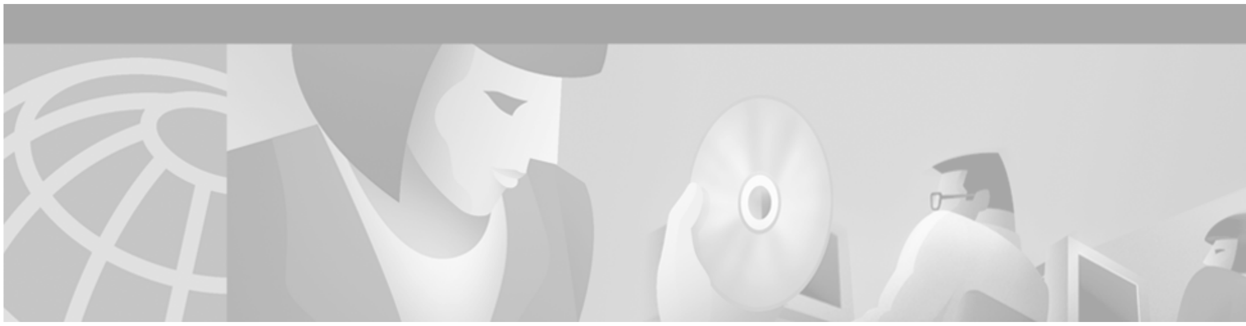

Release Notes for the Cisco 1700 Series Routers for Cisco IOS Release 12.2(8)YJ

August 12, 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(8)YJ. 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.

For a list of the software caveats that apply to Release 12.2(8)YJ, 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.

Contents

These release notes discuss the following topics:

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

System Requirements

This section describes the system requirements for Release 12.2(8)YJ and includes the following sections:

- Memory Requirements, page 2
- Hardware Supported, page 4
- Determining Your Software Release, page 4
- Upgrading to a New Software Release, page 5
- Feature Sets, page 5

Memory Requirements

This section describes the memory requirements for the Cisco IOS feature sets supported by Cisco IOS Release 12.2(8)YJ on the Cisco 1700 series routers.

Table 1 Recommended Memory for the Cisco 1700 Series Routers

Platform	Image Name	Feature Set	Image	Flash Memory	DRAM Memory
Cisco 1710 Routers	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
	Cisco 1710 IOS IP Plus FW/IDS IPSec 3DES	IP Plus FW/IDS IPSec 3DES	c1710-k9o3sy-mz	8 MB	48 MB
Cisco 1720, Cisco 1721, Cisco 1750, Cisco 1751, and Cisco 1760	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
	Cisco 1700 IOS IP Plus ADSL/IPX/ AT/IBM	IP Plus ADSL/IPX/ AT/IBM	c1700-bnr2sy7-mz	16 MB	48 MB
	Cisco 1700 IOS IP/IPX/AT/IBM	IP/IPX/AT/IBM	c1700-bnr2y-mz	8 MB	32 MB
	Cisco 1700 IOS IP Plus ADSL/FW/IDS IPSec 56	IP Plus ADSL/FW/IDS IPSec 56	c1700-k8o3sy7-mz	16 MB	48 MB
	Cisco 1700 IOS IP Plus ADSL IPSec 56	IP Plus ADSL IPSec 56	c1700-k8sy7-mz	16 MB	48 MB
	Cisco 1700 IOS IP Plus ADSL/FW/ IDS IPSec 3DES	IP Plus ADSL/FW/ IDS IPSec 3DES	c1700-k9o3sy7-mz	16 MB	48 MB
	Cisco 1700 IOS IP Plus ADSL IPSec 3DES	IP Plus ADSL IPSec 3DES	c1700-k9sy7-mz	16 MB	48 MB
	Cisco 1700 IOS IP Plus ADSL/IPX/ FW/IDS	IP Plus ADSL/IPX/ FW/IDS	c1700-no3sy7-mz	16 MB	48 MB
	Cisco 1700 IOS IP/IPX	IP/IPX	c1700-ny-mz	8 MB	32 MB
	Cisco 1700 IOS IP/FW/IDS	IP/FW/IDS	c1700-o3y-mz	8 MB	32 MB
	Cisco 1700 IOS IP Plus	IP Plus	c1700-sy-mz	16 MB	32 MB
	Cisco 1700 IOS IP Plus ADSL	IP Plus ADSL	c1700-sy7-mz	16 MB	48 MB
	Cisco 1700 IOS IP	IP	c1700-y-mz	8 MB	32 MB
	Cisco 1700 IOS IP/ADSL	IP/ADSL	c1700-y7-mz	8 MB	32 MB

Table 1 Recommended Memory for the Cisco 1700 Series Routers

Platform	Image Name	Feature Set	Image	Flash Memory	DRAM Memory
Cisco 1721, Cisco 1751, and Cisco 1760	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	64 MB
Cisco 1750, Cisco 1751, and Cisco 1760	Cisco 1700 IOS IP Plus Voice	IP Plus Voice	c1700-sv3y-mz	16 MB	48 MB
Cisco 1751 and Cisco 1760	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
	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	32 MB	64 MB
	Cisco 1700 IOS IP Plus ADSL/IPX/ AT/IBM/Voice/FW/IDS IPSec 3DES	IP Plus ADSL/IPX/ AT/IBM/Voice/FW/IDS IPSec 3DES	c1700-bk9no3r2sv3y7-mz	32 MB	64 MB
	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
	Cisco 1700 IOS IP Plus ADSL/Voice/ FW/IDS IPSec 56	IP Plus ADSL/Voice/ FW/IDS IPSec 56	c1700-k8o3sv3y7-mz	16 MB	64 MB
	Cisco 1700 IOS IP Plus ADSL/VOX/ FW/IDS IPSec 56	IP Plus ADSL/VOX/ FW/IDS IPSec 56	c1700-k8o3sv8y7-mz	16 MB	64 MB
	Cisco 1700 IOS IP Plus ADSL/Voice IPSec 56	IP Plus ADSL/Voice IPSec 56	c1700-k8sv3y7-mz	16 MB	64 MB
	Cisco 1700 IOS IP Plus ADSL/VOX IPSec 56	IP Plus ADSL/VOX IPSec 56	c1700-k8sv8y7-mz	16 MB	64 MB
	Cisco 1700 IOS IP Plus ADSL/Voice/ FW/IDS IPSec 3DES	IP Plus ADSL/Voice/ FW/IDS IPSec 3DES	c1700-k9o3sv3y7-mz	16 MB	64 MB
	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
	Cisco 1700 IOS IP Plus ADSL/Voice IPSec 3DES	IP Plus ADSL/Voice IPSec 3DES	c1700-k9sv3y7-mz	16 MB	64 MB
	Cisco 1700 IOS IP Plus ADSL/VOX IPSec 3DES	IP Plus ADSL/VOX IPSec 3DES	c1700-k9sv8y7-mz	16 MB	64 MB
	Cisco 1700 IOS IP Plus ADSL/IPX/ Voice/FW/IDS	IP Plus ADSL/IPX/ Voice/FW/IDS	c1700-no3sv3y7-mz	16 MB	64 MB
	Cisco 1700 IOS IP Plus ADSL/IPX/ VOX/FW/IDS	IP Plus ADSL/IPX/ VOX/FW/IDS	c1700-no3sv8y7-mz	16 MB	64 MB

Table 1 Recommended Memory for the Cisco 1700 Series Routers

Platform	Image Name	Feature Set	Image	Flash Memory	DRAM Memory
Cisco 1751 and Cisco 1760 (Continued)	Cisco 1700 IOS IP Plus ADSL/Voice/ FW/IDS	IP Plus ADSL/Voice/ FW/IDS	c1700-o3sv3y7-mz	16 MB	64 MB
	Cisco 1700 IOS IP Plus ADSL/VOX/ FW/IDS	IP Plus ADSL/VOX/ FW/IDS	c1700-o3sv8y7-mz	16 MB	64 MB
	Cisco 1700 IOS IP Plus ADSL/Voice	IP Plus ADSL/Voice	c1700-sv3y7-mz	16 MB	64 MB
	Cisco 1700 IOS IP Plus VOX	IP Plus VOX	c1700-sv8y-mz	16 MB	64 MB
	Cisco 1700 IOS IP Plus ADSL/VOX	IP Plus ADSL/VOX	c1700-sv8y7-mz	16 MB	64 MB

Hardware Supported

Cisco IOS Release 12.2(8)YJ supports the following Cisco 1700 series routers:

- Cisco 1710 Routers
- Cisco 1720 Routers
- Cisco 1721 Router
- Cisco 1750, 1750-2V, and 1750-4V Routers
- Cisco 1751 and 1751-V Routers
- Cisco 1760 and 1760-V Routers

The Cisco 1710, 1720, and 1721 routers run data images only. The Cisco 1750, 1750-2V, and 1750-4V routers run data or data-and-voice images, providing analog voice support. Cisco 1751, 1751-V, 1760, and 1760-V routers run data or data-and-voice images, providing digital and analog voice support.

For detailed descriptions of new hardware features and which features are supported on each router, see the "New and Changed Information" section on page 10. For descriptions of existing hardware features and supported modules, see the hardware installation guides, configuration and command reference guides, and additional documents specific to Cisco 1700 series routers, which are available on Cisco.com and the Documentation CD at the following location:
http://www.cisco.com/univercd/cc/td/doc/product/access/acs_mod/1700/index.htm

This URL is subject to change without notice. If it changes, point your web browser to CCO, and click the following path:
Cisco Product Documentation: **Access Servers and Access Routers**: **Modular Access Routers**: **Cisco 1700 Series Routers**: **<platform_name>**

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(8)YJ, EARLY DEPLOYMENT RELEASE SOFTWARE (fc1)
Synched to technology version 12.2(5.4)T
```

Upgrading to a New Software Release

For general information about upgrading to a new software release, see *Software Installation and Upgrade Procedures* located at: http://www.cisco.com/warp/public/130/upgrade_index.shtml.

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(8)YJ supports the same feature sets as Releases 12.2 and 12.2(8)T, but Release 12.2(8)YJ includes 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 6 list the features and feature sets supported in Cisco IOS Release 12.2(8)YJ:

- Table 2—Cisco 1710 routers
- Table 3—Cisco 1720, 1721, 1750, 1751, and 1760 routers
- Table 4—Cisco 1721, 1751, and 1760 routers
- Table 5—Cisco 1750, 1751, and 1760 routers
- Table 6—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(8)YJ" means the feature was introduced in 12.2(8)YJ. 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(8)*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 IPX/AT/IBM/ FW/IDS Plus IPSec 3DES	**IP Plus FW/IDS IPSec 3DES**
IP Routing			
DHCP - IP spoofing	12.2(8)YJ	Yes	Yes

Table 2 Feature List by Feature Set for Cisco 1710 Routers

Feature	In	Feature Set	
		IP IPX/AT/IBM/ FW/IDS Plus IPSec 3DES	IP Plus FW/IDS IPSec 3DES
Cisco IOS DHCP accounting	12.2(8)YJ	Yes	Yes
Security			
Easy VPN Enhancements	12.2(8)YJ	Yes	Yes
WAN Connectivity			
Cisco 1- and 2-port T1/E1 multiflex interface cards	12.2(8)YJ	No	No
Voice			
Cisco 1- and 2-port T1/E1 multiflex interface cards		No	No

Table 3 Feature List by Feature Set for Cisco 1720, 1721, 1750, 1751, and 1760 Routers, Part 1 of 2

Feature	In	Feature Set						
		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	IP Plus ADSL/FW/ IDS IPSec 3DES	IP Plus ADSL IPSec 3DES
IP Routing								
DHCP - IP spoofing	12.2(8)YJ	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Cisco IOS DHCP accounting	12.2(8)YJ	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Security								
Easy VPN Enhancements	12.2(8)YJ	Yes	No	No	Yes	Yes	Yes	Yes
WAN Connectivity								
Cisco 1- and 2-port T1/E1 multiflex interface cards[1]	12.2(8)YJ	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Voice								
Cisco 1- and 2-port T1/E1 multiflex interface cards		No	No	No	No	No	No	No

[1] WAN Connectivity through the Cisco T1/E1 multiflex interface cards is NOT supported on the Cisco 1720 or 1750 routers, but is supported on the other platforms for these images.

Table 3 Feature List by Feature Set for Cisco 1720, 1721, 1750, 1751, and 1760 Routers, Part 2 of 2

Feature	In	Feature Set						
		IP Plus ADSL/ IPX/ FW/IDS	IP/IPX	IP/FW/IDS	IP Plus	IP Plus ADSL	IP	IP/ ADSL
IP Routing								
DHCP - IP spoofing	12.2(8)YJ	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Cisco IOS DHCP accounting	12.2(8)YJ	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Security								
Easy VPN Enhancements	12.2(8)YJ	No	No	No	No	No	No	No
WAN Connectivity								
Cisco 1- and 2-port T1/E1 multiflex interface cards[1]	12.2(8)YJ	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Voice								
Cisco 1- and 2-port T1/E1 multiflex interface cards		No	No	No	No	No	No	No

[1] WAN Connectivity through the Cisco T1/E1 multiflex interface cards is NOT supported on the Cisco 1720 or 1750 routers, but is supported on the other platforms for these images.

Table 4 Feature List by Feature Set for Cisco 1721, 1751, and 1760 Routers

Feature	In	Feature Set
		IP Plus ADSL/IPX/ AT/IBM/FW/IDS IPSec 56
IP Routing		
DHCP - IP spoofing	12.2(8)YJ	Yes
Cisco IOS DHCP accounting	12.2(8)YJ	Yes
Security		
Easy VPN Enhancements	12.2(8)YJ	Yes
WAN Connectivity		
Cisco 1- and 2-port T1/E1 multiflex interface cards	12.2(8)YJ	Yes
Voice		
Cisco 1- and 2-port T1/E1 multiflex interface cards		No

Table 5 Feature List by Feature Set for Cisco 1750, 1751, and 1760 Routers

Feature	In	Feature Set
		IP Plus Voice
IP Routing		
DHCP - IP spoofing	12.2(8)YJ	Yes
Cisco IOS DHCP accounting	12.2(8)YJ	Yes
Security		
Easy VPN Enhancements	12.2(8)YJ	No
WAN Connectivity		
Cisco 1- and 2-port T1/E1 multiflex interface cards[1]	12.2(8)YJ	Yes
Voice		
Cisco 1- and 2-port T1/E1 multiflex interface cards		No

[1] WAN Connectivity through the Cisco T1/E1 multiflex interface cards is NOT supported on The Cisco 1750 router, but is supported on the other platforms for this image.

Table 6 Feature List by Feature Set for Cisco 1751 and 1760 Routers, Part 1 of 3

Feature	In	Feature Set					
		IP Plus ADSL/IPX/ AT/IBM/ Voice/FW/ IDS IPSec 56	IP Plus ADSL/ IPX/ AT/IBM/ VOX/FW/IDS IPSec 56	IP Plus ADSL/ IPX/ AT/IBM/ Voice/FW/IDS IPSec 3DES	IP Plus ADSL/ IPX/ AT/IBM/ VOX/FW/IDS IPSec 3DES	IP Plus ADSL/Voice/ FW/IDS IPSec 56	IP Plus ADSL/VOX/ FW/IDS IPSec 56
IP Routing							
DHCP - IP spoofing	12.2(8)YJ	Yes	Yes	Yes	Yes	Yes	Yes
Cisco IOS DHCP accounting	12.2(8)YJ	Yes	Yes	Yes	Yes	Yes	Yes
Security							
Easy VPN Enhancements	12.2(8)YJ	Yes	Yes	Yes	Yes	Yes	Yes
WAN Connectivity							
Cisco 1- and 2-port T1/E1 multiflex interface cards	12.2(8)YJ	Yes	Yes	Yes	Yes	Yes	Yes
Voice							
Cisco 1- and 2-port T1/E1 multiflex interface cards		No	Yes	No	Yes	No	Yes

Table 6 Feature List by Feature Set for Cisco 1751 and 1760 Routers, Part 2 of 3

Feature	In	Feature Set					
		IP Plus ADSL/Voice IPSec 56	IP Plus ADSL/VOX IPSec 56	IP Plus ADSL/Voice / FW/IDS IPSec 3DES	IP Plus ADSL/VOX/ FW/IDS IPSec 3DES	IP Plus ADSL/Voice IPSec 3DES	IP Plus ADSL/VOX/ IPSec 3DES
IP Routing							
DHCP - IP spoofing	12.2(8)YJ	Yes	Yes	Yes	Yes	Yes	Yes
Cisco IOS DHCP accounting	12.2(8)YJ	Yes	Yes	Yes	Yes	Yes	Yes
Security							
Easy VPN Enhancements	12.2(8)YJ	Yes	Yes	Yes	Yes	Yes	Yes
WAN Connectivity							
Cisco 1- and 2-port T1/E1 multiflex interface cards	12.2(8)YJ	Yes	Yes	Yes	Yes	Yes	Yes
Voice							
Cisco 1- and 2-port T1/E1 multiflex interface cards		No	Yes	No	Yes	No	Yes

Table 6 Feature List by Feature Set for Cisco 1751 and 1760 Routers, Part 3 of 3

Feature	In	Feature Set						
		IP Plus ADSL/IPX/ Voice/FW/ IDS	IP Plus ADSL/IPX/ VOX/FW/IDS	IP Plus ADSL/ Voice/ FW/IDS	IP Plus ADSL/VOX/ FW/IDS	IP Plus ADSL/ Voice	IP Plus VOX	IP Plus ADSL/ VOX
IP Routing								
DHCP - IP spoofing	12.2(8)YJ	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Cisco IOS DHCP accounting	12.2(8)YJ	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Security								
Easy VPN Enhancements	12.2(8)YJ	No	No	No	No	No	No	No
WAN Connectivity								
Cisco 1- and 2-port T1/E1 multiflex interface cards	12.2(8)YJ	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Table 6 Feature List by Feature Set for Cisco 1751 and 1760 Routers, Part 3 of 3 (continued)

Feature	In	Feature Set						
		IP Plus ADSL/IPX/ Voice/FW/ IDS	IP Plus ADSL/IPX/ VOX/FW/IDS	IP Plus ADSL/ Voice/ FW/IDS	IP Plus ADSL/VOX/ FW/IDS	IP Plus ADSL/ Voice	IP Plus VOX	IP Plus ADSL/ VOX
Voice								
Cisco 1- and 2-port T1/E1 multiflex interface cards		No	Yes	No	Yes	No	Yes	Yes

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(8)YJ.

New Hardware Features in Release 12.2(8)YJ

The following sections describe the new hardware features supported by the Cisco 1700 series routers for Release 12.2(8)YJ.

Cisco 1- and 2-Port T1/E1 Multiflex Interface Cards

Release 12.2(8)YJ introduces 1- and 2-port T1/E1 Multiflex Voice/WAN interface cards (VWICs) on Cisco 1721 routers to provide basic structured and unstructured service, two data channel groups over a single port, and TDM cross-connect link services for T1 or E1 networks on the Cisco 1721 routers. Cisco 1721 routers support 56Kbps connections for fractional and full T1/E1 services when these VWICs are installed.

The following T1/E1 VWICS are available for the Cisco 1721 routers:

- VWIC-1MFT-E1
- VWIC-2MFT-E1
- VWIC-1MFT-T1
- VWIC-2MFT-T1
- VWIC-1MFT-G703
- VWIC-2MFT-G703
- VWIC-2MFT-T1-DI
- VWIC-2MFT-E1-DI

Note Prior to Release 12.2(8)YJ, Cisco 1- and 2-port T1/E1 multiflex interface cards were supported on the Cisco 1751 and 1760 routers and on the Cisco 2600 and 3600 series routers.

Note Starting with Release 12.2(8)YJ, the Cisco 1751 and 1760 routers no longer need a voice image to support data applications on T1/E1 VWICs.

The T1 and E1 VWICs allow individual DS0s or channels of a DS1 circuit to be grouped together to create channel groups. For example, the 64kb channels of a T1 circuit could form a channel group to connect to a frame relay network. The Cisco 1721 router supports up to two data channel groups over a single port.

Drop and Insert (DI) VWICs have two T1/E1 ports. In addition to the functionality described above, the DI VWICs enable specified TDM DS0 channels from one port to be directly cross-connected to another port within the same slot. For example, the first three DS0s of one port can be directly cross-connected to the first three DS0s of a second port. The remaining DS0s can group together as a channel group to or from other interfaces on the router. DI VWICs provide easy multiplexing of TDM voice and data over a single circuit, within two locals ports of a T1/E1 DI VWIC.

The G.703 VWICs support unframed and framed E1 circuits.

New Software Features in Release 12.2(8)YJ

The following sections describe the new software features supported by the Cisco 1700 series routers for Release 12.2(8)YJ.

Cisco Easy VPN Client

Cable modems, xDSL routers, and other forms of broadband access provide high-performance connections to the Internet, but many applications also require the security of VPN connections that perform a high level of authentication and that encrypt the data between two particular endpoints. However, establishing a VPN connection between two routers can be complicated, and typically requires tedious coordination between network administrators to configure the VPN parameters for the two routers.

The Cisco Easy VPN Client feature eliminates much of this tedious work by implementing the Cisco Unity Client protocol, which allows most VPN parameters to be defined at a VPN remote access server. This server can be a dedicated VPN device such as a VPN 3000 concentrator or a Cisco PIX Firewall, or a Cisco IOS router that supports the Cisco Unity Client protocol.

After the VPN remote access server has been configured, a VPN connection can be created with minimal configuration on an IPSec client, such as the Cisco 806, 826, 827, and 828 routers and the Cisco 1700 series routers. When the IPSec client then initiates the VPN tunnel connection, the VPN remote access server pushes the IPSec policies to the IPSec client and creates the corresponding VPN tunnel connection.

Note Release 12.2(8)YJ is the first release to support both Easy VPN server and client functionality in the Cisco 1700 IOS images.

The Cisco Easy VPN Client feature provides for automatic management of the following details:

- Negotiating tunnel parameters—Addresses, algorithms, lifetime, and so on.
- Establishing tunnels according to the parameters.
- Automatically creating the NAT and PAT translation and associated access lists that are needed, if any.

- Authenticating users—Making sure users are who they say they are, by way of usernames, group names and passwords.
- Managing security keys for encryption and decryption.
- Authenticating, encrypting, and decrypting data through the tunnel.

Release 12.2(8)YJ provides functionality for a Cisco 1700 series router to simultaneously act as a Cisco Easy VPN client and as a VPN server (supporting VPN remote office extensions, such as a Unity server) for Cisco VPN software clients.

Release 12.2(8)YJ provides functionality for a Cisco 1700 series router to simultaneously act as a Cisco Easy VPN client and as a VPN server (supporting VPN remote office extensions, such as a unity server) for Cisco VPN software clients.

Release 12.2(8)YJ also supports the following IP Security functionality:

- ACL Firewall interoperability with Easy VPN (CSCdx23393)
- Configurable inside interface support (CSCdw15005)
- DHCP server enhancements/DNS proxy (CSCdw14394)
- Multiple WAN interface support (CSCdx23393)
- NAT configuration restoration (CSCdw03052)
- Peer hostname enhancements (CSCdx23393)

This functionality is supported in the images: IP Plus ADSL IPSec 3DES, IP Plus ADSL/FW/IDS IPSec 3DES, and IP Plus ADSL/IPX/AT/IBM/FW/IDS IPSec 3DES. For more information, see the "Resolved Caveats - Release 12.2(8)YJ" section on page 20 or the specific "Important Notes" sections listed above. The related caveat numbers are provided in the parenthesis above.

The following sections and the section Resolved Caveats - Release 12.2(8)YJ describe the feature enhancements for Cisco Easy VPN Client that are supported in Release 12.2(8)YJ:

- Manual Tunnel Control Enhancement
- Multiple Inside Interface Enhancements

Manual Tunnel Control Enhancement

In the initial release of the Cisco Easy VPN feature, the IPSec Virtual Private Network (VPN) tunnel is automatically connected when the Easy VPN Client is configured on an interface. If the tunnel times out or fails, the tunnel automatically reconnects and retries indefinitely.

The Cisco Easy VPN Client Phase II release adds support for manual control of the IPSec VPN tunnels, so that you can establish and terminate the IPSec VPN tunnel on demand. Manual tunnel control is enabled or disabled using the following command in Cisco Easy VPN Client configuration mode:

```
router(config-crypto-ezvpn)# connect [auto | manual]
```

The **auto** setting is the default setting and matches the functionality of the initial release of the Cisco Easy VPN Client feature. You do not need to use the **connect** command if you want to retain the automatic configuration.

To enable manual tunnel control, use the **connect manual** command in Cisco Easy VPN Client configuration mode:

```
router# config t
router(config)# crypto ipsec client ezvpn telecommuter-client
router(config-crypto-ezvpn)# connect manual
router(config-crypto-ezvpn)#
```

When you have configured a client configuration for manual control, the router does not establish the IPSec VPN connection until you give the **crypto ipsec client ezvpn connect** command in Privileged EXEC mode.

```
    router# crypto ipsec client ezvpn connect <name>
```

Note If the tunnel times out or fails, you must also use the **crypto ipsec client ezvpn connect** command to reestablish the connection.

You can also use the **clear crypto ipsec client ezvpn** command to manually disconnect a specific tunnel.

```
    router# clear crypto ipsec client ezvpn [<name>]
```

Multiple Inside Interface Enhancements

Easy VPN supports only one inside interface, which defaults to Fast Ethernet on 1700 series routers and to Ethernet on Cisco 800 series routers, in releases prior to Release 12.2(8)YJ. However, multiple inside interfaces are supported in Release 12.2(8)YJ, which can be configured using the following commands:

```
router> interface interface-name
router> crypto ipsec client Easy VPN name [[outside] | inside]
```

DHCP - IP Spoofing

This feature addresses the requirements of Wireless LAN customers to avoid IP spoofing. This feature for the IOS DHCP server keeps its database in sync with the ARP table so that IP spoofing can be avoided.

The Cisco IOS DHCP server adds an ARP entry to the ARP table for a client when an address is allocated that can only be deleted by the Cisco IOS DHCP server when a binding expires. The ARP entry created by the DHCP server should not be overwritten by any unsolicited ARP requests.

Cisco IOS DHCP Accounting

This feature addresses the requirements of clients in a Public Wireless LAN (PWLAN) access network. This feature adds the capability to send an accounting start when an address is allocated for a client and an accounting stop when a DHCP lease is terminated. The server receiving the Accounting Start and Stop messages can then act on the notification for accounting purposes. For example, an accounting session can be started when the Accounting Start or Stop is received or the accounting session can be cleaned up for the particular DHCP client upon lease termination.

New Software Features in Release 12.2(8)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

Cisco 1- and 2-Port T1/E1 Multiflex Interface Card Channel Group Assignments

A maximum of 2 channel-groups can be configured on each Cisco 1- and 2-port T1/E1 multiflex interface card. A system administrator can assign one channel group to each port or both channel-groups to a single port, leaving the other port unassigned.

Maximum Number of Store and Forward Fax Calls

The Cisco 1751 router supports 30 voice calls and the Cisco 1760 router supports 48 voice calls. However, these routers might not be able support more than 10 store and forward fax calls due to memory constraints.

Unsupported Features

Release 12.2(8)YJ does not support the following features. (Also, see the "Caveats" section on page 16.)

- Global system for mobile communication over frame relay (GSM-FR).
- Establishing Easy VPN tunnels over sub-interfaces.
- Dedicated inside and outside interfaces: Every interface used for establishing Easy VPN tunnels has to be either an inside interface or an outside interface but not both. The roles of an interface cannot overlap.

Additional Restriction Information

See the following Cisco IOS release notes for further information regarding limitations and restrictions:

- *Release Notes for the Cisco 1700 Series Routers for Cisco IOS Release 12.2(4)YB*
- *Release Notes for the Cisco 1700 Series Routers for Cisco IOS Release 12.2(4)XM*
- *Release Notes for the Cisco 1700 Series Routers for Cisco IOS Release 12.2(4)XW*
- *Release Notes for the Cisco 1700 Series Routers for Cisco IOS Release 12.2(2)XT*
- *Release Notes for the Cisco 1700 Series Routers for Cisco IOS Release 12.2(2)XH*

Important Notes

The following sections contain important notes about Cisco IOS Release 12.2(8)YJ that can apply to the Cisco 1700 series routers. (Also, see the "Caveats" section on page 16.)

Cisco Easy VPN Enhancements

Any changes to an active Cisco Easy VPN Client configuration or IP address changes to the involved interfaces, such as adding or removing an inside interface, result in a reset of the Cisco Easy VPN Client connection.

On the Cisco 1700 series routers, if you have an existing Cisco Easy VPN Phase I configuration and then upgrade to the Cisco Easy VPN Client Phase II image, you must configure the inside interfaces because there is no longer a default inside interface.

Cisco Easy VPN Client Phase II supports Cisco PIX Firewall Version 6.2. Refer to *Cisco PIX Firewall and VPN Configuration Guide Version 6.2*.

When you manually connect a tunnel, if the tunnel name is not specified, the active tunnel is connected. If there is more than one active tunnel, the command fails with an error requesting that you specify the tunnel name.

When you have configured the Cisco Easy VPN Server configuration on the VPN 3000 Concentrator to use hostname as its identity, then you must configure the peer on the Cisco Easy VPN Client using hostname. You can either configure DNS on the client to resolve the peer hostname, or you can configure the peer hostname locally on the client using the **ip host** *peer_hostname ip_address* command. As an example, you can configure the peer hostname locally on an Easy VPN Client with the **ip host** *crypto-gw.cisco.com 10.0.0.1* command. Or you can configure the Easy VPN Client to use the hostname with the **peer** *hostname* command, such as **peer** *crypto-gw.cisco.com*.

T1/E1 VWIC Support on Cisco 1751 and 1760 Routers

Starting with Release 12.2(8)YJ, the Cisco 1751 and 1760 routers no longer need a voice image to support data applications on T1/E1 VWICs.

Fan Operation in Cisco 1700 Series Routers

Cisco 1760 and 1760-V router fans are always on and Cisco 1710 routers do not contain a fan. However, the fans in Cisco 1720, 1721, 1750, and 1751 routers stay off until thermally activated.

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.

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:**.)

Using Dialer Interface with MLPPPoATM

This feature is not supported on the Cisco 1700 series platforms. Please use the Virtual Template interface instead.

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.

Caveats in Release 12.2 T are also in Release 12.2(8)YJ. 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.

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 toCisco.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.

Open Caveats - Release 12.2(8)YJ

This section describes unexpected behavior in Release 12.2(8)YJ.

Miscellaneous

CSCin09150

SSG VoiceStream:Unable to send Interim Host acct records when service acct disabled

CSCin09177

SSG Voicestream:Unable to disable accounting for a particular service

CSCin09186

SSG VoiceStream:SSG turns off connection acct for a service on relogin.

CSCin09188

SSG VoiceStream:show ssg service displays acct disabled when L attr has 0 acct interval.

CSCin09241

The “IPV4_ADDR” identity only is supported.

CSCin09442

SSG VoiceStream:Spurious memory access in downloading service profile.

CSCin09456

SSG VoiceStream:SSG rejects L attribute for non-integer acct interval.

CSCin09555

SSG VoiceStream:Not enabling acct for 2nd time service login.

CSCin09598

SSG VoiceStream:Acct Stop packet contains stale entries for tx/rx pa

CSCin09602

SSG VoiceStream:sh ssg attr 44 CLI does not get saved in NVRAM

CSCdw25878

When using SIP, the URL name in the terminating message is not the same as the URL name in the originating message. An IP address shows up instead.

CSCdw30639

A tunnel comes up when the concentrator is not reachable through the tunnel interface.

CSCdw67404

Should send “ike” cookies when forwarding an “xauth” request to Easy VPN.

CSCdw92918

Using “bvi/irb/network-extension mode”, unable to ping server.

CSCdx09694

Bridging fails with dialer profile configuration and HDLC encapsulation on BRI interfaces. The workaround is to use other encapsulations, such as PPP or LAPB.

CSCdx28612

Secure ARP entry is added to a BOOTP client

CSCdx29007

Secure ARP entries are not restored after the server reloaded

CSCdx31992

Loopback remote v54 feature does not work when connecting a Cisco 1721 router back-to-back with a Cisco 1751, 1760, or 3600 series router. To work around this problem, use a Cisco 2600 router to connect back-to-back with the Cisco 1721 router.

CSCdx36668

Virtual access interfaces are created without any dialer or virtual templates configuration binding to ATM or ISDN interfaces. Even with all physical interfaces sown, and without any ATM or ISDN interfaces, virtual access interfaces get created and remain in the UP state. This has been observed on Cisco 1721, 1751 and 7200 routers. For example:

```
Router# sh ip int brief
Interface         IP-Address   OK?    Method   Status                  Protocol
FastEthernet0/0   unassigned   YES    unset    administratively down   down
Ethernet0/0       unassigned   YES    unset    administratively down   down
Virtual-Access1   unassigned   YES    unset    up                      up
```

Even though the virtual access interface is created, it does not affect the router in any way.

CSCdx41557

E&M ports sometimes get stuck in the “S_WAIT_RELEASE” VTSP state while in use. This is seen with Type 2, 4-wire connections. To work around this problem, issue **shut** and **no shut** commands on the voice interface several times. If this does not work, reload the router.

CSCdx47760

If an IP Address is acquired through DHCP and the interface is subsequently shut down, theIP address is not assigned to the Fast Ethernet interface after you enter the following command for the interface: **ip address** *a.b.c.d mask*. This occurs on all 1700 platforms. To work around this problem, follow these steps:

1. Under the Fast Ethernet interface, enter the command **ip address** *a.b.c.d mask*.
2. Enter the command **no shut**.
3. Enter enable mode and enter the command **write memory**.
4. Reload the router.

CSCdx50070

The serial interface for the cards VWIC-2MFT-T1/E1-DI and VWIC-2MFT-G703 can not come up after a reload when switching between data only and voice supported images and vice versa. This issue applies to the Cisco 1721, 1751, and 1760 routers. To work around this problem, power cycle the router after every switch from a data-only image to a voice-supported image and vice versa.

CSCdx51968

Doing no service dhcp did not remove the secure ARP entry

CSCdx61109

Fax transmission is not successful for SIP when using T.38 for the fax relay. To work around this problem, use the proprietary method instead of T.38.

CSCdx62600

Voice calls are dropped for the E1 R2 feature on Cisco 1751 and Cisco 1760 routers when inter-register signaling “semi-compelled” is configured. This happens with all line signaling: digital, pulse and analog.

CSCdx64053

Spurious access at “crypto_ikmp_config_send_reply_addr” on the server.

CSCdx64872

The command line interface for Easy VPN is not forward compatible from Release 12.2(4)YB to upgrade the image to BL4A.

CSCdx64884

The Easy VPN feature is not supported with sub-interfaces.

CSCdx64971

IPSec does not work when **set pfs group#**, for any group number is part of the configuration. To work around this problem, remove **set pfs group#** from the configuration.

CSCdx67758

DTMF relay fails when an IVR application is configured under dial-peer. This has been observed for all dtmf relay types: cisco rtp, h245-alphanumeric, and h245-signal. To work around this problem, remove the IVR application’s configuration under the dial-peer.

CSCdx71669

When running MLPPP/LFI over ATM , the ping (packet transmission) between the routers fails.

CSCdx90524

Memory leak in dialer_release when no **dialer in-band** command is issued.

Resolved Caveats - Release 12.2(8)YJ

This section describes unexpected behavior that is fixed in Release 12.2(8)YJ.

Miscellaneous

CSCdv89988

Manual tunnel control.

CSCdv90114

The tunnel is “stuck” with minimum timers and traffic after one day.

CSCdw03052

When an Easy VPN tunnel is down, users lose Internet connectivity. Release 12.2(8)YJ prevents this loss of Internet connectivity by saving any existing Internet Access NAT configurations during tunnel creation and then restoring them when the tunnel goes down.

CSCdw12739

Telnet console supported for “xauth” prompting.

CSCdw14371

Show technical support for the Easy VPN feature.

CSCdw14394

Previously, Cisco IOS software performed the prepending and selective deletion of imported attributes so that DNS and WINS attributes could be set up correctly in the DHCP Server, regardless of whether a tunnel was up or down. The router now acts as a Proxy DNS server. Therefore, when a tunnel is down, use your Internet Service Provider (ISP) domain name system (DNS) to resolve DNS requests and when a tunnel is up, use your site DNS to resolve DNS requests.

When the router now acts as a Proxy DNS server, the router receives DNS queries on behalf of the real DNS servers and proxy for the users connected to the LAN. This functionality enables the DHCP server to immediately send out its LAN address as the DNS server IP address. The router forwards DNS queries from local users to real DNS servers after the WAN connection comes up and caches the DNS records supplied with the answers from the real DNS servers.

CSCdw15005

Currently the Easy VPN feature assumes that the remote network resides on fast ethernet 0 interface. Since 1700 platform has many different wics, this is a big restriction for customers. This feature adds a command which allows the network administrator to specify, which interfaces will have remote users when they configure the Easy VPN profile.

CSCdw20209

PIX interoperability problems.

CSCdw21149

Secure ID authentication causes the router to unexpectedly reset.

CSCdw24510

The command **no shut** on the dialer interface is not recognized by the Easy VPN state machine.

CSCdw34902

Memory leak in “crypto_isakmp_init_phase1_fields” and “crypto_ss_c.”

CSCdw36857

Dialer interface issues with tunnel up and down messages.

CSCdx39297

NAT unexpectedly causes the router to reset when using “ipnat_verify_timeout”. This is a “mgd_timer” issue.

CSCdw40136

Add support for the “MODECFG_DEFDOMAIN” attribute.

CSCdw48809

The router cannot accept DHCP.

CSCdw52815

The router unexpectedly resets from “reg_invoke_crypto_remove_transform_from_list()”.

CSCdw52595

Memory leak in “mtree_create_les”.

CSCdw54053

The peer in an Easy VPN configuration can be specified as a dotted decimal IP address or as a hostname. If you specify a hostname, a DNS lookup is performed immediately and the IP address is internally set. However, if the DNS entry changes, implementations previous to Release 12.2(8)YJ are not flexible enough to support the change. A feature included in Release 12.2(8)YJ supports the change by storing the text string of the hostname and using this information to perform a DNS lookup at the time a tunnel connection is made.

CSCdw68648

The router unexpectedly resets from “ike_fsm_config_mode_process_reply.”

CSCdx07519

Needs to allow concentrator dictate IKE&IPSEC lifetime.

CSCdx20031

Possible memory leak in “ezvpn_msg_pool”.

CSCdx21922

Issue regarding the “show encryption IPSec client Easy VPN” privileged level.

CSCdx23134

In previous releases of Easy VPN, problems occur when connecting Easy VPN to PIX firewall.
IP security associations fail to come up between an Easy VPN client and the PIX firewall and when Easy VPN sends a mode configuration request to PIX, the PIX does not send back a mode configuration reply. This problem is fixed in Release 12.2(8)YJ.

CSCdx23393

Release 12.2(8)YJ supports multiple WAN interfaces on Cisco 1700 series routers for Easy VPN Remote tunnels.

CSCdx35553

An “ezvpn_logic_error” occurs when trying to reconnect.

CSCdx36141

Cannot turn on Easy VPN debug.

CSCdx37283

The default inside interface Easy VPN status is not displayed when it is not active.

CSCdx57737

Exec commands should be backward-compatible with phase 1.

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.

Use these release notes with the documents listed in the following sections:

- Release-Specific Documents
- Platform-Specific Documents

Release-Specific Documents

The following documents are specific to Release 12.2 and apply to Release 12.2(8)YJ. They are located on Cisco.com and the Documentation CD (under the heading **Service & Support**):

- To reach the *Release Notes for the Cisco 1700 Series Routers for Cisco IOS Release 12.2(8)YJ*, 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(8)YJ**

- 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 toCisco.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

Hardware installation guides, configuration and command reference guides, and additional documents specific to Cisco 1700 series routers are available on Cisco.com and the Documentation CD at the following location:

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_mod/1700/index.htm

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

Cisco Product Documentation: **Access Servers and Access Routers**: **Modular Access Routers**: **Cisco 1700 Series Routers**: **<platform_name>**

Obtaining Documentation and Technical Assistance

The *Cross-Platform Release Notes for Cisco IOS Release 12.2 T* contains the latest descriptions and locations of the following sources for obtaining documentation and technical assistance from Cisco Systems. See the section "Release-Specific Documents" for the location of the *Cross-Platform Release Notes for Cisco IOS Release 12.2 T*.

- World Wide Web, Cisco.com—Cisco Systems website: http://www.cisco.com.
- Documentation CD—Cisco documentation and additional literature are available in a CD package, which ships with your product.

- Ordering documentation—Methods for ordering documentation include Networking Products MarketPlace, the online Subscription Store, and calling a local account representative using the Cisco corporate headquarters or North America phone numbers.
- Documentation feedback—When using the World Wide Web, you can submit technical comments electronically. You can also send e-mail, mail in the response card that is behind the front cover of many documents, or send correspondence to Cisco Systems. We appreciate your comments.
- Technical Assistance Center (TAC)—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. You can contact the TAC using Cisco.com or by phone. Toll-free numbers are available for many countries.

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