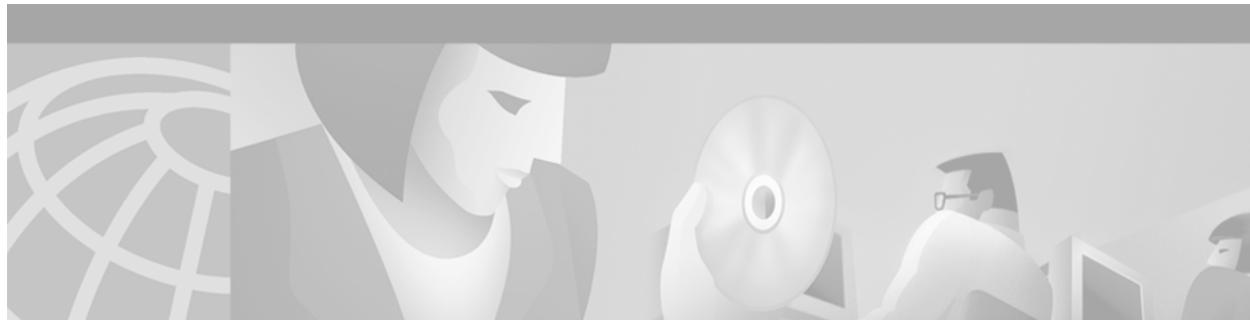




Release Notes for the Cisco 1700 Series Routers for Cisco IOS Release 12.2(4)XM

August 15, 2002

These release notes describe new features and significant software components for the Cisco 1700 series routers that support Cisco IOS Release 12.2 T, up to and including Release 12.2(4)XM4. 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 [Cross-Platform Release Notes for Cisco IOS Release 12.2 T](#) located on CCO and the Documentation CD-ROM.

For a list of the software caveats that apply to Release 12.2(4)XM4, refer to the section “[Caveats](#)” and to the online [Caveats for Cisco IOS Release 12.2 T](#) document. The caveats document is updated for every 12.2 T maintenance release and is located on Cisco Connection Online (CCO) and the Documentation CD-ROM.

Contents

These release notes discuss the following topics:

- [System Requirements, page 2](#)
- [New and Changed Information, page 17](#)
- [Limitations, page 34](#)
- [Important Notes, page 36](#)
- [Caveats, page 37](#)
- [Related Documentation, page 40](#)
- [Obtaining Documentation, page 46](#)
- [Obtaining Technical Assistance, page 47](#)



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

Copyright © 2002. Cisco Systems, Inc. All rights reserved.

System Requirements

This section describes the system requirements for Release 12.2(4)XM4 and includes the following sections:

- [Memory Requirements, page 2](#)
- [Hardware Supported, page 4](#)
- [Determining Your Software Release, page 10](#)
- [Upgrading to a New Software Release, page 10](#)
- [Feature Sets, page 11](#)

Memory Requirements

This section describes the memory requirements for the Cisco IOS feature sets supported by Cisco IOS Release 12.2(4)XM4 on the Cisco 1700 series routers.

Table 1 Recommended Memory for the Cisco 1700 Series Routers

Platform	Image Name	Feature Set	Image	Recommended Flash Memory	Recommended DRAM Memory	Runs from
Cisco 1710 router	Cisco 1710 IOS IP Plus IPX/AT/IBM/ FW/IDS IPSec 3DES	IP Plus IPX/AT/ IBM/FW/IDS IPSec 3DES	c1710-bk9no3r2sy-mz	16 MB	48 MB	RAM
	Cisco 1710 IOS IP Plus FW/IDS IPSec 3DES	IP Plus FW/IDS IPSec 3DES	c1710-k9o3sy-mz	8 MB	32 MB	RAM
Cisco 1720, 1750, 1751, and 1760 routers	Cisco 1700 IOS IP Plus ADSL/IPX/AT/IBM/FW/ IDS IPSec 56	IP Plus ADSL/ IPX/AT/IBM/ FW/IDS IPSec 56	c1700-bk8no3r2sy7-mz	16 MB	48 MB	RAM
	Cisco 1700 IOS IP Plus ADSL/IPX/AT/IBM/FW/ IDS IPSec 3DES	IP Plus ADSL/ IPX/AT/IBM/ FW/IDS IPSec 3DES	c1700-bk9no3r2sy7-mz	16 MB	48 MB	RAM
	Cisco 1700 IOS IP Plus ADSL/IPX/AT/IBM	IP Plus ADSL/ IPX/AT/IBM	c1700-bnr2sy7-mz	16 MB	48 MB	RAM
	Cisco 1700 IOS IP/IPX/AT/IBM	IP/IPX/AT/IBM	c1700-bnr2y-mz	8 MB	32 MB	RAM
	Cisco 1700 IOS IP Plus ADSL/FW/IDS IPSec 56	IP Plus ADSL/ FW/IDS IPSec 56	c1700-k8o3sy7-mz	16 MB	48 MB	RAM
	Cisco 1700 IOS IP Plus ADSL IPSec 56	IP Plus ADSL IPSec 56	c1700-k8sy7-mz	16 MB	48 MB	RAM
	Cisco 1700 IOS IP Plus ADSL/FW/IDS IPSec 3DES	IP Plus ADSL/ FW/IDS IPSec 3DES	c1700-k9o3sy7-mz	16 MB	48 MB	RAM

Table 1 Recommended Memory for the Cisco 1700 Series Routers

Platform	Image Name	Feature Set	Image	Recommended Flash Memory	Recommended DRAM Memory	Runs from
Cisco 1720, 1750, 1751, and 1760 routers (continued)	Cisco 1700 IOS IP Plus ADSL IPSec 3DES	IP Plus ADSL IPSec 3DES	c1700-k9sy7-mz	16 MB	48 MB	RAM
	Cisco 1700 IOS IP Plus ADSL/IPX/FW/IDS Plus	IP Plus ADSL/ IPX/FW/IDS	c1700-no3sy7-mz	16 MB	48 MB	RAM
	Cisco 1700 IOS IP/IPX	IP/IPX	c1700-ny-mz	8 MB	32 MB	RAM
	Cisco 1700 IOS IP/FW/IDS	IP/FW/IDS	c1700-o3y-mz	8 MB	32 MB	RAM
	Cisco 1700 IOS IP Plus ADSL	IP Plus ADSL	c1700-sy7-mz	8 MB	48 MB	RAM
	Cisco 1700 IOS IP	IP	c1700-y-mz	8 MB	32 MB	RAM
	Cisco 1700 IOS IP/ADSL	IP/ADSL	c1700-y7-mz	8 MB	32 MB	RAM
Cisco 1750, Cisco 1751, and Cisco 1760 routers	Cisco 1700 IOS IP Plus ADSL/IPX/AT/IBM/Voice/FW/IDS IPSec 56	IP Plus ADSL/ IPX/AT/IBM/ Voice/FW/IDS IPSec 56	c1700-bk8no3r2sv3y7-mz	32 MB	64 MB	RAM
	Cisco 1700 IOS IP Plus ADSL/IPX/AT/IBM/Voice/FW/IDS Plus IPSec 3DES	IP Plus ADSL/ IPX/AT/IBM/ Voice/FW/IDS IPSec 3DES	c1700-bk9no3r2sv3y7-mz	32 MB	64 MB	RAM
	Cisco 1700 IOS IP Plus ADSL/Voice/FW/IDS Plus IPSec 56	IP Plus ADSL/ Voice/FW/IDS IPSec 56	c1700-k8o3sv3y7-mz	16 MB	48 MB	RAM
	Cisco 1700 IOS IP Plus ADSL/Voice Plus IPSec 56	IP Plus ADSL/ Voice IPSec 56	c1700-k8sv3y7-mz	16 MB	48 MB	RAM
	Cisco 1700 IOS IP Plus ADSL/Voice/FW/IDS IPSec 3DES	IP Plus ADSL/ Voice/FW/IDS IPSec 3DES	c1700-k9o3sv3y7-mz	16 MB	48 MB	RAM
	Cisco 1700 IOS IP Plus ADSL/Voice IPSec 3DES	IP Plus ADSL/ Voice IPSec 3DES	c1700-k9sv3y7-mz	16 MB	48 MB	RAM
	Cisco 1700 IOS IP Plus ADSL/IPX/Voice/FW/IDS	IP Plus ADSL/ IPX/Voice/FW/ IDS	c1700-no3sv3y7-mz	16 MB	48 MB	RAM

Table 1 Recommended Memory for the Cisco 1700 Series Routers

Platform	Image Name	Feature Set	Image	Recommended Flash Memory	Recommended DRAM Memory	Runs from
Cisco 1750, Cisco 1751, and Cisco 1760 routers (continued)	Cisco 1700 IOS IP Plus ADSL/Voice/FW/IDS	IP Plus ADSL/Voice/FW/IDS	c1700-o3sv3y7-mz	16 MB	48 MB	RAM
	Cisco 1700 IOS IP Plus Voice	IP Plus Voice	c1700-sv3y-mz	16 MB	48 MB	RAM
	Cisco 1700 IOS IP Plus ADSL/Voice	IP Plus ADSL/Voice	c1700-sv3y7-mz	16 MB	48 MB	RAM
	Cisco 1700 IOS IP Plus VOX	IP Plus VOX	c1700-sv8y-mz	16 MB	48 MB	RAM
Cisco 1751 and Cisco 1760 routers	Cisco 1700 IOS IP Plus ADSL/IPX/AT/IBM/VOX/ FW IDS IPsec 56	IP Plus ADSL/IPX/AT/IBM/VOX/ FW/IDS IPsec 56	c1700-bk8no3r2sv8y7-mz	16 MB	64 MB	RAM
	Cisco 1700 IOS IP Plus ADSL/IPX/AT/IBM/VOX/FW/IDS IPsec 3DES	IP Plus ADSL/IPX/AT/IBM/VOX/FW/IDS IPsec 3DES	c1700-bk9no3r2sv8y7-mz	32 MB	64 MB	RAM
	Cisco 1700 IOS IP Plus ADSL/VOX/FW/IDS IPsec 56	IP Plus ADSL/VOX/FW/IDS IPsec 56	c1700-k8o3sv8y7-mz	32 MB	64 MB	RAM
	Cisco 1700 IOS IP Plus ADSL/VOX IPsec 56	IP Plus ADSL/VOX IPsec 56	c1700-k8sv8y7-mz	16 MB	64 MB	RAM
	Cisco 1700 IOS IP Plus ADSL/VOX/FW/IDS IPsec 3DES	IP Plus ADSL/VOX/FW/IDS IPsec 3DES	c1700-k9o3sv8y7-mz	16 MB	64 MB	RAM
	Cisco 1700 IOS IP Plus ADSL/VOX IPsec 3DES	IP Plus ADSL/VOX IPsec 3DES	c1700-k9sv8y7-mz	16 MB	64 MB	RAM
	Cisco 1700 IOS IP Plus ADSL/VOX/FW/IDS	IP Plus ADSL/VOX/FW/IDS	c1700-o3sv8y7-mz	16 MB	64 MB	RAM
	Cisco 1700 IOS IP Plus ADSL/IPX/VOX/FW/IDS	IP Plus ADSL/IPX/VOX/FW/IDS	c1700-no3sv8y7-mz	16 MB	64 MB	RAM
	Cisco 1700 IOS IP Plus ADSL/VOX	IP Plus ADSL/VOX	c1700-sv8y7-mz	16 MB	64 MB	RAM

Hardware Supported

Cisco IOS Release 12.2(4)XM4 supports the following Cisco 1700 series routers:

- [Cisco 1710 Routers](#)
- [Cisco 1720 Routers](#)
- [Cisco 1750, 1750-2V, and 1750-4V Routers](#)

- [Cisco 1751 and 1751-V Routers](#)
- [Cisco 1760 and 1760-V Routers](#)

The Cisco 1710 and 1720 routers run data images only. The Cisco 1750, 1750-2V, and 1750-4V routers run data and data-and-voice images, providing analog voice support. Cisco 1751, 1751-V, 1760, and 1760-V routers run data and data-and-voice images, providing digital and analog voice support.

For detailed descriptions of the new hardware features, see the documents listed in the [“Platform-Specific Documents” section on page 41](#).

Cisco 1710 Routers

The 1710 router provides Internet and intranet access and includes the following:

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

The Cisco 1710 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 Ethernet (10BASE-T) port, which operates in full- or half-duplex mode.
- One auxiliary (AUX) port (up to 115.2 kbps asynchronous serial).
- One console port.
- Motorola MPC855T PowerQUICC at 48 MHz. The hardware encryption module offloads the processor for encryption and decryption.
- One internal expansion slot for support of hardware-assisted services such as encryption (up to T1/E1) and compression.
- DRAM memory: 32 MB default, expandable to 64 MB.
- Flash memory: 16 MB default, 16 MB maximum.
- One security slot that supports Kensington or similar lockdown equipment.
- Desktop form factor.

Cisco 1720 Routers

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, which operates in full- or half-duplex mode (with manual override available).
- Two WAN interface card slots.
- One 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 hardware-assisted services such as encryption (up to T1/E1) and compression.
- DRAM memory: 32 MB default, expandable to 48 MB.
- Flash memory: 8 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:

- 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.
- WIC-1ENET—One-port 10Base-T Ethernet interface.
- WIC-1ADSL—One-port asymmetrical digital subscriber line.
- WIC-1SHDSL—One-port G-Standard High bit-rate Digital Subscriber Loop.

Cisco 1750, 1750-2V, and 1750-4V Routers

The voice-and-data capable Cisco 1750, 1750-2V and 1750-4V routers provide 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, 1750-2V and 1750-4V routers have 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 (VIC) slot—Supports a single voice interface card with two ports per card.
- Two WAN interface card (WIC) slots for either WICs or VICs.
- Synchronous serial interfaces on serial WICs.
- Asynchronous serial interfaces on serial WICs.
- ISDN WICs—ISDN dialup and ISDN leased line (IDSL) at 144 kbps; encapsulation over ISDN leased line; Frame Relay and PPP.
- One AUX port (up to 115.2 kbps asynchronous serial).
- One console port.
- One internal expansion slot—Supports hardware-assisted services such as encryption (up to T1/E1 speeds).

- RISC Processor—Motorola MPC860T PowerQUICC at 48 MHz.
- One security slot that supports Kensington or similar lockdown equipment.
- DRAM: 16 MB default, expandable to 48 MB.
- Flash memory: 4 MB default, expandable to 16 MB.
- Desktop form factor.

The Cisco 1750, 1750-2V and 1750-4V routers support any combination of one or two of the following WICs:

- 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.
- WIC-1ENET—One-port 10Base-T Ethernet interface.
- WIC-1ADSL—One-port asymmetrical digital subscriber line.
- WIC-1SHDSL—One-port G-Standard High bit-rate Digital Subscriber Loop.

The Cisco 1750, 1750-2V and 1750-4V routers support any combination of one or two of the following voice interface cards:

- VIC-2FXS—Two-port Foreign Exchange Station (FXS) voice interface card.
- VIC-2FXO—Two-port Foreign Exchange Office (FXO) voice interface card.
- VIC-2FXO-EU—Two-port FXO voice interface card for Europe.
- VIC-2E/M—Two-port Ear and Mouth (E & M) voice interface card.
- VIC-2FXO-M1—Two-port FXO for the United States with battery reversal.
- VIC-2FXO-M2—Two-port FXO for Europe with battery reversal.
- VIC-2FXO-M3—Two-port FXO for Australia.

Cisco 1751 and 1751-V Routers

The voice-and-data capable Cisco 1751 and 1751-V routers provide global Internet and company intranet access and include the following:

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

The Cisco 1751 and 1751-V routers have the following hardware components:

- One autosensing 10/100 Fast Ethernet port, which operates in full- or half-duplex mode (with manual override available).
- Institute of Electrical and Electronic Engineers (IEEE) 802.1Q VLAN support.

- One VIC slot—Supports a single voice interface card with two ports per card.
- Two WIC slots for either WICs or VICs.
- Synchronous serial interfaces on serial WICs.
- Asynchronous serial interfaces on serial WICs.
- ISDN WICs—ISDN dialup and IDSL at 144 kbps; encapsulation over ISDN leased line; Frame Relay and PPP.
- One AUX port (up to 115.2 kbps asynchronous serial).
- One console port.
- One internal expansion slot—Supports hardware-assisted services such as encryption (up to T1/E1 speeds).
- RISC Processor—Motorola MPC860P PowerQUICC at 48.384 MHz.
- One security slot that supports Kensington or similar lockdown equipment.
- DRAM:
 - Cisco 1751: 32 MB default, expandable to 96 MB.
 - Cisco 1751-V: 64 MB default, expandable to 128 MB.
- Flash memory:
 - Cisco 1751: 16 MB.
 - Cisco 1751-V: 32 MB.
- Desktop form factor.

The Cisco 1751 and 1751-V routers support any combination of one or two of the following WICs:

- 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.
- WIC-1ADSL—One-port asymmetric digital subscriber line.
- WIC-1SHDSL—One-port G-Standard High bit-rate Digital Subscriber Loop.
- WIC-1ENET—One-port 10Base-T Ethernet interface.
- WIC-1-ADSL—One-port asymmetrical digital subscriber line.

The Cisco 1751 and 1751-V routers support any combination of one, two or three of the following VICs:

- VIC-2FXS—Two-port FXS voice interface card.
- VIC-2FXO—Two-port FXO voice interface card.
- VIC-2FXO-EU—Two-port FXO voice interface card for Europe.
- VIC-2E/M—Two-port E & M voice interface card.
- VIC-2FXO-M1—Two-port FXO for the United States with battery reversal.
- VIC-2FXO-M2—Two-port FXO for Europe with battery reversal.

- VIC-2FXO-M3—Two-port FXO for Australia.
- VIC-2BRI-NT/TE—Two-port ISDN interface.
- VIC-2DID—Two-port direct inward-dialing voice interface card.

Cisco 1760 and 1760-V Routers

The voice-and-data capable Cisco 1760 and 1760-V routers provide global Internet and company intranet access and include the following:

- VoIP voice-and-data functionality; the router can provide support for digital and analog voice traffic (for example, telephone calls and faxes) over an IP network.
- Cisco 1760-V routers integrate data and voice services with support for multiple voice channels.
- VoIP and Voice-over-Frame Relay (VoFR) connections.
- Support for virtual private networking.
- Modular architecture.
- Network device integration.
- Support for the following network management tools and applications:
 - Simple Network Management Protocol (SNMP).
 - AutoInstall (for downloading configuration files to the router over a WAN connection).

The Cisco 1760 and 1760-V routers have the following hardware components:

- One autosensing 10/100 Fast Ethernet port, which operates in full- or half-duplex mode (with software override support).
- IEEE 802.1Q VLAN support.
- Two VIC slots—Support voice interface cards with two ports per card.
- Two WIC slots for either WICs or VICs.
- Synchronous serial interfaces on serial WICs.
- Asynchronous serial interfaces on serial WICs.
- One AUX port (to support a modem connection to the router, which can be configured and managed from a remote location, up to 115.2 kbps asynchronous serial).
- One console port (for router configuration and management from a connected terminal or PC, up to 115.2 kbps).
- One internal expansion slot—Supports hardware-assisted services such as encryption (up to T1/E1 speeds).
- RISC Processor—Motorola MPC860P PowerQUICC at 40 MHz externally and 80MHz internally.
- DRAM:
 - Cisco 1760: 32 MB default, expandable to 96 MB.
 - Cisco 1760-V: 64 MB default, expandable to 96 MB.
- Flash memory:
 - Cisco 1760: 16 MB default, expandable to 64 MB.
 - Cisco 1760-V: 32 MB default, expandable to 64 MB.

The Cisco 1760 and 1760-V routers support any combination of one or two of the following WICs:

- 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.
- WIC-1-ADSL—One-port asymmetric digital subscriber line.
- WIC-1ENET—One-port 10Base-T Ethernet interface.
- WIC-1SHDSL—One-port G-Standard High bit-rate Digital Subscriber Loop.

The Cisco 1760 and 1760-V routers support any combination of one, two, three, or four of the following VICs:

- VIC-2FXS—Two-port FXS voice interface card.
- VIC-2FXO—Two-port FXO voice interface card.
- VIC-2FXO-EU—Two-port FXO voice interface card for Europe.
- VIC-2E/M—Two-port E & M voice interface card.
- VIC-2FXO-M1—Two-port FXO for the United States with battery reversal.
- VIC-2FXO-M2—Two-port FXO for Europe with battery reversal.
- VIC-2FXO-M3—Two-port FXO for Australia.
- VIC-2BRI-NT/TE—Two-port ISDN interface.
- VIC-2DID—Two-port direct inward-dialing voice interface card.

Determining Your Software Release

To determine the version of Cisco IOS software currently running on your Cisco 1700 series router, log in to the 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) c1700 Software (c1700-y-mz), Version 12.2(4)XM4, RELEASE SOFTWARE
```

Upgrading to a New Software Release

For general information about upgrading to a new software release, see [Technical Support for 1700 Series Access Routers](#).

Feature Sets

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 12.2(4)XM4 supports the same feature sets as Releases 12.2 and 12.2 T, but Release 12.2(4)XM4 include new features supported by the Cisco 1700 series routers.



Caution

Cisco IOS images with strong encryption (including, but not limited to 168-bit (3DES) data encryption feature sets) are subject to United States government export controls and have limited distribution. Strong encryption images to be installed outside the United States are likely to require an export license. Customer orders can be denied or subject to delay due to United States government regulations. When applicable, the purchaser/user must obtain local import and use authorizations for all encryption strengths. Please contact your sales representative or distributor for more information, or send an e-mail to export@cisco.com.

Table 2 through Table 5 list the features and feature sets supported in Cisco IOS Release 12.2(4)XM4:

- [Table 2](#)—Cisco 1710 routers
- [Table 3](#)—Cisco 1720, 1750, 1751, and 1760 routers
- [Table 4](#)—Cisco 1750, 1751, and 1760 routers
- [Table 5](#)—Cisco 1751 and 1760 routers

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, “12.2(4)XM” means the feature was introduced in Release 12.2(4)XM. If a cell in this column is empty, the feature was included in a previous release or the initial base release.



Note

These feature set tables only contain a selected list of features, which are cumulative for Release 12.2(4)*nn* early deployment releases only (*nn* identifies each early deployment release). The tables do not list all features in each image—additional features are listed in the [Cross-Platform Release Notes for Cisco IOS Release 12.2 T](#) and Release 12.2 T Cisco IOS documentation.

Table 2 Feature List by Feature Set for Cisco 1710 Routers

Feature	In	Feature Set	
		IP Plus IPX/AT/IBM/FW/IDS IPSec 3DES	IP Plus FW/IDS IPSec 3DES
Multimedia & Quality of Service			
CAC for VoIP call		No	No
DiffServ for voice signaling traffic		No	No
Layer 2 COS matching and marking		Yes	Yes

Table 2 Feature List by Feature Set for Cisco 1710 Routers

Feature	In	Feature Set	
		IP Plus IPX/AT/ IBM/FW/IDS IPSec 3DES	IP Plus FW/IDS IPSec 3DES
Multiservice Applications			
G.728 codec support		No	No
TCL scripting for IVR		No	No
RTSP enhanced IVR		No	No
T.37 fax relay		No	No
T.38 fax relay		No	No
SIP features ¹		No	No
MGCP features ²		No	No
Modem pass through over VoIP		No	No

1. SIP features include:

- Call transfer capabilities using the refer method
- Configurable public switched telephone network (PSTN) cause code to SIP response
- Gateway support for bind command
- ISDN progress indicator support for SIP using 183 session progress
- NAT support for SIP
- RFC2782 compliance for DNS SRV
- Session initiation protocol (SIP)
- Session initiation protocol for VoIP enhancements
- SIP diversion header implementation for redirecting number
- SIP DTMF relay using NTE
- SIP gateway support for third party call control
- SIP gateway support of RSVP and “tel” URL
- SIP intra-gateway hair-pinning
- SIP INVITE request with malformed via header
- SIP T.38 fax relay
- SIP user agent MIB

2. MGCP features include:

- MGCP 1.0
- MGCP based fax (T.38) and DTMF relay
- MGCP basic CLASS and operator services
- MGCP VoIP call admission control

Table 3 Feature List by Feature Set for Cisco 1720, 1750, 1751, and 1760 Routers, Part 1 of 2

Feature	In	Feature Set					
		IP Plus ADSL/ IPX/AT/IBM/FW/ IDS IPSec 56	IP Plus ADSL/ IPX/AT/IBM/FW/ IDS IPSec 3DES	IP Plus ADSL/ IPX/AT/ IBM	IP/IPX/ AT/IBM	IP Plus ADSL/FW/ IDS IPSec 56	IP Plus ADSL IPSec 56
Multimedia & Quality of Service							
CAC for VoIP call		No	No	No	No	No	No
DiffServ for voice signaling traffic		No	No	No	No	No	No
Layer 2 COS matching and marking ¹	12.2(4)XM	Yes	Yes	Yes	Yes	Yes	Yes
Multiservice Applications							
G.728 codec Support		No	No	No	No	No	No
TCL scripting for IVR		No	No	No	No	No	No
RTSP enhanced IVR		No	No	No	No	No	No
T.37 fax relay		No	No	No	No	No	No
T.38 fax relay		No	No	No	No	No	No
SIP features ²		No	No	No	No	No	No
MGCP features ³		No	No	No	No	No	No
Modem pass through over VoIP		No	No	No	No	No	No

1. The Layer 2 COS matching and marking feature is supported on the Cisco 1710, 1751, and 1760 routers only.

2. For a list of the SIP features, see [Table 2, Footnote 1](#).

3. For a list of the MGCP features, see [Table 2, Footnote 2](#).

Table 3 Feature List by Feature Set for Cisco 1720, 1750, 1751, and 1760 Routers, Part 2 of 2 (continued)

Feature	In	Feature Set							
		IP Plus FW/ ADSL/IDS IPSec 3DES	IP Plus ADSL IPSec 3DES	IP Plus ADSL/IPX/ FW/IDS	IP/IPX	IP/FW/ IDS	IP Plus ADSL	IP	IP/ ADSL
Multimedia & Quality of Service									
CAC for VoIP call		No	No	No	No	No	No	No	No
DiffServ for voice signaling traffic		No	No	No	No	No	No	No	No
Layer 2 COS matching and marking ¹	12.2(4)XM	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Multiservice Applications									
G.728 codec support		No	No	No	No	No	No	No	No
TCL scripting for IVR		No	No	No	No	No	No	No	No
RTSP enhanced IVR		No	No	No	No	No	No	No	No

Table 3 Feature List by Feature Set for Cisco 1720, 1750, 1751, and 1760 Routers, Part 2 of 2 (continued)

Feature	In	Feature Set							
		IP Plus FW/ ADSL/IDS IPSec 3DES	IP Plus ADSL IPSec 3DES	IP Plus ADSL/IPX/ FW/IDS	IP/IPX	IP/FW/ IDS	IP Plus ADSL	IP	IP/ ADSL
T.37 fax relay		No	No	No	No	No	No	No	No
T.38 fax relay		No	No	No	No	No	No	No	No
SIP features ²		No	No	No	No	No	No	No	No
MGCP features ³		No	No	No	No	No	No	No	No
Modem pass through over VoIP		No	No	No	No	No	No	No	No

1. The Layer 2 COS matching and marking feature is supported on the Cisco 1710, 1751, and 1760 routers only.
2. For a list of the SIP features, see [Table 2, Footnote 1](#).
3. For a list of the MGCP features, see [Table 2, Footnote 2](#).

Table 4 Feature List by Feature Set for Cisco 1750, 1751, and 1760 Routers, Part 1 of 2 (continued)

Feature	In	Feature Set					
		IP Plus ADSL/ IPX/AT/IBM/ Voice/FW/IDS IPSec 56	IP Plus ADSL/ IPX/AT/IBM/ Voice/FW/IDS IPSec 3DES	IP Plus ADSL/FW/ Voice/IDS IPSec 56	IP Plus ADSL/ Voice IPSec 56	IP Plus ADSL/FW/ Voice/IDS IPSec 3DES	IP Plus ADSL/ Voice IPSec 3DES
Multimedia & Quality of Service							
CAC for VoIP call		No	No	No	No	No	No
DiffServ for voice signaling traffic	12.2(4)XM	No	No	Yes	Yes	No	Yes
Layer 2 COS matching and marking ¹	12.2(4)XM	Yes	Yes	Yes	Yes	Yes	Yes
Multiservice Applications							
G.728 codec support	12.2(4)XM	Yes	Yes	Yes	Yes	Yes	Yes
TCL scripting for IVR		No	No	No	No	No	No
RTSP enhanced IVR		No	No	No	No	No	No
T.37 fax relay		No	No	No	No	No	No
T.38 fax relay		No	No	No	No	No	No
SIP features ²		No	No	No	No	No	No

Table 4 Feature List by Feature Set for Cisco 1750, 1751, and 1760 Routers, Part 1 of 2 (continued)

Feature	In	Feature Set					
		IP Plus ADSL/ IPX/AT/IBM/ Voice/FW/IDS IPSec 56	IP Plus ADSL/ IPX/AT/IBM/ Voice/FW/IDS IPSec 3DES	IP Plus ADSL/FW/ Voice/IDS IPSec 56	IP Plus ADSL/ Voice IPSec 56	IP Plus ADSL/FW/ Voice/IDS IPSec 3DES	IP Plus ADSL/ Voice IPSec 3DES
MGCP features ³		No	No	No	No	No	No
Modem pass through over VoIP		No	No	No	No	No	No

1. The Layer 2 COS matching and marking feature is supported on the Cisco 1710, 1751, and 1760 routers only.
2. For a list of the SIP features, see [Table 2, Footnote 1](#).
3. For a list of the MGCP features, see [Table 2, Footnote 2](#).

Table 4 Feature List by Feature Set for Cisco 1750, 1751, and 1760 Routers, Part 2 of 2

Feature	In	Feature Set				
		IP Plus ADSL/ IPX/Voice/ FW/IDS	IP Plus ADSL/IDS/ Voice/FW	IP Plus Voice	IP Plus ADSL/ Voice	IP Plus VOX
Multimedia & Quality of Service						
CAC for VoIP call	12.2(4)XM	No	No	No	No	Yes
DiffServ for voice signaling traffic	12.2(4)XM	Yes	Yes	Yes	Yes	Yes
Layer 2 COS matching and marking ¹	12.2(4)XM	Yes	Yes	Yes	Yes	No
Multiservice Applications						
G.728 codec support	12.2(4)XM	Yes	Yes	Yes	Yes	Yes
TCL scripting for IVR	12.2(4)XM	No	No	No	No	Yes
RTSP enhanced IVR	12.2(4)XM	No	No	No	No	Yes
T.37 fax relay	12.2(4)XM	No	No	No	No	Yes
T.38 fax relay		No	No	No	No	Yes
SIP features ²	12.2(4)XM	No	No	No	No	Yes
MGCP features ³	12.2(4)XM	No	No	No	No	Yes
Modem pass through over VoIP	12.2(4)XM	No	No	No	No	Yes

1. The Layer 2 COS matching and marking feature is supported on the Cisco 1710, 1751, and 1760 routers only.
2. For a list of the SIP features, see [Table 2, Footnote 1](#).
3. For a list of the MGCP features, see [Table 2, Footnote 2](#).

**Note**

SIP and Media Gateway Control Protocol (MGCP) features are not supported on Cisco 1760 routers.

Table 5 Feature List by Feature Set for Cisco 1751 and 1760 Routers, Part 1 of 2

Feature	In	Feature Set			
		IP Plus ADSL/ IPX/AT/ IBM/ VOX/ FW/IDS IPSec 56	IP Plus ADSL/ IPX/AT/IBM/ VOX/FW/IDS IPSec 3DES	IP Plus ADSL/VOX/ FW/ IDS IPSec 56	IP Plus ADSL/ VOX IPSec 56
Multimedia & QoS					
CAC for VoIP call	12.2(4)XM	Yes	Yes	Yes	Yes
DiffServ for voice signaling traffic	12.2(4)XM	Yes	Yes	Yes	Yes
Layer 2 COS matching and marking	12.2(4)XM	Yes	Yes	Yes	Yes
Multiservice Applications					
G.728 codec support	12.2(4)XM	Yes	Yes	Yes	Yes
TCL scripting for IVR	12.2(4)XM	Yes	Yes	Yes	Yes
RTSP enhanced IVR	12.2(4)XM	Yes	Yes	Yes	Yes
T.37 fax relay	12.2(4)XM	Yes	Yes	Yes	Yes
T.38 fax relay		Yes	Yes	Yes	Yes
SIP features ¹	12.2(4)XM	Yes	Yes	Yes	Yes
MGCP features ²	12.2(4)XM	Yes	Yes	Yes	Yes
Modem pass through over VoIP	12.2(4)XM	Yes	Yes	Yes	Yes

1. For a list of the SIP features, see [Table 2, Footnote 1](#).

2. For a list of the MGCP features, see [Table 2, Footnote 2](#).

Table 5 Feature List by Feature Set for Cisco 1751 and 1760 Routers, Part 2 of 2

Feature	In	Feature Set				
		IP Plus ADSL/VOX/ FW/IDS IPSec 3DES	IP Plus ADSL/VOX IPSec 3DES	IP Plus ADSL/ IPX/VOX/ FW/IDS	IP Plus ADSL/ VOX/ FW/IDS	IP Plus ADSL/ VOX
Multimedia & QoS						
CAC for VoIP call	12.2(4)XM	Yes	Yes	Yes	Yes	Yes
DiffServ for voice signaling traffic	12.2(4)XM	Yes	Yes	Yes	Yes	Yes
Layer 2 COS matching and marking	12.2(4)XM	Yes	Yes	Yes	Yes	Yes

Table 5 Feature List by Feature Set for Cisco 1751 and 1760 Routers, Part 2 of 2

Feature	In	Feature Set				
		IP Plus ADSL/VOX/ FW/IDS IPSec 3DES	IP Plus ADSL/VOX IPSec 3DES	IP Plus ADSL/ IPX/VOX/ FW/IDS	IP Plus ADSL/ VOX/ FW/IDS	IP Plus ADSL/ VOX
Multiservice Applications						
G.728 codec support	12.2(4)XM	Yes	Yes	Yes	Yes	Yes
TCL scripting for IVR	12.2(4)XM	Yes	Yes	Yes	Yes	Yes
RTSP enhanced IVR	12.2(4)XM	Yes	Yes	Yes	Yes	Yes
T.37 fax relay	12.2(4)XM	Yes	Yes	Yes	Yes	Yes
T.38 fax relay ¹		Yes	Yes	Yes	Yes	Yes
SIP features ^{1 2}	12.2(4)XM	Yes	Yes	Yes	Yes	Yes
MGCP features ^{1 3}	12.2(4)XM	Yes	Yes	Yes	Yes	Yes
Modem pass through over VoIP ¹	12.2(4)XM	Yes	Yes	Yes	Yes	Yes

1. Release 12.2(4)XM and above do not support this feature on Cisco 1760 routers.

2. For a list of the SIP features, see [Table 2, Footnote 1](#).

3. For a list of the MGCP features, see [Table 2, Footnote 2](#).

New and Changed Information

The following sections list the new hardware and software features supported by the Cisco 1700 series routers for Release 12.2(4)XM4.

New Software Features in Release 12.2(4)XM

The following sections describe the new software features supported by the Cisco 1700 series routers for Release 12.2(4)XM.

Basic Session Initiation Protocol

Session Initiation Protocol (SIP) is a signaling protocol that has equivalent or greater functionality than H.323, but is significantly less complex. SIP provides enhanced functionality in protocol extensibility, system scalability, personal mobility services, and inter-vendor interoperability. The following basic SIP features are supported by Release 12.2(4)XM on all digital and analog interfaces:

- User agent (UA) functionality in accordance with RFC2543, with limited compliance.
- Real Time Transport Protocol (RTP) and Real Time Streaming Protocol (RTSP) for media transport.
- Support for g711, g729a, g726r32 and g723r63 data conversion (codecs).
- Signaling using both Transmission Control Protocol (TCP) and User Datagram Protocol (UDP).

- Support for UDP multicast IP addresses to use the SIP REGISTER method.
- Network security through authentication, authorization, and accounting (AAA).

Call Admission Control for H.323 VoIP Gateways

Release 12.2(4)XM supports the call admission control (CAC) for H.323 VoIP gateways feature with the following characteristics:

- CAC based on local resources
- Advanced voice busy out (AVBO)
- Public switched telephone network (PSTN) fallback

The CAC is a set of Quality of Service (QoS) features that provide the capability to act and react against networking and local resource conditions that can impact voice quality. The features provide voice gateway resource monitoring, threshold management and call access denial to the voice gateway. The CAC features enable gateways to gracefully prevent call entry when local resources are unavailable to process the call—when gateway internal resources drop below a user-defined congestion threshold. Resources include system resources such as: CPU utilization, memory, call volume, and interfaces.

You can configure the congestion threshold and the call treatment (that is, how a call should be treated when local resources are not available to handle the call). Two call-treatment action types are available: system denial using AVBO (which “busyouts” incoming calls) or per-call denial. Per-call denial treatment choices are as follows:

- Time division multiplexing (TDM) hairpin—Redirects the calls through the Plain Old Telephone Service (POTS) dial peer.
- Reject—Disconnects the call.
- Play message or tone—Plays a configured message or tone.

If an interface-based resource is not available to admit the call, the call is dropped from the session protocol (such as H.323). If an IP network is congested and a POTS dialpeer is configured, a call can be routed through the PSTN network or to an alternate IP destination.



Note

The PSTN fallback does not ensure that a VoIP call that proceeds over the IP network is protected from the effects of congestion. This functionality is handled by other QoS mechanisms such as IP RTP priority and low latency queuing (LLQ).

For additional information about busyout, the call-denial aspects of this feature, and the PSTN fallback, see the following publications, respectively. Point your web browser to CCO and click the following paths:

- *Advanced Voicebusyout*
[Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 12.2: New Feature Documentation: New Features in 12.2-Based Limited Lifetime Releases: New Features in 12.2 X Releases: New Features in Release 12.2\(2\)XA: Advanced Voice Busyout](#)
- *Call Admission Control Based on CPU Utilization*
[Cisco Product Documentation: Access Servers and Access Routers: Access Servers: Cisco AS5400: Configuration documents for Cisco AS5400: Configuring selected Cisco IOS 12.1-based software features: Call Admission Control based on CPU Utilization](#)

- [PSTN Fallback](#)

Cisco Product Documentation: [Cisco IOS Software Configuration: Cisco IOS Release 12.1: New Feature Documentation: New Features in Release 12.1 T: New Features in Release 12.1\(3\)T: PSTN Fallback](#)

**Note**

The call admission control for H.323 VoIP gateways feature was released previous to Release 12.2(4)XM on some other Cisco routers and access servers. Release 12.2(4)XM introduces the feature on Cisco 1700 series routers.

Call Transfer Capabilities Using the Refer Method

The Call Transfer Capabilities Using the Refer Method feature provide call transfer capabilities that supplement the Bye and Also methods implemented on SIP gateways. Call transfer allows a wide variety of decentralized multiparty call operations. These operations form the basis for third-party call control and are important features for VoIP and SIP. Call transfer also enables conference calls to transition smoothly between multiple point-to-point links and IP level multicasting.

For additional information about the following components of transfer functionality, see the online-only document [Call Transfer Capabilities Using the Refer Method](#):

- Refer Method
- Refer-To Header
- Referred-By Header
- Notify Method
- Using the Refer Method to Achieve Call Transfer
- Blind Transfer
- Attended Transfer

To access this document, point your web browser to CCO, and click the following path:

Cisco Product Documentation: [Cisco IOS Software Configuration: Cisco IOS Release 12.2: New Feature Documentation: New Features in 12.2-Based Limited Lifetime Releases: New Features in 12.2 X Releases: New Features in Release 12.2 XB: New Features in Release 12.2\(2\)XB: Call Transfer Capabilities Using the Refer Method](#)

**Note**

The Call Transfer Capabilities Using the Refer Method feature was released previous to Release 12.2(4)XM on some other Cisco routers and access servers. Release 12.2(4)XM introduces the feature on Cisco 1700 series routers.

Configurable PSTN Cause Code to SIP Response Mapping

For calls to be established between a SIP network and a PSTN network, the two networks must interoperate. The PSTN cause codes indicate the reasons for a PSTN call failure or completion. One aspect of SIP-network and PSTN-network interoperation is the mapping of these PSTN cause codes to SIP status codes or events and the mapping of SIP status codes or events to PSTN cause codes.

The SIP and PSTN networks have standard or default interoperation mappings. Using the Configurable PSTN Cause Code to SIP Response Mapping feature, you can customize the SIP-user-agent software to override the default mappings and configure specific map settings.

Any SIP status code can be mapped to any PSTN cause code, or vice versa. When customized, the settings can be stored in the NVRAM and are restored automatically on bootup.

SIP maps all possible Integrated Services Digital Network (ISDN) cause codes to SIP Error response codes. There is a one-to-one mapping between SIP Response codes and PSTN cause codes. Event mapping tables showing the standard or default mappings between SIP and PSTN are provided in the publication [Configurable PSTN Cause Code to SIP Response Mapping](#).

To access this document, point your web browser to CCO, and click the following path:

Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 12.2: New Feature Documentation: New Features in 12.2-Based Limited Lifetime Releases: New Features in 12.2 X Releases: New Features in Release 12.2 XB: New Features in Release 12.2(2)XB: Configurable PSTN Cause Code to SIP Response Mapping


Note

The Configurable PSTN Cause Code to SIP Response Mapping feature was released previous to Release 12.2(4)XM on some other Cisco routers and access servers. Release 12.2(4)XM introduces the feature on Cisco 1700 series routers.

DTMF Relay for SIP calls Using Named Telephone Events

The dual tone multifrequency (DTMF) Relay using named telephone event (NTE) feature adds support for relaying DTMF tones and hookflash events in SIP on Cisco VoIP gateways.


Note

The DTMF Relay using NTE feature is implemented for SIP only.

Using NTE to relay DTMF tones provides a standardized means of transporting DTMF tones in RTP packets according to section 3 of RFC 2833, *RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals*, developed by the Internet Engineering Task Force (IETF) Audio/Video Transport (AVT) working group. RFC 2833 defines formats of NTE RTP packets used to transport DTMF digits, hookflash, and other telephony events between two peer endpoints.

The DTMF tones are generated when a button is pressed on a touch-tone phone. When the tone is generated, it is compressed, transported to the other party, and decompressed. If a low-bandwidth codec, such as a G.729 or G.723, is used without a DTMF relay method, the tone might be distorted during compression and decompression.

The DTMF-Relay-using-NTE feature allows SIP phones calling voice mail or other Interactive Voice Response (IVR) systems to relay DTMF tones instead of relaying the tones using Cisco Proprietary RTP or transparently in band. Additionally, this feature prevents the distortion of DTMF tones if the RTP session uses a low bit-rate codec, because tones are passed in NTE packets and are not compressed using the default codec.

When using the DTMF-Relay-using-NTE feature, endpoints can perform per-call negotiation of the DTMF relay method. During call setup, the calling and called parties negotiate to choose the DTMF relay mode. They also negotiate to determine the payload type value for the NTE RTP packets.

In a SIP call, the gateway forms a session description protocol (SDP) message that indicates:

- Whether or not NTP is to be used
- Which events are to be sent using NTE
- The NTE payload type value

The DTMF-Relay-using-NTE feature provides support for hookflash, using in-band and out-of-band modes. When using in-band mode, the gateway relays the hookflash without notifying the application and the default session application and any IVR scripts do not receive the hookflash. When using out-of-band mode, the gateway reports the hookflash to the application and the application can relay the hookflash to the next call leg.

**Note**

The DTMF-Relay-using-NTE feature does not support hookflash generation for advanced features such as call waiting and conferencing.

G.728 – CODEC Support on Cisco 1750 and 1751 Routers

Support for the G.728–codec feature on Cisco 1750 and 1750 routers enables the coding of speech at 16 kbps. Codec negotiation involves two phases: a H.245 capability exchange phase and a call establishment phase. Codec negotiation allows a router to offer several codecs during the H.245 capability exchange phase and to ultimately settle on a single common codec during the call establishment phase. Offering several codecs increases the probability of establishing a connection because there is a greater chance of overlapping voice capabilities between endpoints.

Codec negotiation allows a means to specify a prioritized list of codecs associated with a dial peer. During the call establishment phase, the router uses the highest priority codec from the list the router has in common with the remote endpoint. The router also adjusts to the codec selected by the remote endpoint, so a common codec is established for both the receive and the send voice directions.

Codecs have the following characteristics:

- Number of voice data bytes per frame: 10 to 240
- Default number of data bytes per frame: 10
- Bit Rate: 16 kbps

Interactive Voice Response Version 2.0 on VoIP Gateways

The IVR feature consists of simple voice prompting and digit collection to gather caller information for authenticating the user and identifying the destination. You can assign IVR applications to specific ports or invoke them on the basis of the called number; that is, the dialed number identification service (DNIS). An IP public switched telephone network gateway can have several IVR applications to accommodate many different gateway services, and you can customize the IVR applications to present different interfaces to the various callers.

The IVR systems provide information in the form of recorded messages over telephone lines in response to user input in the form of spoken words, or more commonly DTMF signalling. For example, when you make a call with a debit card, an IVR application prompts you to enter a specific type of information, such as an account number. After playing the voice prompt, the IVR application collects the predetermined number of touch tones and then places the call to the destination phone or system.

The IVR uses Tool Command Language (TCL) scripts to gather information and to process accounting and billing. For example, a TCL IVR script plays when a caller receives a voice-prompt instruction to enter a specific type of information, such as a personal identification number (PIN). After playing the voice prompt, the TCL IVR application collects the predetermined number of touch tones and sends the collected information to an external server for user authentication and authorization.

The TCL IVR Version 2.0 on the Cisco 1750 and Cisco 1751 routers consists of the following elements:

- RTSP client implementation
- TCL IVR prompt playout and digit collection on IP call legs
- New TCL verbs to utilize RTSP scripting features
- IVR application MIB

This feature provides the following capabilities:

- Adds scalability and enables TCL IVR scripting functionality on VoIP call legs.
- Reduces the CPU load and saves router memory because no packetization is involved.
- Supports RTSP to enable VoIP gateways to play messages from RTSP-compliant announcement servers and voice mail servers.
- Allows larger prompts to be played.
- Provides support for the use of an external audio server.
- Supports a robust IVR script checking mechanism when a new script is loaded.
- Provides backward-compatible support for TCL IVR 1.0 scripts.

ISDN Progress Indicator Support for SIP Using 183 Session Progress

This feature provides support for handling inband treatments, such as call progress tones and announcements, when SIP is the session protocol for establishing call connections. The feature ensures the correct establishment of the media stream through the SIP network to allow the successful transport of inband treatments, which might ingress from a PSTN node on a SIP gateway or egress to a PSTN node. The feature also allows VoIP calls using SIP to provide inband call treatment such as ringback tones, announcements when interworking with ISDN and channel associated signaling (CAS) PSTN networks.

Release 12.2(4)XM supports SIP 183 Session Progress messages, which facilitate better call treatment for SIP VoIP calls when interworking with PSTN networks. The introduction of the 183 Session Progress message allows a called user agent to suppress local alerting from the calling user agent, and to play a tone or announcement during a preliminary call session, before the full SIP session is set up. This functionality enables the calling party to be notified of the status of the call without being charged for the preliminary portion of the call. A new Session header in the 183 Session Progress message controls whether or not the called user agent plays a tone or announcement for the calling party. The 183 Session Progress message is supported by default and does not require any special configuration.

Layer 2 Class of Service Matching and Marking

The matching and marking of layer 2 class of service (COS) bits to the Differentiated Services Codepoint (DSCP) bits in the IP header and vice versa is supported by Release 12.2(4)XM on Cisco 1700 series routers. Through IEEE 802.1q trunking support, WAN routers can trunk the separate VLANs from Ethernet switch. Ethernet switches use separate VLANs for voice and data. User priority bits in the 802.1p portion of the 802.1q standard header provide prioritization in Ethernet switches. Cisco 1750 and 1751 routers support both 802.1p and 802.1q VLAN trunking.

Prerequisites

The following configuration tasks must be completed before a Cisco 1700 series router can support the layer 2 COS matching and marking feature:

-
- Step 1** Install the required IOS software version on the router.
 - Step 2** Enable IP routing.
 - Step 3** Configure the router for VLAN.
-

Configuring the IEEE 802.1p Feature

To configure Cisco 1700 series routers to support the Cisco IOS Layer 2 COS matching and marking feature, use the following commands, beginning in global configuration mode:

Step	Command	Task
1.	<code>router(config)# class-map [match-all match-any] <i>class-map-name</i></code>	Configure the QoS class map. To verify the class-map configuration, enter the command show class-map class-map-name .
2.	<code>router(config-cmap)# match [ip dscp cos] [<i>differentiated_services_codepoint_values</i> <i>class-of-service_values</i>]</code>	Configure the classification criteria. Up to 8 differentiated services codepoint values or 4 class-of-service values can be entered.
3.	<code>router(config-cmap)# description <i>description_of_the_class-map</i></code>	Provide the class-map description.
4.	<code>router(config-cmap)# rename <i>new class-map name</i></code>	Rename the class-map.
5.	<code>router(config)# policy-map <i>policy-map name</i></code>	Configure the QoS Policy Map. To verify the policy-map configuration, enter the command show policy-map policy-map-name/interface .
6.	<code>router(config-pmap)# class <i>class-map_name</i></code>	Configure the policy criteria. The <i>class_map_name</i> should be one of the names used in Step 1 or Step 4.
7.	<code>router(config-pmap)# description <i>description_of_the_policy-map</i></code>	Enter the Policy-Map description.
8.	<code>router(config-pmap)# rename <i>new_policy-map_name</i></code>	Rename the policy-map.
9.	<code>router(config-pmap-c)# set [cos ip dscp] [<i>cos_value</i> <i>services_codepoint_value</i>]</code>	Set the QoS values.
10.	<code>router(config)# interface [FastEthernet Ethernet] <i>port number.sub-interface number</i></code>	Configure the Ethernet interface to perform the Layer 2 COS matching and marking.
11.	<code>router(config-subif)# encapsulation [dot1Q] [<i>IEEE_802.1Q_VLAN_ID</i>]</code>	Set the encapsulation type for the interface configured in Step 10.
12.	<code>router(config-subif)# ip address 1.9.85.153 255.255.0.0</code>	Configure the IP address and its network mark.
13.	<code>router(config-subif)# service-policy [input output history] <i>policy-map_name</i></code>	Configure the QoS service policy. The <i>policy_map_name</i> should be one of the names used in Step 5 or Step 8.

Configuration Example

The following example shows the configuration of the 802.1p feature on a Cisco 1751 router. This configuration attempts to match DSCP 8 to COS 2. Note the configuration of the class-map, policy-map, and QoS service policy.

```
Router_1751#sh run
Building configuration...

Current configuration : 1078 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Router_1751
!
!
memory-size iomem 25
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip subnet-zero
!
!
ip dhcp pool vespa
    network 192.168.1.0 255.255.255.0
    default-router 192.168.1.1
    option 150 ip 192.168.1.1
!
ip cef
vpdn enable
!
class-map match-all qos-test
    match ip dscp 8
!
!
policy-map 8021p-set
    class qos-test
        set cos 2
!
!
interface FastEthernet0/0
    no ip address
    speed auto
!
interface FastEthernet0/0.1
    encapsulation dot1Q 256
    ip address 1.9.85.153 255.255.0.0
    service-policy output 8021p-set
!
interface Serial1/0
    ip address 3.0.0.3 255.0.0.0
    no keepalive
!
interface Serial1/1
    no ip address
    shutdown
!
ip default-gateway 1.8.0.1
ip classless
```



```

ip route 1.9.0.0 255.255.0.0 FastEthernet0
ip route 223.255.254.254 255.255.255.255 1.8.0.1
no ip http server
ip pim bidir-enable
!
!
tftp-server flash:SEPDEFAULT.cnf
!
trunk group 650
  hunt-scheme round-robin
!
line con 0
line aux 0
line vty 0 4
  login
line vty 5 15
  login
!
end

```

MGCP

The Media Gateway Control Protocol (MGCP) is a device control protocol developed within the IETF which provides call control elements (Softswitches or Call Agents) for controlling Media Gateways (MGs) in a packet telephony system. In this master-and-slave protocol model, the Call Agents are external to the MGs and the gateways execute commands sent by the Call Agents. The MGCP does not define a mechanism for synchronizing Call Agents; the protocol assumes that the commands the Call Agents send to the gateways under their control are synchronized and coherent. The MGCP is not a standard and is currently in version 1.0 as an RFC.

For a description of the MGCP model and a definition of MGCP 1.0, see the publication [MGCP 1.0 Including NCS 1.0 and TGCP 1.0 Profiles](#). To access this document, point your web browser to CCO, and click the following path:

Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 12.2: New Feature Documentation: New Features in Release 12.2T: New Features in Release 12.2(4)T: MGCP 1.0 Including NCS 1.0 and TGCP 1.0 Profiles



Note

The MGCP model and MGCP 1.0 were released previous to Release 12.2(4)XM on some other Cisco routers and access servers. Release 12.2(4)XM introduces these features on Cisco 1700 series routers.

MGCP 1.0

The MGCP 1.0 Profile feature implements the MGCP 1.0 (RFC 2705) protocol on supported Cisco media gateways. The feature is backward-compatible with MGCP 0.1, Simple Gateway Control Protocol (SGCP) 1.1, and SGCP 1.5.

MGCP-Based Fax (T.38) and DTMF Relay

The MGCP-Based Fax (T.38) and DTMF Relay feature provides capabilities on Cisco IOS voice gateways to reliably transmit fax and DTMF in an MGCP network. The feature enhances the existing proprietary DTMF and fax pass-through implementations by supporting RFC2833 and International

Telegraph Union-T (ITU-T) T.38 standards, respectively. The T.38 standard is a real-time, Group 3, Fax-over-IP standard, which enhances the reliability of fax transmissions and reduces bandwidth requirements.

Support for RFC 2833 provides a standardized method of DTMF transmission, based on telephony events. The RFC 2833 facilitates interoperability with third-party platforms including, but not limited to: voice mail, unified messaging, voice gateways, and media servers.

MGCP Basic Class and Operator Services

The MGCP basic class and operator services (BCOS) are a set of calling features, sometimes called “custom calling” features, that use MGCP to transmit voice, video, and data over the IP network. These features are usually found in circuit-based networks. MGCP BCOS brings them to the Cisco IOS gateways on packet-based networks.

The following MGCP BCOS features are available on RGWs:

- Distinctive power ring
- Various tones and rings
- Visual Message Waiting Indicator
- Caller ID (Caller ID Type 1)
- Caller ID with Call Waiting (Caller ID Type 2)
- Distinctive Call Waiting Tone
- Message Waiting Tone
- Off-Hook Warning Tone
- Three-Way Calling
- xGCP support for the following codecs: G.711, G.723, G.726, G.729, G.729a and G.728



Caution

Cisco 1751 routers do not support Network-based Call Signaling (NCS) 1.0, the PacketCable profile of MGCP 1.0 for residential gateways (RGWs) or Trunking Gateway Control Protocol (TGCP) 1.0, the PacketCable profile of MGCP 1.0 for trunking gateways (TGWs).

MGCP VoIP Call Admission Control

The MGCP VoIP CAC feature enables gateways managed by Call Agents to identify and gracefully refuse calls that are susceptible to poor voice quality. Poor voice quality on an MGCP voice network can result from the following sources:

- Transmission artifacts such as echo
- The use of low quality codecs
- Network congestion and delay
- Overloaded gateways

The first two causes of poor voice quality are overcome by the use of echo cancellation and better codec selection. The last two causes are addressed by the MGCP VoIP CAC feature, which ensures gateway and network resource availability. The MGCP VoIP CAC feature disallows calls when resources are above configured thresholds and reserves guaranteed bandwidth throughout the network for each completed call.

MGCP VoIP CAC has three components for improving voice quality and reliability:

- System Resource Check (SRC) CAC—Evaluates memory and call resources local to the gateway. It is supported on MGCP 1.0 and MGCP 0.1.
- Resource Reservation Protocol (RSVP) CAC—Surveys bandwidth availability on the network, reports the results of the reservation request to the call agent, and reserves bandwidth across IP networks using RSVP. Trigger thresholds are configurable on the gateway. RSVP CAC is supported on MGCP 1.0 and MGCP 0.1.
- Cisco Service Assurance Agent (SA Agent) CAC—Uses Response Time Reporter (RTR) to appraise network congestion conditions. It is supported on MGCP 1.0 only.



Note SA Agent was called RTR in earlier Cisco IOS software releases.

If all three CAC types are configured on a gateway, the gateway checks resources in the following order:

1. SRC CAC
2. RSVP CAC
3. SA Agent CAC

If any resource check fails, the call fails and no further checks are performed. When the call fails, the gateway refuses to accept it.



Note

The MGCP VoIP CAC feature is not supported on the NCS 1.0 and TGCP 1.0 profiles of MGCP 1.0.

Modem Passthrough over VoIP

The modem passthrough over VoIP feature provides the transport of modem signals through a packet network by using pulse code modulation (PCM) encoded packets. The Modem Passthrough over VoIP feature performs the following functions:

- Represses processing functions like compression, echo cancellation, high-pass filter, and voice activity detection (VAD).
- Issues redundant packets to protect against random packet drops.
- Provides static jitter buffers of 200 milliseconds to protect against clock skew.
- Discriminates modem signals from voice and fax signals, indicating the detection of the modem signal across the connection, and placing the connection in a state that transports the signal across the network with the least amount of distortion.
- Reliably maintains a modem connection across the packet network for a long duration under normal network conditions.

For additional information, see the [Modem Passthrough over Voice over IP](#) publication. To access this document, point your web browser to CCO, and click the following path:

Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 12.1: New Feature Documentation: New Features in Release 12.1 T: New Features in Release 12.1(3)T: Modem Passthrough over Voice over IP

**Note**

The Modem Passthrough over VoIP feature was released previous to Release 12.2(4)XM on some other Cisco routers and access servers. Release 12.2(4)XM introduces the feature on Cisco 1700 series routers.

NAT Support for SIP

Release 12.2(4)XM2 supports the ability to deploy Network Address Translation (NAT) between VoIP solutions that are based on the SIP. The SIP is an application-layer signaling protocol for creating and controlling multimedia sessions with two or more participants and a client-server protocol transported over TCP or UDP. An Application Layer Gateway (ALG) with NAT enables the SIP. The messages in the protocol might have IP addresses embedded in the packet payload. If a message passes through a router configured with NAT, the embedded information must be translated and encoded back to the packet.

**Note**

Note: NAT only translates embedded IP version 4 addresses.

In Release 12.2(4)XM2 the new option **sip** is available for the command **debug ip nat**. When the **sip** debug option is on, the router displays messages related to the NAT processing of SIP messages:

```
debug ip nat [ ACL | detailed | h323 | sip | pptp ]
```

By default, NAT expects SIP messages only on port 5060 (TCP and UDP). To configure more ports, use the following command:

```
ip nat register port port_number protocol sip [ tcp | udp ]
```

RFC2782 Compliance (Style of DNS SRV Queries)

SIP on Cisco VoIP gateways uses a Domain Name System Server (DNS SRV) query to determine the IP address of the user endpoint. The query string has a prefix in the form of “protocol.transport.” and is attached to the fully qualified domain names (FQDNs) of the next hop SIP server. This prefix style, from RFC 2052, has always been available; however, with this release, a second style is also available.

The second style is in compliance with RFC 2782, and prepends the protocol label with an underscore “_”; as in “_protocol._transport.”. The addition of the underscore reduces the risk of the same name being used for unrelated purposes. The form compliant with RFC 2782 is the default style. Use the command **srv version** to configure the DNS SRV feature.

SIP Diversion Header Implementation for Redirecting Number

The SIP Diversion Header Implementation for Redirecting Number feature provides support for a new SIP header field; Call Control (CC)-Diversion. The CC-Diversion header field enables the SIP gateway to pass call control redirecting information during the call setup. Call control redirection is the redirection of a call based on a subscriber service such as call forwarding or call deflection. Call redirection information is information that is typically used for Unified Messaging and voice mail services to identify the recipient of a message. Call control redirection information can also be used to support applications such as automatic call distribution and enhanced telephony features such as Do Not Disturb and Caller ID.

If the CC-Diversion header field is generated by the SIP gateway during the call process, the header field is based on the contents of the Redirecting Number Information Element (IE) in the ISDN Setup message. In addition, information such as the reason the call was redirected is included in the CC-Diversion header field.

See the online-only document [SIP Diversion Header Implementation for Redirecting Number](#) for call flow samples of the following types of gateway-to-gateway calls:

- Redirection with CC-diversion
- SIP 3xx redirection response after receipt of a SIP 18x information response

To access this document, point your web browser to CCO, and click the following path:

Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 12.1: Related Documentation: Session Initiation Protocol Gateway Call Flows: SIP Gateway Support for Third Party Call Control



Note

The SIP Diversion Header Implementation for Redirecting Number feature was released previous to Release 12.2(4)XM2 on some other Cisco routers and access servers. Release 12.2(4)XM2 introduces the feature on Cisco 1700 series routers.

SIP for VoIP Enhancements

VoIP currently implements the ITU's H.323 specification within Internet Telephony Gateways (ITGs) to signal voice call setup. SIP is a new protocol developed by the IETF for multimedia conferencing over IP. SIP features are compliant with IETF RFC 2543, SIP: Session Initiation Protocol, published in March 1999. The Cisco SIP functionality in Release 12.2(4)XM2 enables Cisco 1700 series routers to signal the setup of voice and multimedia calls over IP networks.

Release 12.2(4)XM2 supports SIP feature enhancements on Cisco 1700 series routers, which enable SIP gateways with the following functionality:

- Enables Cisco voice-enabled platforms to provide RFC2543 compliant user-agent client gateways.
- Supports proxy-routed calls.
- Redirects an unanswered call to another SIP gateway or SIP-enabled IP phone.
- Allows end users to place calls on hold.
- Hides the identity of the calling party, based on the setting of the ISDN presentation indicator.

Additionally, the following SIP for VoIP feature enhancements are supported by Release 12.2(4)XM:

- SIP mid-call changes of SDP sessions using an INVITE with changed SDP.
- Enhanced SIP stack to support new routing headers (including the headers: Also, Contact, Expires, Max-Forwards, Record-Route, Requested-By, Route, Timestamp, and Unsupported).
- Call Hold and Call Transfer.
- Session Progress Messages 180, 183, and 184, with inband alerts.
- Enhanced PSTN-to-SIP Event and Cause-Code Mapping.
- UDP socket layer enhancements to support connected sockets; enabling Internet Control Message Protocol (ICMP) network notifications to be used to identify destinations rather than relying only on SIP timers.
- Interoperation with the Amteva UCS Messaging platform.
- IPSec in SIP security.

SIP Gateway Support for Bind Command

In previous releases of Cisco IOS software, the source address of a packet going out of the gateway was never deterministic. That is, the session protocols and VoIP layers always depended on the IP layer to give the *best local address*. The best local address was then used as the source address (the address showing where the SIP request came from) for signaling and media packets. Using this nondeterministic address occasionally caused confusion for firewall applications, as a firewall could not be configured with an exact address and would take action on several different source address packets.

However, the **bind** interface command allows you to configure the source IP address of signaling and media packets to a specific interface's IP address. Thus, the address that goes out on the packet is bound to the IP address of the interface specified with the **bind** command. Packets that are not destined to the bound address are discarded. When you do not want to specify a bind address, or if the interface is down, the IP layer still provides the best local address.

The bind command performs different functions based on the state of the interface:

Interface State	Result Using Bind Command
Shutdown With or without active calls	The TCP and UDP socket listeners are initially closed. (Socket listeners receive datagrams addressed to the socket.) The sockets are then opened to listen to any IP address. If the outgoing gateway has the bind command enabled and has an active call, the call becomes a one-way call with media flowing from the outgoing gateway to the terminating gateway.
No Shutdown No Active Calls	The TCP and UDP socket listeners are initially closed. The sockets are then opened and bound to the IP address that are set by the bind command. The sockets accept packets destined for the bound address only.
No Shutdown Active Calls	The TCP and UDP socket listeners are initially closed. The sockets are then opened to listen to any IP address.
Bound interface IP address is removed	The TCP and UDP socket listeners are initially closed. The sockets are then opened to listen to any address, because the IP address has been removed. A message is printed stating that the IP address has been deleted from a SIP-bound interface. If the command bind is enabled on an outgoing gateway and the gateway has an active call, the call becomes a one-way call, with media flowing from the outgoing gateway to the terminating gateway.
The physical cable is pulled on the bound port, or the Interface Layer goes down	The TCP and UDP socket listeners are initially closed. The sockets are then opened and bound to listen to any address. When the pulled cable is replaced, the result is as documented for no shutdown interfaces.
A bind interface is shutdown, or its IP address is changed, or the physical cable is pulled while SIP calls are active	The call becomes a one-way call with media flowing in only one direction. Media flows from the gateway where the change or shutdown took place, to the gateway where no change occurred. Thus, the gateway with the status change no longer receives media. The call is then disconnected, but the disconnected message is not understood by the gateway with the status change, and the call is still assumed to be active.

**Note**

If there are active calls and the command **bind** is issued for the first time or issued while another **bind** command is in effect, the **bind** command does **not** take effect. A message is printed to remind you that there are active calls and the **bind** command changes cannot take effect.

SIP Gateway Support for Third Party Call Control

Release 12.2(4)XM2 supports the SIP Gateway Support for Third-Party Call Control feature, which enables one endpoint (for example, a call controller) to create, modify, or terminate calls between other endpoints via *delayed media negotiation*. In delayed media negotiation, the SDP information is not completely advertised in the initial call setup. Third-party call control is often used for conferencing and operator services (creating a call connecting two parties together).

Release 12.2(4)XM2 also supports the following functionality:

- Negotiation enhancements for codec
- Enhancements in the SDP parser and builder on SIP gateways
- Endpoints specified as FQDNs in the SDP

Gateways can route on an FQDN in addition to routing on an IP address. When the SIP gateway receives a SIP message containing a FQDN in the c= SDP field, it parses the c= field of the SDP body, determines that it is a FQDN and resolves the next hop via a DNS query.

See the online-only document [SIP Gateway Support for Third Party Call Control](#) for a diagram and description of each handshaking event for the following types of calls:

- SIP Gateway-to-SIP Gateway Call—Call Setup with Delayed Media via Third-Party Call Controller
- SIP IP Phone-to-SIP Gateway—Call Setup and Call Hold with Delayed Media
- SIP Gateway-to-One Call—Call Setup with Voice Mail
- SIP Gateway-to-SIP Gateway—Call Setup using a FQDN and Delayed Media

To access this document, point your web browser to CCO, and click the following path:

Cisco Product Documentation: [Cisco IOS Software Configuration: Cisco IOS Release 12.1: Related Documentation: Session Initiation Protocol Gateway Call Flows: SIP Gateway Support for Third Party Call Control](#)

**Note**

The SIP Gateway Support for Third-Party Call Control feature was released previous to Release 12.2(4)XM2 on some other Cisco routers and access servers. Release 12.2(4)XM2 introduces the feature on Cisco 1700 series routers.

SIP Gateway Support of RSVP and "tel" URL

The SIP Gateway Support of RSVP and Telephone Uniform Resource Locators (TEL URL) feature provides the following new headers:

- Content-Disposition
- Supported
- Unsupported
- RSeq
- RSck

The feature also supports the following SIP enhancements:

- **RSVP**—The coordination of SIP call signaling and RSVP resource management. A QoS module is provided that acts as a broker between the VoIP Service Provider Interfaces (SPIs) and the Cisco IOS RSVP subsystem. The QoS module enables the VoIP SPIs to initiate resource reservation, modify parameters of an existing reservation, and clean up the reserved resources. The QoS module then communicates the results of the operation to the RSVP subsystem.
- **Telephone URL Format in SIP Messages**—Support for TEL URL. The TEL URL formats describe voice call connections, including the originator, recipient, and destination. The TEL URLs enable a gateway to accept TEL calls sent through the Internet and to generate TEL URLs in the request line of outgoing INVITEs requests.
- **Interaction with Forking Proxies**—Call forking enables the terminating gateway to handle multiple requests and enables the originating gateway to handle multiple provisional responses for the same call. Interaction with forking proxies applies to gateways acting as a user agent client (UAC), and takes place when a user is registered to several different locations.
- **Reliability of SIP Provisional Responses**—SIP reliable provisional responses ensure that media information is exchanged and resource reservation can take place prior to connecting the call. Provisional acknowledgement (PRACK) and conditions met (COMET) are two methods that have been implemented. PRACK allows reliable exchanges of SIP provisional responses between SIP endpoints. COMET indicates if the pre-conditions for a given call or session have been met.
- **RFC2782 Compliance (Style of DNS SRV Queries)**—SIP on Cisco VoIP gateways uses DNS SRV query to determine the IP address of the user endpoint. The query string has a prefix in the form of “protocol.transport.”, which is attached to the FQDN of the next hop SIP server. This prefix style, from RFC 2052, has always been available; however, with this release, a second style is also available. The second style is in compliance with RFC 2782, and prepends the protocol label with an underscore “_”; as in “_protocol._transport.”. The addition of the underscore reduces the risk for the same name to be used for unrelated purposes. The form compliant with RFC 2782 is the default style. Use the command **srv version** to configure the DNS SRV feature.

SIP Intra-Gateway Hairpinning

SIP Intra-Gateway Hairpinning—SIP hairpinning is a call routing capability in which an incoming call on a specific gateway is signaled through the IP network and back out the same gateway. This can be a PSTN call routed into the IP network and back out to the PSTN over the same gateway. Similarly, SIP hairpinning can be a call signaled from a line (for example, a telephone line) to the IP network and back out to a line on the same access gateway. With SIP hairpinning, unique gateways for ingress and egress are no longer necessary.

SIP INVITE Request with Malformed Via Header

A SIP INVITE requests a user or service to participate in a session. Each INVITE contains a Via header that indicates the previous transport path of the request and where to send a response.

When an INVITE contains a malformed Via header, the SIP INVITE Request with Malformed Via Header feature provides a response to the malformed request. When a response to a malformed Via field is sent to the source IP address at UDP port 5060 (the IP address where the SIP request originated), a counter, *Client Error: Bad Request*, also increments. *Bad Request* is a class 400 response and includes the explanation *Malformed Via Field*.

**Note**

This feature applies to messages arriving on UDP because the Via header is not used to respond to messages arriving on TCP.

SIP T.38 Fax Relay

The SIP T.38 fax relay feature adds standards-based fax support to SIP and conforms to ITU-T T.38, *Procedures for real-time Group 3 facsimile communication over IP networks*. The ITU-T standard specifies real-time transmission of faxes between two regular fax terminals over an IP network. Much like a voice call, SIP T.38 fax relay requires call establishment, data transmission, and release signaling.

The following functionality is also included in SIP T.38 fax relay:

- Support for Facsimile User Datagram Protocol transport layer (UDPTL)

UDPTL, as defined in ITU-T T.38, is a transport layer that is used on top of UDP. The UDPTL makes the delivery of packets more reliable by providing data redundancy.

- Support for QoS

SIP T.38 fax relay supports QoS when establishing T.38 sessions. If the dial peer is already configured for QoS, then the T.38 stream maintains the QoS support. QoS ensures certain bandwidth reservations for calls.

SIP User Agent MIB

The SIP User Agent MIB adds the ability to manage a SIP network via an SNMP-based network management platform.

T.37 Store and Forward Fax

The Store and Forward Fax feature enables Cisco 1700 series routers to transmit and receive faxes across packet-based networks using the H.323 protocol. This feature is an implementation of the RFC 2305 proposed standard from the IETF, which is the same as the T.37 recommendation from the ITU.

Store and Forward Fax supports the following functionality:

- Single number access for voicemail and fax access
- Sending and receiving faxes to and from Group 3 fax devices
- Receiving faxes that are delivered as e-mail attachments
- Creating and sending standard e-mail messages to be delivered as faxes to standard Group 3 fax devices
- Real-time fax fallback

**Caution**

Before configuring the store and forward fax feature, ensure that VoIP software is installed and functional on the Cisco 1700 series routers.

When configured for fax detection, Cisco 1700 series routers automatically listen to incoming calls to discriminate between voice and fax. The routers then direct the calls to the appropriate application or server.

Fax detection is implemented by configuring a fax detection application and dial peers for fax detection. The fax detection application (a Cisco IVR application) determines whether a call is voice or fax so that the call is routed appropriately. A voice call can be broken into discrete call segments, or call legs, that connect the various intermediate points and end points of a call. Voice technologies use configuration constructs called dial peers to define call legs and to associate various attributes with them. The attributes are used to make routing decisions that provide more flexibility than simply routing by a dialed number.

New Software Features in Release 12.2(4)T

For information regarding the features supported in Cisco IOS Release 12.2 T, refer to the Cross-Platform Release Notes and New Feature Documentation links at the following location on CCO:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122relnt/xprn122t/index.htm>

This URL is subject to change without notice. If it changes, point your web browser to CCO, and click the following path:

Service & Support: Technical Documents: Cisco IOS Software: Release 12.2: Release Notes: Cross-Platform Release Notes (Cisco IOS Release 12.2T)

Limitations

The following sections describe limitations about Cisco IOS Release 12.2(4)XM4 that can apply to the Cisco 1700 series routers. (Also, see the “Caveats” section on page 37.)

Commands Not Supported on Cisco 1750 and 1751 Routers

The following command line interface (CLI) commands and functionality are not supported on Cisco 1750 or 1751 routers:

- The AVBO commands (Cisco 1750 and 1751 routers do not support T1/E1 CAS and T1/E1 primary rate interface [PRI]):
 - `ds0 busyout`
 - `isdn service b_channel`
 - `isdn service dsl`
- CAC commands (Cisco 1750 and 1751 routers do not support T1 CAS):
 - `ds0-group`
- Fax interface-type modem commands (Cisco 1750 and 1751 routers do not support modem cards). The following associated debug commands are also disabled:
 - `debug text-to-fax`
 - `debug tiff reader`
 - `debug tiff writer`

Features Not Supported on Cisco 1700 Series Routers

Release 12.2(4)XM4 does not support the following features on the Cisco 1700 series routers mentioned below:

- Global system for mobile communication over frame relay (GSM-FR) on Cisco 1700 series routers.
- NCS 1.0, the PacketCable profile of MGCP 1.0 for RGWs on Cisco 1751 routers.
- TGCP 1.0, the PacketCable profile of MGCP 1.0 for TGWs on Cisco 1751 routers.

Features Not Supported on Cisco 1760 Routers

The following features are not supported by Release 12.2(4)XM4 on Cisco 1760 routers:

- CAC for VoIP call
- DiffServ for voice signaling traffic
- G.728 codec support
- Modem pass through over VoIP
- MGCP features
 - MGCP 1.0
 - MGCP based fax (T.38) and DTMF relay
 - MGCP basic CLASS and operator services
 - MGCP VoIP call admission control
- RTSP enhanced IVR
- SIP features
 - Call transfer capabilities using the refer method
 - Configurable PSTN cause code to SIP response
 - Gateway support for bind command
 - ISDN progress indicator support for SIP using 183 session progress
 - NAT support for SIP
 - RFC2782 compliance for DNS SRV
 - SIP
 - SIP diversion header implementation for redirecting number
 - SIP DTMF relay using NTE
 - SIP for VoIP enhancements
 - SIP gateway support for third party call control
 - SIP gateway support of RSVP and “tel” URL
 - SIP intra-gateway hairpinning
 - SIP INVITE request with malformed via header
 - SIP T.38 fax relay
 - SIP user agent MIB

- T.37 fax relay
- TCL scripting for IVR

**Note**

SIP and MGCP features are not supported on Cisco 1760 routers.

Functionality Not Supported on Cisco 1750 and 1751 Routers

The following functionality is not supported by Release 12.2(4)XM4 on Cisco 1750 or 1751 routers:

- Remote alarm indication (RAI) is not supported because Cisco 1750 series routers do not support T1 CAS.
- Soft Busyout is not supported because this functionality is supported only for DS0 and ISDN.

Cisco 1751 routers do not support the following PacketCable profiles of MGCP 1.0:

- NCS 1.0 for RGWs
- TGCP 1.0 for TGWs

Cisco 1751 routers do not support ISDN PRI/CAS; therefore, the following SIP call sequence is also not supported:

ISDN PRI/CAS - SIP Orig. Gateway - SIP Term. Gateway - ISDN PRI/CAS

Important Notes

The following sections contain important notes about Cisco IOS Release 12.2(4)XM4 that can apply to the Cisco 1700 series routers. (Also, see the [“Caveats” section on page 37.](#))

“Faxrate 14000” for T.38

T.37 works in conjunction with T.38, which was released for Cisco 1750 and 1751 routers in a release prior to Release 12.2(4)XM. The “faxrate 14000” is now added to T.38.

Fan Operation in Cisco 1700 Series Routers

The fans in some Cisco 1700 series routers stay off until thermally activated. The fans in Cisco 1760 and 1760-V routers are always on.

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.

H.450 Features Supported on Cisco 1750 and 1751 Routers

Previous to Release 12.2(4)XM, H.450 features were not supported on Cisco 1750 and 1751 routers because IVR was not supported. The H.450 features are now supported, as Release 12.2(4)XM supports IVR on Cisco 1750 and 1751 routers.

Layer 2 COS Matching and Marking Feature Configuration Sequence

The class-map, policy-map, and service-policy for the Layer 2 COS matching and marking feature must be configured in the proper sequence. For example, if you change the class-map configuration, you must also update the policy-map and the service-policy. To change the policy-map configuration, you must first update the class-map, then change the policy-map, and finally update the service-policy.

Peak Cell Rate and Sustainable Cell Rate Values

On Cisco 1700 routers, specify the Peak Cell Rate (PCR) and Sustainable Cell Rate (SCR) as multiples of 32 Kbps. Other rates are treated as the next lower value of a multiple of 32. For example, an entered PCR value of 150 is considered 128.

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:**).

Caveats

Caveats describe unexpected behavior or defects in Cisco IOS software releases. Severity 1 caveats are the most serious caveats, severity 2 caveats are less serious, and severity 3 caveats are the least serious of these three severity levels.

All caveats in Release 12.2 T are also in Release 12.2(4)XM4. For information on caveats in Cisco IOS Release 12.2 T, refer to the [Caveats for Cisco IOS Release 12.2 T](#) document. For information on caveats in Cisco IOS Release 12.2, refer to the [Caveats for Cisco IOS Release 12.2](#) document. These documents list severity 1 and 2 caveats, and are located on CCO and the Documentation CD-ROM.



Note

If you have an account with Cisco.com, you can also use the Bug Toolkit to find select caveats of any severity. To reach the Bug Toolkit, log in to Cisco.com and click **Service & Support: Technical Assistance Center: Tool Index: Bug Toolkit**. Another option is to go to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl.

Caveats - Releases 12.2(4)XM2, 12.2(4)XM3, and 12.2(4)XM4

There are no new or resolved caveats in software Releases 12.2(4)XM2, 12.2(4)XM3, or 12.2(4)XM4.

Resolved Caveats - Release 12.2(4)XM1

This section describes unexpected behavior in software Release 12.2(4)XM that is fixed in Release 12.2(4)XM1.

Management

CSCdv65207

The command-line interface (CLI) does not prompt for the **erase** keyword when the **copy [/erase] source-url destination-url EXEC** command is entered. This behavior does not allow a file system to be erased using the **copy [/erase] source-url destination-url EXEC** command. To work around this problem, enter the **erase filesystem:** command before entering the **copy EXEC** command.

CSCdu86498

When AAA Authentication is enabled and default group RADIUS is configured, you are prompted for a user-name and password. Previous Cisco IOS releases only prompted you for “enable password.” To work around this problem, enter any character(s) at the user-name prompt and then enter the enable password.

Release 12.2(4)XM - Caveats

This section describes possibly unexpected behavior by Release 12.2(4)XM. Only severity 1 through 3 caveats are included.

Miscellaneous Caveats

CSCdu53872

When a fax machine sends high-density pages through Cisco 1700 series routers, the required transmission time can be too long, causing a time out and breaking the connection. To work around this problem, decrease the fax-page density.

CSCdu63909

Offramp does not work with FXO cards. When mail is sent from a mail server to an Offramp gateway, a connection is established but is then disconnected without receiving a fax.

CSCdv42255

In global level configuration mode, the “mgcp” keyword initiates MGCP processes. However, if the voice port associated with “mgcpapp” is in an active (off-hook) state and a system administrator issues the global command **no mgcp** during an unconfigure stage, Cisco 1700 series routers do not stop MGCP processes. To shut down MGCP processes, force the voice-port to the inactive (on-hook) state.

CSCdv91375

When SIP messages must be mapped to ISDN SETUP or CONNECT messages, the corresponding PI value is missing from the messages. To work around this issue, explicitly set the command **progress_ind** in the corresponding dial-peer, as follows:

```
progress_ind setup enable 1
progress_ind connect enable 2
```

CSCdw05578

When the call threshold is set to a maximum of one call, many H.323 calls can be made but MGCP calls fail and the error message “403 endpoint does not have resources” is displayed. To work around this issue, set the call thresholds individually for H.323 calls and MGCP calls.

CSCdw09722

The 802.1p matching and marking of layer 2 COS occurs when the command **ip cef** is enabled on Cisco 1700 series routers. After configuring service policies for an interface and disabling the command **ip cef**, the feature works properly and packets are marked with the configured COS value.

CSCdw11276

The 802.1p matching and marking of layer 2 COS CLI and MIB have differing sizes for the policy name and the policy description.

SIP-Related Caveats**CSCdw04200**

When an INVITE is sent to a router without SDP, the router responds with a 183 message, and a subsequent re-INVITE is sent to the router, codec negotiation happens but the command **show voice dsp** is not updated with the new codec. To work around this problem, if the initial INVITE is sent without SDP, send the SDP using the ACK.

MGCP-Related Caveats**CSCdv79984**

The redirection of event notification messages to a new Call Agent by way of “N:new-ca-ip-address:port” in a Call Agent command fails. The failure occurs only for events configured as “persistent events” with the command **mgcp persistent <event-name>** on Cisco 1700 series routers. The event notifications are instead only sent to the original Call Agent.

CSCdw13666

When the “S: vmwi(-)” parameter is sent in a MGCP message to an endpoint that is off hook, the message LED on the phone stays on after the phone is placed on-hook. To work around this problem, rely on the mail waiting indicator tones instead of the voice mail waiting indicator LED.

CSCdw13706

When the “S: vmwi(+)” parameter is sent to an endpoint that is off-hook and the phone is placed on-hook without making a call, the phone LED does not go on. To work around this problem, rely on the mail waiting indicator tones instead of the voice mail waiting indicator LED.

Related Documentation

The following sections describe the documentation available for the Cisco 1700 series routers. 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 Cisco.com 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](#)
- [Cisco IOS Software Documentation Set](#)

Release-Specific Documents

The following documents are specific to Release 12.2 and apply to Release 12.2(4)XM4. They are located on Cisco.com and the Documentation CD-ROM (under the heading **Service & Support**):

- To reach the [Release Notes for the Cisco 1700 Series Routers for Cisco IOS Release 12.2\(4\)XM](#), click this path:
Technical Documents: Cisco IOS Software: Release 12.2: Release Notes: Cisco 1700 Series Routers: Cisco 1700 Series - Release Notes for Release 12.2(4)XM
- To reach the [Cross-Platform Release Notes for Cisco IOS Release 12.2 T](#), click this path:
Technical Documents: Cisco IOS Software: Release 12.2: Release Notes: Cisco IOS Release 12.2 T
- To reach product bulletins, field notices, and other release-specific documents, click this path:
Technical Documents: Product Bulletins
- To reach the [Caveats for Cisco IOS Release 12.2](#) and [Caveats for Cisco IOS Release 12.2 T](#) documents, which contain caveats applicable to all platforms for all maintenance releases of Release 12.2, click this path:
Technical Documents: Cisco IOS Software: Release 12.2: Caveats


Note

If you have an account with Cisco.com, you can also use the Bug Toolkit to find select caveats of any severity. To reach the Bug Toolkit, log in to Cisco.com and click **Service & Support: Technical Assistance Center: Tool Index: Bug Toolkit**. Another option is to go to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl.

Platform-Specific Documents

Cisco 1710 Routers

These documents are available for the Cisco 1720 router on CCO and the Documentation CD-ROM at **Technical Documents: Access Servers and Access Routers: Modular Access Routers: Cisco 1710 Series Routers:**

- *[Quick Start Guide for Installing Your Cisco 1710 Security Router](#)*
- *[Cisco 1710 Security Router Hardware Installation Guide](#)*
- *[Cisco 1710 Security Router Software Configuration Guide](#)*
- *[Regulatory Compliance and Safety Information for Cisco 1700 Routers](#)*

Cisco 1720 Routers

These documents are available for the Cisco 1720 router on CCO and the Documentation CD-ROM at **Technical Documents: Access Servers and Access Routers: Modular Access Routers: Cisco 1720 Series Routers:**

- *[Installing Your Cisco 1700 Router Quick Start Guide](#)*
- *[Cisco 1720 Series Router Hardware Installation Guide](#)*
- *[Cisco 1700 Series Router Software Configuration Guide](#)*
- *[Cisco 1720 Series Router Release Notes](#)*
- *[Installing and Upgrading the Boot ROM in Cisco 1720 Routers](#)*
- *[Cisco 1700 Series \(Cisco IOS\) Router Release Notes](#)*
- *[Configuration Notes for Cisco 1700 Series Routers](#)*
- *[WAN Interface Cards Hardware Installation Guide](#)*

Cisco 1750 Routers

These documents are available for the Cisco 1750 router on CCO and the Documentation CD-ROM at **Technical Documents: Access Servers and Access Routers: Modular Access Routers: Cisco 1750 Series Routers:**

- *[Installing Your Cisco 1700 Router Quick Start Guide](#)*
- *[Cisco 1750 Series Router Hardware Installation Guide](#)*
- *[Cisco 1700 Series Router Software Configuration Guide](#)*
- *[Cisco 1750 Series Router Release Notes](#)*
- *[Cisco 1750 Router Voice-over-IP quick start guide](#)*
- *[Cisco 1750 Voice-over-IP Software Configuration Guide](#)*
- *[Cisco 1700 Series \(Cisco IOS\) Router Release Notes](#)*
- *[Configuration Notes for Cisco 1700 Series Routers](#)*
- *[WAN Interface Cards Hardware Installation Guide](#)*

Cisco 1751 and 1751-V Routers

These documents are available for the Cisco 1751 and 1751-V routers on CCO and the Documentation CD-ROM at [Technical Documents: Access Servers and Access Routers: Modular Access Routers: Cisco 1751 Series Routers](#):

- [*Installing Your Cisco 1700 Router Quick Start Guide*](#)
- [*Cisco 1751 Router Hardware Installation Guide*](#)
- [*Cisco 1751 Router Software Configuration Guide*](#)
- [*Cisco 1700 Series Router Software Configuration Guide*](#)
- [*Cisco 1751 Router Hardware Release Notes*](#)
- [*Configuring the Voice Interface Card for the Cisco 1751 Router*](#)
- [*Installing and Removing Packet Voice/fax DSP Modules*](#)
- [*Cisco 1700 Series \(Cisco IOS\) Router Release Notes*](#)
- [*Configuration Notes for Cisco 1700 Series Routers*](#)
- [*WAN Interface Cards Hardware Installation Guide*](#)

Cisco 1760 and 1760-V Routers

These documents are available for the Cisco 1760 and 1760-V routers on CCO and the Documentation CD-ROM at [Technical Documents: Access Servers and Access Routers: Modular Access Routers: Cisco 1760 Series Routers](#):

- [*Quick Start Guide for Installing Your Cisco 1760 Modular Access Router*](#)
- [*Cisco 1760 Modular Access Router Hardware Installation Guide*](#)
- [*Cisco 1751 Router Software Configuration Guide*](#)
- [*Cisco 1700 Series Router Software Configuration Guide*](#)
- [*Configuration Notes for Cisco 1700 Series Routers*](#)
- [*Configuring the Voice Interface Card for the Cisco 1751 Router*](#)
- [*Installing and Removing Packet Voice/fax DSP Modules*](#)
- [*WAN Interface Cards Hardware Installation Guide*](#)

Feature Modules

Feature modules describe new features supported by Release 12.2 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 12.2 feature modules, click this path (under the heading **Service & Support**): [Technical Documents: Cisco IOS Software: Release 12.2: New Feature Documentation: New Features in 12.2-Based Limited Lifetime Releases: New Features in 12.2X Releases](#)

Feature Navigator

Feature Navigator is a web-based tool that enables you to quickly determine which Cisco IOS software images support a particular set of features and which features are supported in a particular Cisco IOS image. Feature Navigator is available 24 hours a day, 7 days a week.

To access Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, e-mail the Contact Database Administration group at cdbadmin@cisco.com. If you do not have an account on Cisco.com, go to <http://www.cisco.com/register> and follow the directions to set up an account.

To use Feature Navigator, you must have a JavaScript-enabled web browser such as Netscape 3.0 or later, or Internet Explorer 4.0 or later. Internet Explorer 4.0 always has JavaScript enabled. To enable JavaScript for Netscape 3.x or Netscape 4.x, follow the instructions provided with the web browser. For JavaScript support and enabling instructions for other browsers, check with the browser vendor.

Feature Navigator is updated when major Cisco IOS software releases and technology releases occur. You can access Feature Navigator at the following URL:

<http://www.cisco.com/go/fn>

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. The Cisco IOS software documentation set is 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 one or more configuration guides and one or more corresponding command references. Chapters in a configuration guide describe protocols, configuration tasks, and Cisco IOS software functionality, and contain comprehensive configuration examples. Chapters in a command reference provide complete command syntax information. Use each configuration guide with its corresponding command reference. The Cisco IOS software documentation set is available on Cisco.com and on the Documentation CD-ROM (under the heading **Service & Support**) at:

Technical Documents: [Cisco IOS Software: Release 12.2: Configuration Guides and Command References](#)

Release 12.2 Documentation Set

[Table 6](#) lists the contents of the Cisco IOS Release 12.2 software documentation set, which is available in both electronic and printed form (under the heading **Service & Support**) on [Cisco.com](http://www.cisco.com) and on the Documentation CD-ROM:

Technical Documents: [Cisco IOS Software: Release 12.2](#)



Note

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

Table 6 Cisco IOS Release 12.2 Documentation Set

Books	Major Topics
<i>Cisco IOS Configuration Fundamentals Configuration Guide</i> <i>Cisco IOS Configuration Fundamentals Command Reference</i>	Cisco IOS User Interfaces File Management System Management
<i>Cisco IOS Bridging and IBM Networking Configuration Guide</i> <i>Cisco IOS Bridging and IBM Networking Command Reference, Volume 1 of 2</i> <i>Cisco IOS Bridging and IBM Networking Command Reference, Volume 2 of 2</i>	Transparent Bridging SRB Token Ring Inter-Switch Link Token Ring Route Switch Module RSRB DLSw+ Serial Tunnel and Block Serial Tunnel LLC2 and SDLC IBM Network Media Translation SNA Frame Relay Access NCIA Client/Server Airline Product Set DSPU and SNA Service Point SNA Switching Services Cisco Transaction Connection Cisco Mainframe Channel Connection CLAW and TCP/IP Offload CSNA, CMPC, and CMPC+ TN3270 Server
<i>Cisco IOS Dial Technologies Configuration Guide</i> <i>Cisco IOS Dial Technologies Command Reference</i>	Preparing for Dial Access Modem and Dial Shelf Configuration and Management ISDN Configuration Signaling Configuration Dial-on-Demand Routing Configuration Dial Backup Configuration Dial Related Addressing Service Virtual Templates, Profiles, and Networks PPP Configuration Callback and Bandwidth Allocation Configuration Dial Access Specialized Features Dial Access Scenarios
<i>Cisco IOS Interface Configuration Guide</i> <i>Cisco IOS Interface Command Reference</i>	LAN Interfaces Serial Interfaces Logical Interfaces
<i>Cisco IOS IP Configuration Guide</i> <i>Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services</i> <i>Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols</i> <i>Cisco IOS IP Command Reference, Volume 3 of 3: Multicast</i>	IP Addressing and Services IP Routing Protocols IP Multicast
<i>Cisco IOS AppleTalk and Novell IPX Configuration Guide</i> <i>Cisco IOS AppleTalk and Novell IPX Command Reference</i>	AppleTalk Novell IPX

Table 6 Cisco IOS Release 12.2 Documentation Set (continued)

Books	Major Topics
• <i>Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS, and XNS Configuration Guide</i> • <i>Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS, and XNS Command Reference</i>	Apollo Domain Banyan VINES DECnet ISO CLNS XNS
• <i>Cisco IOS Voice, Video, and Fax Configuration Guide</i> • <i>Cisco IOS Voice, Video, and Fax Command Reference</i>	Voice over IP Call Control Signaling Voice over Frame Relay Voice over ATM Telephony Applications Trunk Management Fax, Video, and Modem Support
• <i>Cisco IOS Quality of Service Solutions Configuration Guide</i> • <i>Cisco IOS Quality of Service Solutions Command Reference</i>	Packet Classification Congestion Management Congestion Avoidance Policing and Shaping Signaling Link Efficiency Mechanisms
• <i>Cisco IOS Security Configuration Guide</i> • <i>Cisco IOS Security Command Reference</i>	AAA Security Services Security Server Protocols Traffic Filtering and Firewalls IP Security and Encryption Passwords and Privileges Neighbor Router Authentication IP Security Options Supported AV Pairs
• <i>Cisco IOS Switching Services Configuration Guide</i> • <i>Cisco IOS Switching Services Command Reference</i>	Cisco IOS Switching Paths NetFlow Switching Multiprotocol Label Switching Multilayer Switching Multicast Distributed Switching Virtual LANs LAN Emulation
• <i>Cisco IOS Wide-Area Networking Configuration Guide</i> • <i>Cisco IOS Wide-Area Networking Command Reference</i>	ATM Broadband Access Frame Relay SMDS X.25 and LAPB
• <i>Cisco IOS Mobile Wireless Configuration Guide</i> • <i>Cisco IOS Mobile Wireless Command Reference</i>	General Packet Radio Service

Table 6 Cisco IOS Release 12.2 Documentation Set (continued)

Books	Major Topics
• <i>Cisco IOS Terminal Services Configuration Guide</i> • <i>Cisco IOS Terminal Services Command Reference</i>	ARA LAT NASI Telnet TN3270 XRemote X.28 PAD Protocol Translation
• <i>Cisco IOS Configuration Guide Master Index</i> • <i>Cisco IOS Command Reference Master Index</i> • <i>Cisco IOS Debug Command Reference</i> • <i>Cisco IOS Software System Error Messages</i> • New Features in 12.2-Based Limited Lifetime Releases • New Features in Release 12.2 T • Release Notes (Release note and caveat documentation for 12.2-based releases and various platforms)	

Obtaining Documentation

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

World Wide Web

The most current Cisco documentation is available on the World Wide Web at <http://www.cisco.com>. Translated documentation can be accessed at http://www.cisco.com/public/countries_languages.shtml.

Documentation CD-ROM

Cisco documentation and additional literature are available in a CD-ROM package, which ships with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or as an annual subscription.

Ordering Documentation

Cisco documentation is available in the following ways:

- Registered Cisco Direct Customers can order Cisco product documentation from the Networking Products MarketPlace:
http://www.cisco.com/cgi-bin/order/order_root.pl

- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:
<http://www.cisco.com/go/subscription>
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, in North America, by calling 800 553-NETS(6387).

Documentation Feedback

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

You can e-mail your comments to bug-doc@cisco.com.

For your convenience, many documents contain a response card behind the front cover for submitting your comments by mail. Otherwise, you can mail your comments to the following address:

Cisco Systems, Inc.
Document Resource Connection
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

The following sections provide sources for obtaining technical assistance from Cisco Systems.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information and resources at anytime, from anywhere in the world. This highly integrated Internet application is a powerful, easy-to-use tool for doing business with Cisco.

Cisco.com provides a broad range of features and services to help customers and partners streamline business processes and improve productivity. Through Cisco.com, you can find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online technical support, download and test software packages, and order Cisco learning materials and merchandise. Valuable online skill assessment, training, and certification programs are also available.

Customers and partners can self-register on Cisco.com to obtain additional personalized information and services. Registered users can order products, check on the status of an order, access technical support, and view benefits specific to their relationships with Cisco.

To access Cisco.com, go to the following website:

<http://www.cisco.com>

Technical Assistance Center

The Cisco TAC website is available to all customers who need technical assistance with a Cisco product or technology that is under warranty or covered by a maintenance contract.

Contacting TAC by Using the Cisco TAC Website

If you have a priority level 3 (P3) or priority level 4 (P4) problem, contact TAC by going to the TAC website:

<http://www.cisco.com/tac>

P3 and P4 level problems are defined as follows:

- P3—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- P4—You need information or assistance on Cisco product capabilities, product installation, or basic product configuration.

In each of the above cases, use the Cisco TAC website to quickly find answers to your questions.

To register for Cisco.com, go to the following website:

<http://www.cisco.com/register/>

Cisco.com registered users who cannot resolve a technical issue by using the TAC online resource can open a case online by using the TAC Case Open tool at the following website:

<http://www.cisco.com/tac/caseopen>

Contacting TAC by Telephone

If you have a priority level 1 (P1) or priority level 2 (P2) problem, contact TAC by telephone and immediately open a case. To obtain a directory of toll-free numbers for your country, go to the following website:

<http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml>

P1 and P2 level problems are defined as follows:

- P1—Your production network is down, causing a critical impact to business operations if service is not restored quickly. No workaround is available.
- P2—Your production network is severely degraded, affecting significant aspects of your business operations. No workaround is available.

This document is to be used in conjunction with the documents listed in the [“Related Documentation” section on page 40](#).

CCIP, the Cisco *Powered* Network mark, the Cisco Systems Verified logo, Cisco Unity, Follow Me Browsing, FormShare, Internet Quotient, iQ Breakthrough, iQ Expertise, iQ FastTrack, the iQ Logo, iQ Net Readiness Scorecard, Networking Academy, ScriptShare, SMARTnet, TransPath, and Voice LAN are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, Discover All That’s Possible, The Fastest Way to Increase Your Internet Quotient, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, Fast Step, GigaStack, IOS, IP/TV, LightStream, MGX, MICA, the Networkers logo, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, SlideCast, StrataView Plus, Stratum, SwitchProbe, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0203R)

Copyright © 2000–2002, Cisco Systems, Inc.
All rights reserved.