XQ	8 MB	24 MB	RAM
	IP/Voice Plus IPSEC 3DES	c1700-k2sv3y-mz.120-5.XQ	8 MB	24 MB	RAM

Table 1   Memory Requirements for the Cisco 1750 Routers (continued)

Feature Sets	Image Name	Software Image	Required Flash Memory	Required DRAM Memory	Runs from
IP Feature Sets	IP/FW/Voice Plus	c1700-osv3y-mz.120-5.XQ	8 MB	24 MB	RAM
	IP/FW/Voice Plus IPSEC 56	c1700-osv3y56i-mz.120-5.XQ	8 MB	24 MB	RAM
	IP/FW/Voice Plus 3DES	c1700-k2osv3y-mz.120-5.XQ	8 MB	32 MB	RAM
	IP/IPX/FW/Voice Plus	c1700-nosv3y-mz.120-5.XQ	8 MB	24 MB	RAM
	IP/IPX/AT/IBM/FW/Voice Plus IPSEC 56	c1700-bnor2sv3y56i-mz.120-5.XQ	8 MB	32 MB	RAM
	IP/IPX/AT/IBM/FW/Voice Plus 3DES	c1700-bk2nor2sv3y-mz.120-5.XQ	8 MB	32 MB	RAM

Hardware Supported

Cisco IOS Release 12.0(5)XQ supports the Cisco 1750 Routers. For detailed descriptions of the new hardware features, refer to the "New and Changed Information" section on page 13.

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)
- Two WAN interface card slots for either WAN interface cards (WICs) or voice interface cards (VICs)
- One VIC-only interface card slot
- One auxiliary (AUX) port (up to 115.2 kbps asynchronous serial)
- One console port
- One internal expansion slot for future hardware-assisted services such as encryption (up to T1/E1) and compression processor
- RISC Processor for high performance encryption
- 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 Your Software Release

To determine the version of Cisco IOS software currently running on your Cisco 1750 router, log in to the Cisco 1750 router and enter the **show version** EXEC command. The following sample output from the **show version** command indicates the version number on the second output line:

```
router> show version
Cisco Internetwork Operating System Software
IOS (tm) c1750 Software (c1700-sv3y-mz.120-5.XQ), Version 12.0(5)XQ, RELEASE SOFTWARE
```

Additional command output lines include more information, such as processor revision numbers, memory amounts, hardware IDs, and partition information.

Upgrading to a New Software Release

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

On CCO, click on this path:

Service & Support: 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(5)XQ supports the same feature sets as Releases 12.0 and 12.0 T, but Release 12.0(5)XQ can include new features supported by the Cisco 1750 router. Table 2 lists the feature sets supported by the Cisco 1750 router.

Table 2   Feature Sets Supported by the Cisco 1750 Router

Feature Sets	Image Name	Feature Set Matrix Terms	Software Image	Platform	In[1]
IP Feature Sets	IP	Basic[2]	c1700-y-mz	Cisco 1720[3] Cisco 1750	12.0(1)XA3
	IP Plus	Plus[4]	c1700-sy-mz	Cisco 1720 Cisco 1750	12.0(1)XA3
	IP Plus 40	Plus 40[5]	c1700-sy40-mz	Cisco 1720 Cisco 1750	12.0(1)XA3
	IP Plus 56	Plus 56[6]	c1700-sy56-mz	Cisco 1720 Cisco 1750	12.0(1)XA3
	IP Plus IPSEC 56	Plus, IPSec 56[7]	c1700-sy56i-mz	Cisco 1720 Cisco 1750	12.0(3)T
	IP Plus IPSEC 3DES	Plus, IPSec, 3DES[8]	c1700-k2sy-mz	Cisco 1720 Cisco 1750	12.0(1)XA3
	IP/FW	Basic	c1700-oy-mz	Cisco 1720 Cisco 1750	12.0(1)XA3
	IP/IPX/FW Plus	Plus	c1700-nosy-mz	Cisco 1720 Cisco 1750	12.0(1)XA3
	IP/FW Plus IPSEC 56	Plus, IPSec 56	c1700-osy56i-mz	Cisco 1720 Cisco 1750	12.0(1)XA3
	IP/FW Plus IPSEC 3DES	Plus, IPSec, 3DES	c1700-k2osy-mz	Cisco 1720 Cisco 1750	12.0(1)XA3
	IP/IPX	Basic	c1700-ny-mz	Cisco 1720 Cisco 1750	12.0(1)XA3
	IP/IPX/AT/IBM	Basic	c1700-bnr2y-mz	Cisco 1720 Cisco 1750	12.0(1)XA3
	IP/IPX/AT/IBM Plus	Plus	c1700-bnr2sy-mz	Cisco 1720 Cisco 1750	12.0(1)XA3
	IP/IPX/AT/IBM/FW Plus IPSEC 56	Plus, IPSec 56	c1700-bnor2sy56i-mz	Cisco 1720 Cisco 1750	12.0(1)XA3
	IP/IPX/AT/IBM/FW Plus IPSEC 3DES	Plus, IPSec, 3DES	c1700-bk2nor2sy-mz	Cisco 1720 Cisco 1750	12.0(1)XA3
	IP/Voice Plus	Plus, Voice[9]	c1700-sv3y-mz.120-5.XQ	Cisco 1750	
	IP/Voice Plus 40	Plus 40, Voice	c1700-sv3y40-mz.120-5.XQ	Cisco 1750	

Table 2   Feature Sets Supported by the Cisco 1750 Router (continued)

Feature Sets	Image Name	Feature Set Matrix Terms	Software Image	Platform	In[1]
IP Feature Sets (continued)	IP/Voice Plus 56	Plus 56, Voice	c1700-sv3y56-mz.120-5.XQ	Cisco 1750	
	IP/Voice Plus IPSEC 56	Plus, Voice, IPSec 56	c1700-sv3y56i-mz.120-5.XQ	Cisco 1750	
	IP/Voice Plus IPSEC 3DES	Plus, Voice, IPSec, 3DES	c1700-k2sv3y-mz.120-5.XQ	Cisco 1750	
	IP/FW/Voice Plus	Plus, FW, Voice	c1700-osv3y-mz.120-5.XQ	Cisco 1750	
	IP/FW/Voice Plus IPSEC 56	Plus, FW, Voice, IPSEC 56	c1700-osv3y56i-mz.120-5.XQ	Cisco 1750	
	IP/FW/Voice Plus 3DES	Plus, FW, Voice, 3DES	c1700-k2osv3y-mz.120-5.XQ	Cisco 1750	
	IP/IPX/FW/Voice Plus	Plus, IPX, FW, Voice	c1700-nosv3y-mz.120-5.XQ	Cisco 1750	
	IP/IPX/AT/IBM/FW/Voice Plus IPSEC 56	Plus, IPX, AT, IBM, FW, Voice, IPSEC 56	c1700-bnor2sv3y56i-mz.120-5.XQ	Cisco 1750	
	IP/IPX/AT/IBM/FW/Voice Plus 3DES	Plus, IPX, AT, IBM, FW, Voice, 3DES	c1700-bk2nor2sv3y-mz.120-5.XQ	Cisco 1750	

1. The number in the "In" column indicates the Cisco IOS release in which the feature was introduced. For example, (3T) 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 set of features is provided in the basic feature set.

3. Cisco 1720 routers are mentioned here only to indicate that all images that run on Cisco 1720 routers also run on Cisco 1750 routers, but not vice-versa—voice images do not run on the Cisco 1720 routers.

4. This set of features is provided in the Plus feature set.

5. This set of features is provided in the 40-bit (Plus 40) data encryption feature sets.

6. This set of features is provided in the 56-bit (Plus 56) data encryption feature sets.

7. This set of features is provided in the IPSec 56-bit (Plus IPSec 56) data encryption feature sets.

8. This set of features is provided in the Triple DES (3DES) Encryption data encryption feature sets.

9. 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 (parts 1 through 4) lists the features and feature sets supported by the Cisco 1750 router in Cisco IOS Release 12.0(5)XQ. Both tables use the following conventions:

- Yes—The feature is supported in the software image.

- No—The feature is not supported in the software image.

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   Part 1, Feature List by Feature Set for the Cisco 1750 Routers

Features	Feature Sets						
	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	Yes	Yes	Yes	Yes	Yes	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
Quality of Service							
Classification							
IP Precedence	No	No	No	No	No	No	No

Table 3   Part 1, Feature List by Feature Set for the Cisco 1750 Routers (continued)

Features	Feature Sets						
	IP	IP Plus	IP Plus 40	IP Plus 56	IP Plus IPSEC 56	IP Plus IPSec 3DES	IP/FW
Link Efficiency Mechanisms							
Frame Relay Fragmentation–FRF.12	No	No	No	No	No	No	No
Multi-link PPP with Link Fragmentation & Interleave	No	No	No	No	No	No	No
Policing & Shaping							
Frame Relay Traffic Shaping with per Virtual Circuit queuing	No	No	No	No	No	No	No
Generic Traffic Shaping	No	No	No	No	No	No	No
Switching							
WCCPv2	No	Yes	Yes	Yes	Yes	Yes	No
Voice Services							
DTMF Relay	No	No	No	No	No	No	No
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 4 Part 2, Feature List by Feature Set for the Cisco 1750 Routers

Features	Feature Sets							
	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	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
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
Quality of Service								
Classification								
IP Precedence	No	No	No	No	No	No	No	No
Link Efficiency Mechanisms								
Frame Relay Fragmentation–FRF.12	No	No	No	No	No	No	No	No
Multi-link PPP with Link Fragmentation & Interleave	No	No	No	No	No	No	No	No
Policing & Shaping								
Frame Relay Traffic Shaping with per Virtual Circuit queuing	No	No	No	No	No	No	No	No
Generic Traffic Shaping	No	No	No	No	No	No	No	No

Table 4   Part 2, Feature List by Feature Set for the Cisco 1750 Routers (continued)

Features	Feature Sets							
	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
Switching								
WCCPv2	Yes	Yes	Yes	No	No	Yes	Yes	Yes
Voice Services								
DTMF Relay	No	No	No	No	No	No	No	No
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 5   Part 3, Feature List by Feature Set for the Cisco 1750 Routers

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	Yes	Yes	Yes	Yes	Yes	Yes
Management						
Cisco IOS File System	Yes	Yes	Yes	Yes	Yes	Yes
Entity MIB	Yes	Yes	Yes	Yes	Yes	Yes

Table 5 *Part 3, Feature List by Feature Set for the Cisco 1750 Routers (continued)*

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
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
Quality of Service						
Classification						
IP Precedence	Yes	Yes	Yes	Yes	Yes	Yes
Link Efficiency Mechanisms						
Frame Relay Fragmentation–FRF.12	Yes	Yes	Yes	Yes	Yes	Yes
Multi-link PPP with Link Fragmentation & Interleave	Yes	Yes	Yes	Yes	Yes	Yes
Policing & Shaping						
Frame Relay Traffic Shaping with per Virtual Circuit queuing	Yes	Yes	Yes	Yes	Yes	Yes
Generic Traffic Shaping	Yes	Yes	Yes	Yes	Yes	Yes
Switching						
WCCPv2	Yes	Yes	Yes	Yes	Yes	Yes
Voice Services						
DTMF Relay	Yes	Yes	Yes	Yes	Yes	Yes
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 6   *Part 4, Feature List by Feature Set for the Cisco 1750 Routers*

Features	Feature Sets				
	IP/FW/Voice Plus IPSEC 56	IP/FW/Voice Plus 3DES	IP/IPX/FW/ Voice Plus	IP/IPX/AT/IBM/F W/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	Yes	Yes	Yes	Yes	Yes
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
Quality of Service					
Classification					
IP Precedence	Yes	Yes	Yes	Yes	Yes
Link Efficiency Mechanisms					
Frame Relay Fragmentation–FRF.12	Yes	Yes	Yes	Yes	Yes
Multi-link PPP with Link Fragmentation & Interleave	Yes	Yes	Yes	Yes	Yes
Policing & Shaping					
Frame Relay Traffic Shaping with per Virtual Circuit queuing	Yes	Yes	Yes	Yes	Yes
Generic Traffic Shaping	Yes	Yes	Yes	Yes	Yes

Table 6   Part 4, Feature List by Feature Set for the Cisco 1750 Routers (continued)

Features	Feature Sets				
	IP/FW/Voice Plus IPSEC 56	IP/FW/Voice Plus 3DES	IP/IPX/FW/ Voice Plus	IP/IPX/AT/IBM/F W/Voice Plus IPSEC 56	IP/IPX/AT/IBM/ FW/Voice Plus 3DES
Switching					
WCCPv2	Yes	Yes	Yes	Yes	Yes
Voice Services					
DTMF Relay	Yes	Yes	Yes	Yes	Yes
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 1750 router in Release 12.0 T.

New Hardware Features in Release 12.0(5)XQ

The following new hardware enhancements are supported by the Cisco 1750 in Release 12.0(5)XQ and later releases. For more information about new hardware and configuring the new software features, see the "Platform-Specific Documents" section on page 21.

Support for Cisco 1750 Router

Cisco IOS Release 12.0(5)XQ 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(5)XQ1

The following software enhancements are supported by the Cisco 1750 in Release 12.0(5)XQ1 and later releases. For an introduction to the new software features, see the "Release-Specific Documents" section on page 20 and the "Feature Modules and the Quality of Service Solutions Configuration Guide" section on page 22.

Quality of Service

Cisco IOS Release 12.0(5)XQ1 supports the following features:

- Dual tone multifrequency (DTMF) relay
- Frame relay fragmentation–FRF.12
- FRF traffic shaping (with per virtual circuit [VC] queuing)
- Generic traffic shaping (GTS)
- Internet protocol (IP) precedence
- Multi-link point-to-point protocol (PPP) with link fragmentation and interleave

To configure these features on Cisco 1750 series routers, see the online document *Quality of Service Solutions Configuration Guide*. From CCO, click on the path (under the heading **Service & Support**):

Technical Documents: **Documentation Home Page**: **Cisco IOS Software Configuration**: **Cisco IOS Release 12.0**: **Configuration Guides and Command References**: **Configuration Guides and Command References**: **Quality of Service Solutions Configuration Guide**

Important Notes

The following sections contain important notes about Cisco IOS Release 12.0 that can apply to the Cisco 1750 router.

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 type "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, type "show flash ?" This will list all of the valid partitions. Then enter "show flash:xx: all" on each valid partition.

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 7, *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 7. Cisco is correcting the problem in certain special releases and will correct it in future maintenance and interim releases. See Table 7, *Affected and Repaired Software Versions* for details. Cisco intends to provide fixes for all affected Cisco 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 16 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 7 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 7, 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 Cisco 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 Cisco 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 7 specifies information about affected and repaired software versions.

✎
Note   All dates within this table are subject to change.

Table 7   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

Table 7   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 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
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 or defects in Cisco IOS software releases. For information on caveats in Cisco IOS Release 12.0 T, refer to the *Caveats for Cisco IOS Release 12.0 T* document. All caveats in Release 12.0 are also in Release 12.0 T.

For information on caveats in Cisco IOS Release 12.0, refer to the *Caveats for Cisco IOS Release 12.0* document, which lists severity 1 and 2 caveats, and is located on CCO and the Documentation CD-ROM. Severity 1 caveats are the most serious caveats; severity 2 caveats are less serious.

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**: **BUG TOOLKIT**: **Cisco Bug Navigator II**, or at http://www.cisco.com/support/bugtools/bugtool.shtml.

Caveats for Release 12.0(5)XQ

This section describes possibly unexpected behavior by Release 12.0(5)XQ. Only severity 1 and 2 caveats are included.

Miscellaneous

- CSCdk31542

  Booting a Cisco 1700 series router with the commands **boot flash** or **boot system flash** results in unpredictable behavior. For example, SNMP queries fail when a Cisco 1750 router is booted in 0x0 mode, although the router appears to boot up properly. To work around this problem, do not use the commands **boot flash** or **boot system flash** to boot up a Cisco 1700 series router.

- CSCdm62047

  The command **session target loopback:rtp** (which loops all voice data back to the originating source using Real-Time Transport Protocol [RTP] for VoIP dial peers) causes an unexpected router reload on a Cisco 1750 router. As a workaround for this problem, the command **session target loopback:rtp** is disabled in this release.

- CSCdp31143

  If you use the command **no frame-relay payload-compress packet-by-packet** to disable Stacker payload compression on an interface while the interface is up, the router might unexpectedly reload. To work around this problem, shut down the interface before disabling the feature.

Related Documentation

The following sections describe the documentation available for the Cisco 1750 router. Typically, 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 the documents listed in the following sections:

- Release-Specific Documents
- Platform-Specific Documents
- Feature Modules and the Quality of Service Solutions Configuration Guide
- Cisco IOS Software Documentation Set

Release-Specific Documents

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

- *Release Notes for Cisco IOS Release 12.0*

  – To reach the *Cross-Platform Release Notes for Cisco IOS Release 12.0* from CCO, click on this path (under the heading **Service & Support**):

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

  – To reach the *Cross-Platform Release Notes for Cisco IOS Release 12.0* on the Documentation CD-ROM, click on this path:

    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

  To reach these documents from CCO, click on this path (under the heading **Service & Support**):

  Technical Documents: **Product Bulletins**

- *Caveats for Cisco IOS Release 12.0 T*

  As a supplement to the caveats listed in the "Caveats" section on page 19 section in these release notes, see the *Caveats for Cisco IOS Release 12.0* and *Caveats for Cisco IOS Release 12.0 T* documents, which contains caveats applicable to all platforms for all maintenance releases of Release 12.0.

  – To reach the caveats document from CCO, click on this path (under the heading **Service & Support**):

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

  – To reach the caveats document on the Documentation CD-ROM, click on this path:

    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**: **BUG TOOLKIT**: **Cisco Bug Navigator II**, or at http://www.cisco.com/support/bugtools/bugtool.shtml.

Platform-Specific Documents

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

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

To reach Cisco 1750 documentation from CCO, click on this path (under the heading **Service & Support**):

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

On the Documentation CD-ROM, click on this path:

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

Feature Modules and the Quality of Service Solutions Configuration Guide

Feature modules describe new features supported by Release 12.0(5)XQ 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.

To reach the Release 12.0(5)XQ feature modules:

- From CCO, click on this path (under the heading **Service & Support**):

  Technical Documents: **Documentation Home Page**: **Cisco IOS Software Configuration**: **Cisco IOS Release 12.0**: **New Feature Documentation**: **New Features in 12.0-Based Limited Lifetime Releases**: **New Features in Release 12.0 XQ**

- From the Documentation CD-ROM, click on this path:

  Cisco Product Documentation: **Cisco IOS Software Configuration**: **Cisco IOS Release 12.0**: **New Feature Documentation**: **New Features in 12.0-Based Limited Lifetime Releases**: **New Features in Release 12.0 XQ**

The *Quality of Service Solutions Configuration Guide* is part of the Cisco IOS software document set described in the next section. This specific document is emphasized here because it relates specifically to the Cisco IOS release 12.0(5)XQ software features.

To reach the *Quality of Service Solutions Configuration Guide*:

- From CCO, click on the path (under the heading **Service & Support**):

  Technical Documents: **Documentation Home Page**: **Cisco IOS Software Configuration**: **Cisco IOS Release 12.0**: **Configuration Guides and Command References**: **Configuration Guides and Command References**: **Quality of Service Solutions Configuration Guide**

- From the Documentation CD-ROM, click on this path:

  Cisco Product Documentation: **Cisco IOS Software Configuration**: **Cisco IOS Release 12.0**: **Configuration Guides and Command References**: **Configuration Guides and Command References**: **Quality of Service Solutions Configuration Guide**

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 they 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: configuration guides and command references.

To reach these documents from CCO, click on this path (under the heading **Service & Support**):

Technical Documents: **Documentation Home Page**: **Cisco IOS Software Configuration**: **Cisco IOS Release 12.0**: **Configuration Guides and Command References**

To reach these documents on the Documentation CD-ROM, click on this path:

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

Release 12.0 Documentation Set

Table 8 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 might contain updates and modifications made after the hard-copy documents were printed.

To reach the Cisco IOS documentation set from CCO, click on this path (under the heading **Service & Support**):

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

To reach the Cisco IOS documentation set on the Documentation CD-ROM, click on this path:

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

Table 8   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
Dial Solutions Configuration Guide *Dial Solutions Command Reference*	Dial-In Port Setup Dial-In Terminal Services Dial-on-Demand Routing (DDR) Dial Backup Dial-Out Modem Pooling Large-Scale Dial Solutions Cost-Control Solutions ISDN X.25 over ISDN VPDN Dial Business Solutions and Examples
Cisco IOS Interface Configuration Guide *Cisco IOS Interface Command Reference*	Interface Configuration Overview
Network Protocols Configuration Guide, Part 1 *Network Protocols Command Reference, Part 1*	IP Addressing IP 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*	Apollo Domain Banyan VINES DECnet ISO CLNS XNS

Table 8   Cisco IOS Software Release 12.0 Documentation Set

Books	Chapter Topics
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 Paths for IP Networks Virtual LAN (VLAN) Switching and Routing
Wide-Area Networking Configuration Guide *Wide-Area Networking Command Reference*	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 Video Support Universal Broadband Features
Quality of Service Solutions Configuration Guide *Quality of Service Solutions Command Reference*	Classification Scheduling Packet Drop Traffic Shaping ATM QoS SNA QoS Line Protocols
Cisco IOS Software Command Summary *Dial Solutions Quick Configuration Guide* *System Error Messages* *Debug Command Reference*	

Note The *Cisco Management Information Base (MIB) User Quick Reference* publication is no longer published. For the latest list of MIBs supported by Cisco, see the 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. Resellers offer a wide variety of Cisco service and support programs that are described in the "Service and Support" section of the information packet shipped with your product.

Note If you purchased your product from a reseller, you can access CCO as a guest. CCO is the 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 helpful 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:

- Configuration Cookbooks—Contains common configurations or recipes for configuring various access routes and dial technologies.
- Field Notices—Designed to notify you of any critical issues regarding Cisco products. These notices include problem descriptions, safety or security issues, and hardware defects.
- Hardware—Technical Tips related to specific hardware platforms.
- Hot Tips—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—Tips on using and deploying Cisco IOS software features and services.
- Sample Configurations—Actual configuration examples that are complete with topology and annotations.
- Software Products—MultiNet & Cisco Suite 100, Network Management, Cisco IOS Software Bulletins, and CiscoPro Configurations.
- Special Collections—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 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.