Release Notes for Cisco uBR905 and Cisco uBR925 Cable Access Routers for Cisco IOS Release 12.2 YJ

June 24, 2002
Cisco IOS Release 12.2(8)YJ
OL-2815-01

Note You can find the most current Cisco IOS documentation on Cisco.com. These electronic documents may contain updates and modifications made after this document was published.

These release notes for the Cisco uBR905 and Cisco uBR925 cable access routers describe the enhancements provided in Cisco IOS Release 12.2(8)YJ. These release notes are updated as needed to describe new features, memory requirements, hardware support, software platform deferrals, and changes to the microcode or modem code and related documents.

Cisco IOS Release 12.2(8)YJ is based on Cisco IOS Release 12.2(8)T and is the upgrade path for Cisco IOS Release 12.2(4)YA2, which provided the initial release for the Cisco Easy VPN Remote Phase I feature. Release 12.2(8)YJ provides bug fixes and feature enhancements for the Cisco Easy VPN Remote Phase II feature, which is the next phase of the Cisco Easy VPN Remote feature.

For a list of software caveats that apply to Release 12.2(8)YJ, see the "Caveats" section on page 28 and *Caveats for Cisco IOS Release 12.2 T.* The caveats document is updated for every maintenance release and is located on Cisco.com and the Documentation CD-ROM.

Use these release notes with *Cross-Platform Release Notes for Cisco IOS Release 12.2* located on Cisco.com and the Documentation CD-ROM. For complete documentation on the Cisco uBR905 and Cisco uBR925 cable access routers, see the documentation listed in the "Related Documentation" section on page 30.

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

Contents

These release notes describe the following topics:

Introduction

The DOCSIS-based Cisco uBR905 and Cisco uBR925 cable access routers give small office, home office (SOHO) and branch office subscribers high-speed Internet or intranet access.The Cisco uBR905 and Cisco uBR925 cable access routers act as cable modems to connect computers and other customer premises devices at a subscriber site to the service provider cable, hybrid fiber-coaxial (HFC), and IP backbone network.

The Cisco uBR905 cable access router supports data traffic via a shared two-way cable system and IP backbone network. The Cisco uBR925 cable access router supports both data and Voice over IP (VoIP) traffic via a shared two-way cable system and IP backbone network.

Both cable access router models support four Ethernet hub ports to connect to PCs and other customer premises equipment (CPE) devices. The Cisco uBR925 cable access router also supports connecting one PC or CPE device through a Universal Serial Bus (USB) port.

The Cisco uBR905 and Cisco uBR925 cable access routers are based on Data-over-Cable Service Interface Specifications (DOCSIS) and interoperates with any bidirectional, DOCSIS-qualified cable modem termination system (CMTS). These cable access routers ship from the Cisco factory with a Cisco IOS software image stored in nonvolatile Flash memory that supports DOCSIS-compliant bridging data operations.

Based on the feature licenses your company purchased, other Cisco IOS images can be downloaded from Cisco.com. Special operating modes, based on your service offering and the practices in place for your network, can be supported for the Cisco uBR905 and Cisco uBR925 cable access routers, based on the available images in Cisco IOS Release 12.2(8)YJ. Both the Cisco uBR905 and Cisco uBR925 cable access routers can also function as an advanced router, providing WAN data connectivity in a variety of configurations.

Note In previous Cisco IOS releases, the Cisco uBR905 and Cisco uBR925 cable access routers used the same software images. In Cisco IOS Release 12.2(8)YJ, however, the Cisco uBR905 cable access router must use the non-voice image (ubr925-k9o3sy5-mz) due to memory requirements.

Cisco uBR905 Cable Access Router

The Cisco uBR905 cable access router features a single F-connector interface to the cable system, four RJ-45 (10BASE-T Ethernet) hub ports to connect to a local PC or LAN, and one RJ-45 console port to connect to a laptop computer/console terminal for local Cisco IOS configuration. The Cisco uBR905 router also provides an onboard IPSec hardware accelerator, which provides high-performance encryption that is substantially faster than software-based encryption.

Cisco uBR925 Cable Access Router

The Cisco uBR925 cable access router features a single F-connector interface to the cable system, four RJ-45 (10BASE-T Ethernet) hub ports to connect to a local PC or LAN, one Universal Serial Bus (USB) port to connect to a local PC, and one RJ-45 console port to connect to a laptop computer/console terminal for local Cisco IOS configuration. The Cisco uBR925 router also provides two RJ-11 voice ports to connect to FXS telephone devices for VoIP support. The Cisco uBR925 router also provides an onboard IPSec hardware accelerator, which provides high-performance encryption that is substantially faster than software-based encryption.

Early Deployment Releases

These release notes describe the Cisco uBR905 and Cisco uBR925 cable access routers for Cisco IOS Release 12.2(8)YJ, which is an early deployment (ED) release based on Cisco IOS Release 12.2 T, and is the upgrade path for Cisco IOS Release 12.2(4)YA2. Early deployment releases contain fixes for software caveats and support for new Cisco hardware and software features.

Table 1 shows the 12.2 YA and 12.2 YJ early deployment release for both the Cisco uBR905 and Cisco uBR925 cable access routers.

Table 1 Early Deployment Releases for the Cisco uBR905 and Cisco uBR925 Cable Access Routers

ED Release	Additional Software Features	Availability
12.2(8)YJ	The Cisco Easy VPN Remote Phase II feature, which includes the following subfeatures: • Manual Tunnel Control • Multiple Inside Interface Enhancements • Multiple Outside Interfaces Support • NAT Interoperability Support • Local Address Support for Cisco Easy VPN Remote Phase II • Cable DHCP Proxy Enhancement • Peer Hostname Enhancement • Proxy DNS Server Support • PIX Interoperability Support • Cisco IOS Firewall Support • Simultaneous Easy VPN Remote and Server Support • Cisco Easy VPN Remote Web Manager	Now
12.2(4)YA2	None	—

Table 1 Early Deployment Releases for the Cisco uBR905 and Cisco uBR925 Cable Access Routers (continued)

ED Release	Additional Software Features	Availability
12.2(4)YA1	None	—

Table 1 Early Deployment Releases for the Cisco uBR905 and Cisco uBR925 Cable Access Routers (continued)

ED Release	Additional Software Features	Availability
12.2(4)YA	The following feature is new for Cisco IOS Release 12.2(4)YA: • Cisco Easy VPN Remote feature support The following features were inherited from the parent train, Cisco IOS Release 12.2(4)T: • Cable-Modem VoIP Clock-Internal Command • Cable Monitor Web Diagnostics Tool • Cisco Firewall (Phases I and II)—Cisco IOS Firewall Software • Cisco Secure Intrusion Detection System (IDS) (formerly known as NetRanger) support • DF Bit Override Functionality with IPSec Tunnels • DOCSIS 1.0+ Extensions—Dynamic Multi-SID[1] Assignment and Concatenation • DOCSIS Baseline Privacy Interface (BPI) • Dynamic Host Configuration Protocol (DHCP) Proxy Support • Easy IP—DHCP Server and Network address translation and port address translation (NAT/PAT) • Enhanced bridging functionality • Full and DOCSIS-compliant bridging • H.323v2 Protocol[2] • H.323 Version 2 Phase 2 Gateway Features, which include: – H.323v2 Fast Connect – H.245 Tunneling of DTMF Relay in conjunction with Fast Connect – H.450.2 Call Transfer – H.450.3 Call Deflection – H.235 Security – Translation of FXS Hookflash Relay • H.323 Call Redirection Enhancements • HSRP[3] Support for ICMP[4] Redirect • Interface Index Display and Interface Alias Long Name Support for SNMP • IPSec—56-bit encryption/decryption at network layer (Phase I) • IPSec 3DES—Triple DES[5] (Phase I): 168-bit encryption/decryption at network layer (Phase I) • IPSec Hardware Accelerator—onboard encryption hardware accelerator is automatically used by default for all IPSec encryption • IP Address DOCSIS Command • L2TP—Layer 2 tunneling protocol (Phase I) • MGCP Including NCS • NAT—Support for NetMeeting Directory (Internet Locator Service—ILS) • NAT Support of H.323 RAS	Now

Table 1 Early Deployment Releases for the Cisco uBR905 and Cisco uBR925 Cable Access Routers (continued)

ED Release	Additional Software Features	Availability
12.2(4)YA (continued)	• Radio frequency interface • RFC 2233 support for link up/down traps and for the IF-MIB MIB[6] • RFC 2669 and RFC 2670 Support • Routing (RIP V2) • Secure Shell (SSH) Version 1 Client and Server Support • Support for the [**no**] **cable-modem qos drop-ack** command • VPN[7] Enhancements—Dynamic Crypto Map	Now

1. SID = Service ID
2. VoIP and USB support exist only when the Cisco IOS Release 12.2(4)YA image is loaded on the Cisco uBR925 cable access router. The Cisco uBR905 cable access router does not support either VoIP traffic or the USB interface.
3. HSRP = Hot-Standby Routing Protocol
4. ICMP = Internet Control Message Protocol
5. DES = Data Encryption Standard
6. MIB = Management Information Base
7. VPN = Virtual Private Network

System Requirements

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

Memory Recommendations

Table 2 lists the minimum memory recommendations for Cisco IOS Release 12.2(8)YJ for the Cisco uBR905 cable access router.

Table 2 Cisco IOS Release 12.2(8)YJ Memory Recommendations for the Cisco uBR905 Cable Access Router

Feature Set	Image Name	Recommended Flash Memory	Recommended DRAM Memory	Runs from
Performance Small Office/FW/IPSec 3DES	ubr925-k9o3sy5-mz	8 MB	24 MB	RAM

Table 3 lists the minimum memory recommendations for Cisco IOS Release 12.2(8)YJ for the Cisco uBR925 cable access router.

Table 3 Cisco IOS Release 12.2(8)YJ Memory Recommendations for the Cisco uBR925 Cable Access Router

Feature Set	Image Name	Recommended Flash Memory	Recommended DRAM Memory	Runs from
Performance Small Office/Voice/FW/IPSec 3DES	ubr925-k9o3sv4y5-mz	8 MB	32 MB	RAM

Note In previous Cisco IOS releases, the Cisco uBR905 and Cisco uBR925 cable access routers used the same software images. In Cisco IOS Release 12.2(8)YJ, however, the Cisco uBR905 cable access router must use the non-voice image (ubr925-k9o3sy5-mz) due to memory requirements.

Headend Interoperability

DOCSIS Concatenation

If DOCSIS concatenation with a 16-QAM (quadrature amplitude modulation) symbol rate is used, the CMTS must be configured for Unique Word 16 in the preamble for both short and long data burst profiles. On Cisco CMTS universal broadband routers, use the cable modulation-profile global configuration command and specify **uw16** for both the long and short modulation profiles.

DOCSIS 1.0+ Extensions

Cisco IOS Release 12.2(8)YJ images support the Cisco DOCSIS 1.0+ Extensions, which include dynamic multi-SID assignment and concatenation. To use the dynamic multi-SID and concatenation features, the Cisco uBR905 and Cisco uBR925 cable access routers and the CMTS router must support them. If you are using a Cisco CMTS router as the headend equipment, Cisco IOS Release 12.1(1)T or a later release is required on the Cisco CMTS router to ensure that these features are activated.

To configure the Cisco uBR905 and Cisco uBR925 cable access routers to support multiple classes of service, use either the Cisco Subscriber Registration Center (CSRC) tool or the configuration file editor of your choice. DOCSIS configuration files can contain multiple classes of service (CoS) to support voice and other real-time traffic. The first CoS is used for data (and voice if no other CoS is defined), and up to three additional classes of service can be defined to give higher priority for voice and other real-time traffic.

IPSec Encryption Support

To use IPSec encryption with the Cisco uBR905 and Cisco uBR925 cable access routers, the destination endpoint must also support IPSec encryption and be configured for the same encryption policy. The endpoint is typically an IPSec server such as a peer router, Cisco PIX Firewall, or other device that can be configured for IPSec. (The CMTS does not need to support IPSec encryption unless it is desired that the CMTS act as an IPSec server.)

In Cisco IOS Release 12.2(8)YJ, IPSec encryption support is enhanced with the Cisco Easy VPN Remote Phase II feature, which simplifies the IPSec configuration on the client router. Most of the IPSec configuration is done on the IPSec server, with a minimal configuration on the IPSec client.

The Cisco Easy VPN Remote Phase II feature requires that the IPSec server support the Cisco Unity Client protocol. The server could be a VPN 3000 series concentrator, or it could be a Cisco router that supports the VPN Remote Access feature, which is available for selected platforms in Cisco IOS Release 12.2(8)T and later T releases.

When the Cisco Easy VPN Remote Phase II feature is enabled, the IPSec client initiates the VPN tunnel connection, and the IPSec server responds by transmitting the IPSec policies to the client and then creating the corresponding VPN tunnel connection. See the "Cisco Easy VPN Remote Feature" section on page 17 for more information.

Note The IPSec feature set encrypts traffic sent between endpoints, such as between two Cisco uBR905 cable access routers, to protect traffic sent across the Internet and other unprotected networks. The DOCSIS BPI feature encrypts traffic on the cable interface between the cable access router and the CMTS. To use BPI encryption, the cable access router and the CMTS must support and enable BPI encryption.

Hardware Supported

The Cisco uBR905 cable access router contains the following interfaces:

- A single F-connector interface to the cable system.
- Four RJ-45 (10BASE-T Ethernet) hub ports to connect:
  - Up to three computers directly to the four Ethernet hub ports at the rear of the Cisco uBR905 router when operating in bridging mode. When operating in routing mode, all four Ethernet hub ports can be connected directly to four computers.
  - One of the four Ethernet hub ports at the rear of the Cisco uBR905 router can be connected to an Ethernet hub, which then connects additional computers or devices at the site when operating in routing or bridging mode.
- One RJ-45 console port (optional) to connect to a laptop computer or console terminal when locally configuring the Cisco uBR905 router; the router ships from the Cisco factory with the console port enabled.
- The onboard hardware accelerator for IPSec encryption is automatically used by default to encrypt and decrypt all traffic protected by either 56-bit or 168-bit IPSec encryption.

The Cisco uBR925 cable access router contains the following interfaces:

- A single F-connector interface to the cable system.
- Four RJ-45 (10BASE-T Ethernet) hub ports to connect:
  - Up to three computers directly to the four Ethernet hub ports at the rear of the cable access router when operating in bridging mode. When operating in routing mode, all four Ethernet hub ports can be connected directly to four computers.
  - One of the four Ethernet hub ports at the rear of the cable access router can be connected to an Ethernet hub, which then connects additional computers or devices at the site when operating in routing or bridging mode.
- One USB port to connect the cable access router to a computer.

- Two RJ-11 Foreign Exchange Station (FXS) ports connect telephones and fax devices to the cable system and IP backbone. The FXS ports on the Cisco uBR925 router can be connected to analog telephones or fax machines but cannot be used for private branch exchange (PBX) extensions.
- One RJ-45 console port (optional) to connect to a laptop computer or console terminal when locally configuring the Cisco uBR905 router; the router ships from the Cisco factory with the console port enabled.
- The onboard hardware accelerator for IPSec encryption is automatically used by default to encrypt and decrypt all traffic protected by either 56-bit or 168-bit IPSec encryption.

Determining the Software Version

To determine the version of Cisco IOS software running on your cable access router, log into the cable access router and enter the **show version** EXEC command:

For the Cisco uBR905 and Cisco uBR925 cable access routers:

```
router# show version
Cisco Internetwork Operating System Software
IOS (tm) 925 Software (ubr925-k9o3sv4y5-mz), Version 12.2(8)YJ, RELEASE SOFTWARE
```

Upgrading to a New Software Release

For technical information about upgrading to a new software release, see *Cisco IOS Upgrade Ordering Instructions* on Cisco.com located at:

http://www.cisco.com/warp/public/620/6.html

For other information about upgrading to Cisco IOS Release 12.2 T, see the product bulletin *Cisco IOS Software Release 12.2 T Ordering Procedures and Platform Support* on Cisco.com at:

Service & Support: Software Center: Cisco IOS Software: Product Bulletins: Software

Under Cisco IOS 12.2, click on Cisco IOS Software Release 12.2 T Ordering Procedures and Platform Support

Feature Set Tables

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

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

Table 4 lists the features and feature sets supported by the Cisco uBR905 and Cisco uBR925 cable access routers in Cisco IOS Release 12.2(8)YJ and uses the following conventions:

Yes—The feature is supported in the software image.

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

Note This table might not be cumulative or list all the features in each image. You can find the most current Cisco IOS documentation on Cisco.com.

This set of electronic documents may contain updates and modifications made after the hard-copy documents were printed. If you have a Cisco.com login account, you can find image and release information regarding features prior to Cisco IOS Release 12.2(8)YJ by using the Feature Navigator tool at http://www.cisco.com/go/fn.

Table 4 Feature Lists for the Cisco uBR905 and Cisco uBR925 Cable Access Routers

	Feature Set	Feature Set
Features	**Perf Small Office/Voice/FW/IPSec 3DES**	**Perf Small Office/FW/ IPSec 3DES**
IPv6 for Cisco IOS Software	No	No
uBR905 Cable Access Router	Yes	Yes
uBR925 Cable Access Router	Yes	Yes
Cable Device MIB (RFC 2669)	Yes	Yes
Cable-Modem VoIP Clock-Internal Command	Yes	Yes
Cable Monitor	Yes	Yes
Cisco Easy VPN Remote feature	Yes	Yes
Cisco Easy VPN Remote Phase II feature	Yes	Yes
Cisco H.323 Version 2 Phase 2	Yes	No
Cisco IOS Firewall Software	Yes	Yes
Cisco Secure Intrusion Detection System (IDS)	Yes	Yes
Cisco Standard MIBs	Yes	Yes
DF Bit Override Functionality with IPSec Tunnels	Yes	Yes
DHCP Proxy Support	Yes	Yes
DOCSIS 1.0+ Extensions (Dynamic multi-SID assignment and concatenation)	Yes	Yes
DOCSIS Baseline Privacy Interface (BPI) Encryption	Yes	Yes
DOCSIS Baseline Privacy Interface (BPI) MIB	Yes	Yes
DOCSIS-Compliant Bridging	Yes	Yes
Easy IP	Yes	Yes
H.323 Call Redirection Enhancements	Yes	No
H.323v2 Caller ID	Yes	No

Table 4 Feature Lists for the Cisco uBR905 and Cisco uBR925 Cable Access Routers (continued)

Features	Feature Set Perf Small Office/Voice/FW/IPSec 3DES	Feature Set Perf Small Office/FW/ IPSec 3DES
H.323v2 Protocol	Yes	No
HSRP Support for ICMP Redirect	Yes	Yes
IP Address DOCSIS Command	Yes	Yes
IPSec Encryption with 56-bit DES	Yes	Yes
IPSec Encryption with Triple DES (3DES)	Yes	Yes
Layer 2 Tunneling Protocol (L2TP)	Yes	Yes
MGCP Including NCS	Yes	No
MGCP Model	Yes	No
NAT Support of H.323 RAS	Yes	No
NAT—Support for NetMeeting Directory (Internet Locator Service—ILS)	Yes	Yes
Parser Cache	Yes	Yes
RFC 2233 Support	Yes	Yes
Radio Frequency Interface MIB (RFC 2670)	Yes	Yes
Routing (RIP V2)	Yes	Yes
Secure Shell (SSH)—56-bit encryption	Yes	Yes
Secure Shell (SSH)—3DES encryption	Yes	Yes
VoIP Support (Cisco uBR925 router only)	Yes	No
VPN Enhancement—Dynamic Crypto Map	Yes	Yes

New and Changed Information

No New Hardware Features in Release 12.2(8)YJ

Cisco IOS Release 12.2(8)YJ does not support any new hardware features.

New Software Features in Release 12.2(8)YJ

The following new software features are supported in Cisco IOS Release 12.2(8)YJ.

Note See the Cisco IOS Release 12.2(8)T release notes for a complete feature list for the Cisco uBR905 and Cisco uBR925 cable access routers.

Cisco Easy VPN Remote Phase II Features

The Phase II implementation of the Cisco Easy VPN Remote feature provides enhancements and additional capabilities to Phase I features. In Phase II, the Cisco Easy VPN Remote feature can provide the following enhancements and feature capabilities:

- Manual Tunnel Control, page 12—Establishes and terminates the IPSec VPN tunnel on demand.
- Multiple Inside Interface Support, page 13—Adds up to three inside interfaces on the Cisco Easy VPN Remote configuration.
- Multiple Outside Interfaces Support, page 14—Configures up to four outside tunnels for outside interfaces.
- NAT Interoperability Support, page 14—Automatically restores a manually-configured NAT configuration when the IPSec VPN tunnel is disconnected.
- Local Address Support for Cisco Easy VPN Remote, page 14—The Cisco Easy VPN Remote feature is enhanced to support an additional **local-address** attribute that specifies which interface is used to determine the IP address used to source the Cisco Easy VPN Remote tunnel traffic.
- Cable DHCP Proxy Enhancement, page 15—The **cable-modem dhcp-proxy interface** configuration command is enhanced to support the loopback interface for Cisco uBR905 and Cisco uBR925 cable access routers, so that a public IP address is automatically assigned to the loopback interface.
- Peer Hostname Enhancement, page 15 —If a peer is defined as a hostname, the DNS lookup is done only at the time of the tunnel connection.
- Proxy DNS Server Support, page 16 —The router in a Cisco Easy VPN Remote Phase II configuration can be configured to act as a proxy DNS server for LAN connected users.
- PIX Interoperability Support, page 16—Cisco Easy VPN Remote Phase II supports Cisco PIX Firewall Version 6.2.
- Cisco IOS Firewall Support, page 16—Cisco Easy VPN Remote Phase II works in conjunction with Cisco IOS Firewall configurations.
- Simultaneous Easy VPN Remote and Server Support, page 16—configures simultaneous Easy VPN Remote and Easy VPN Server support on the same Cisco 1700 series routers. This feature does not apply to the Cisco uBR905 and Cisco uBR925 cable access routers.
- Cisco Easy VPN Remote Web Manager, page 16—Users can manage the Cisco Easy VPN Remote feature on the Cisco uBR905 and Cisco uBR925 cable access routers using a built-in web interface.

In addition, if you are using the VPN 3000 Series Concentrator, the concentrator's configuration has been simplified. For the Cisco Easy VPN Remote Phase II feature, you can use the default IKE and IPSEC client lifetime configured on the VPN 3000 Series Concentrator. You do not need to create a new IPSec Security Association.

For more detailed information and configuration information on the Cisco Easy VPN Remote Phase II enhancements, refer to the *Cisco Easy VPN Remote Phase II* feature module at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122y/122yj/ftezvp2.htm

Manual Tunnel Control

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

Cisco Easy VPN Remote Phase II 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 Remote 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 Remote 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 Remote 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 Support

The Cisco Easy VPN Remote Phase I feature supported only one inside interface which by default was the Ethernet interface on the Cisco uBR905 and Cisco uBR925 cable access routers. Cisco Easy VPN Remote Phase II enhances this feature to allow multiple inside interfaces on the Cisco uBR925 cable access router.

A second inside interface can be manually configured using the new **inside** keyword with the **crypto ipsec client ezvpn** interface configuration command:

```
Router(config-if)# crypto ipsec client ezvpn <name> inside
```

If you want to disable the default inside interface and configure another inside interface on the Cisco uBR905 and Cisco uBR925, you must configure the other inside interface first and then disable the default inside interface. You can use the following command to disable the default inside interface:

```
no crypto ipsec client ezvpn <name> inside
```

If you did not configure the other inside interface first before disabling the default inside interface, you receive a message such as the following:

```
ezvpn_client_37(config)#int e0
ezvpn_client_37(config-if)#no crypto ipsec client ezvpn hw-client inside
Cannot remove the single inside interface unless
one other inside interface is configured
```

This new command has the following limitations and restrictions:

- This command has an effect only on the Cisco uBR925 cable access router, which has both an Ethernet and USB interface. This command has no effect on the Cisco uBR905 cable access router because it supports only one Ethernet interface.
- You must configure at least one inside interface, otherwise the Cisco Easy VPN Remote Phase II does not establish a connection.
- Adding a new inside interface or removing an existing inside interface automatically resets the Cisco Easy VPN Remote Phase II connection (the currently established tunnel). You must reconnect a manually configured tunnel or reconfigure the Cisco Easy VPN Remote Phase II connection.
- Configuration information for the default inside interface is shown with the **show crypto ipsec client ezvpn** command. All inside interfaces, whether they belong to a tunnel, are listed in interface configuration mode, as an inside interface, along with the tunnel name.

Multiple Outside Interfaces Support

The Cisco Easy VPN Remote Phase II feature adds support for configuring additional multiple tunnels for outside interfaces, by establishing one tunnel per outside interface. Up to four tunnels can be configured using the new outside **keyword** with the **crypto ipsec client ezvpn** interface configuration command:

```
Router(config-if)# crypto ipsec client ezvpn <name> outside
```

However, this command has no effect on the Cisco uBR905 and Cisco uBR925 cable access routers because these routers support only one outside interface (the cable interface).

NAT Interoperability Support

Cisco Easy VPN Remote Phase II supports interoperability with Network Address Translation (NAT). You can have a NAT configuration and a Cisco Easy VPN Remote configuration coexist. When an IPSec VPN tunnel is down, the NAT configuration works.

The Cisco Easy VPN Remote automatically creates a NAT configuration, with the corresponding Access Lists (ACLs), to implement client mode and split tunneling. In the initial release of the Cisco Easy VPN feature, this automatic NAT/ACL configuration overrode any previous NAT/ACL configuration. When a tunnel timed out or disconnected, such as due to manual tunnel control, the automatic NAT/ACL configuration was automatically removed, which prevented any Internet access, even to non-tunnel destinations.

In Phase II of the Cisco Easy VPN Remote feature, the router automatically restores the previous NAT configuration when the IPSec VPN tunnel is torn down. The user-defined ACLs are not disturbed. Users can continue to access non-tunnel areas of the Internet when the tunnel times out or disconnects.

Note When a Cisco Easy VPN Remote Phase II tunnel is up, the router processes both the Cisco Easy VPN Remote Phase II ACLs and any user-defined ACLs. However, the Cisco Easy VPN Remote Phase II ACLs are given the highest priority for processing and are executed first, before any user-defined ACLs are processed.

Local Address Support for Cisco Easy VPN Remote

The Cisco Easy VPN Remote Phase II feature is enhanced to support an additional **local-address** attribute that specifies which interface is used to determine the IP address used to source the Easy VPN tunnel traffic. After specifying the interface with the **local-address** subcommand, you can manually

assign a static IP address to the interface or use the **cable-modem dhcp-proxy interface** command to automatically configure the specified interface with a public IP address. See "Cable DHCP Proxy Enhancement" section on page 15 for more information on the **cable-modem dhcp-proxy interface** command.

The local-address support is available for all platforms, but it is more applicable to the Cisco uBR905 and Cisco uBR925 cable access routers in conjunction with the **cable-modem dhcp-proxy interface** command. Typically, the loopback interface is the interface used to source tunnel traffic for the Cisco uBR905 and Cisco uBR925 cable access routers.

The following example specifies that the loopback interface be used to source tunnel traffic:

```
router# config t
router(config)# crypto ipsec client ezvpn telecommuter-client
router(config-crypto-ezvpn)# local-address loopback0
router(config-crypto-ezvpn)#
```

Cable DHCP Proxy Enhancement

In a typical DOCSIS network, the Cisco uBR905 and Cisco uBR925 cable access routers are normally configured with a private IP address on the cable-modem interface. In Cisco Easy VPN Remote Phase I, a public IP address is required on the cable-modem interface to support the Easy VPN Remote feature.

In Phase II, cable providers can use the Cable DHCP Proxy feature to obtain a public IP address and assign it to the cable modem interface, which is usually the loopback interface.

To support Cisco Easy VPN Remote Phase II on the uBR905 and uBR925 cable access routers, the existing **cable-modem dhcp-proxy interface** configuration command is enhanced to support the loopback interface. The router automatically configures the loopback interface with the public IP address obtained from the DHCP server. You must create the loopback interface, which is a virtual interface, first before issuing the **cable-modem dhcp-proxy interface** command.

```
router# config t
router(config)# interface cable-modem 0
router(config-if)# cable-modem dhcp-proxy interface loopback0
router(config-if)#
```

For more information on the **cable-modem dhcp-proxy interface** command, refer to the "Cable CPE Commands" chapter at http://www.cisco.com/univercd/cc/td/doc/product/cable/bbccmref/bbcmcpe.htm in the *Cisco Broadband Cable Command Reference Guide* at http://www.cisco.com/univercd/cc/td/doc/product/cable/bbccmref/index.htm.

Peer Hostname Enhancement

The peer in a Cisco Easy VPN Remote Phase II configuration can be defined either as an IP address or a hostname. In the initial release of the Cisco Easy VPN Remote feature, the Domain Name System (DNS) lookup was done immediately at configuration time to get the peer's IP address.

In Phase II of the Cisco Easy VPN Remote feature, the DNS lookup is done when the IPSec VPN tunnel is connected, which allows the router to deal with topology and network changes that can happen when a remote peer goes down and additional or redundant servers come online to handle the tunnel connections.

This feature is automatically enabled whenever you specify a hostname with the **peer** command in Cisco Easy VPN Remote configuration mode.

Proxy DNS Server Support

The Cisco uBR905 and Cisco uBR925 cable access routers perform DNS resolutions depending on whether an IPSec VPN tunnel is up or not. When the IPSec VPN tunnel is up, the enterprise's DNS servers are used, but when the IPSec VPN tunnel is down, the DNS servers at the ISP or cable provider are used. This can result in name-resolution conflicts when the user connects or disconnects the IPSec VPN tunnel.

To avoid some of these problems, the Cisco uBR905 and Cisco uBR925 cable access routers can be configured to act as a proxy DNS server when the IPSec VPN tunnel is down. In this capacity, the router receives DNS queries from local users on behalf of the real DNS server and replies with the router's LAN address as the DNS server's IP address. After the WAN connection comes up, the router forwards the DNS queries to the real DNS server and caches the DNS query records.

To enable the proxy DNS server feature, use the **ip dns server** command in global configuration mode.

PIX Interoperability Support

The Cisco Easy VPN Remote Phase II feature supports Cisco PIX Firewall Version 6.2.

You can refer to *Cisco PIX Firewall and VPN Configuration Guide Version 6.2* documentation on Cisco.com at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_62/config/index.htm

Cisco IOS Firewall Support

Cisco Easy VPN Remote Phase II works in conjunction with Cisco IOS Firewall configurations on all platforms.

Simultaneous Easy VPN Remote and Server Support

In Cisco IOS Release 12.2(8)YJ, this feature is supported for multiple outside interfaces platforms, such as the Cisco 1700 series routers. This feature does not affect the Cisco uBR905 and Cisco uBR925 cable access routers because these routers support only one outside interface (the cable interface).

Cisco Easy VPN Remote Web Manager

In Cisco IOS Release 12.2(8)YJ, the Cisco Easy VPN Remote Web Manager is a web interface used to manage the Cisco Easy VPN Remote Phase II feature for Cisco uBR905 and Cisco uBR925 cable access routers. Users do not need access to the command-line interface (CLI) to manage the Cisco Easy VPN Remote connection. The web interface allows the user to:

- See the current status of theCisco Easy VPN Remote Phase II tunnel.
- Connect a tunnel that is configured for manual control.
- Disconnect a tunnel that is configured for manual control or reset a tunnel configured for automatic connection.
- Be prompted for Xauth information if Xauth information is needed.

For information on configuring and using the Cisco Easy VPN Remote Web Manager, refer to the *Cisco Easy VPN Remote Phase II* feature module at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122y/122yj/ftezvp2.htm

No New Hardware Features in Release 12.2(4)YA2

Cisco IOS Release 12.2(4)YA2 does not support any new hardware features.

No New Software Features in Release 12.2(4)YA2

Cisco IOS Release 12.2(4)YA2 does not support any new software features

No New Hardware Features in Release 12.2(4)YA1

Cisco IOS Release 12.2(4)YA1 does not support any new hardware features.

No New Software Features in Release 12.2(4)YA1

Cisco IOS Release 12.2(4)YA1 does not support any new software features

New Hardware Features in Release 12.2(4)YA

Cisco IOS Release 12.2(4)YA supports both the Cisco uBR905 and Cisco uBR925 cable access routers.

New Software Features in Release 12.2(4)YA

The following new software features are supported in Cisco IOS Release 12.2(4)YA.

Note See the Cisco IOS Release 12.2(4)T release notes for a complete feature list.

Cisco Easy VPN Remote Feature

Cable modems, DSL/ADSL 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 two routers' VPN parameters.

The Cisco Easy VPN Remote feature eliminates much of this tedious work by implementing Cisco's Unity Client protocol, which allows most VPN parameters to be defined at an IPSec server. This server can be a dedicated VPN device such as a VPN 3000 concentrator or a Cisco PIX Firewall, or a VPN router such as the Cisco 7100 router.

After the IPSec server has been configured, a VPN connection can be created with minimal configuration on an IPSec client, such as a Cisco uBR905 or Cisco uBR925 cable access router. When the IPSec client initiates the VPN tunnel connection, the IPSec server pushes the IPSec policies to the IPSec client and creates the corresponding VPN tunnel connection.

The Cisco Easy VPN Remote feature supports two modes of operation:

- Client—Specifies that Network Address Translation/Port Address Translation (NAT/PAT) be done, so that the PCs and other hosts at the client end of the VPN tunnel form a private network that does not use any IP addresses in the destination server's IP address space.

  In client mode, the Cisco Easy VPN Remote feature automatically configures the NAT/PAT translation and access lists that are needed to implement the VPN tunnel. These configurations are automatically created when the IPSec VPN connection is initiated. When the tunnel is torn down, the NAT/PAT and access list configurations are automatically deleted.
- Network Extension—Specifies that the PCs and other hosts at the client end of the VPN tunnel should be given IP addresses in the destination enterprise network's IP address space, so that they form one logical network.

The following commands are new or have been modified in Cisco IOS Release 12.2(8)YJ to support the Cisco Easy VPN Remote feature:

- **clear crypto ipsec client ezvpn**
- **crypto ipsec client ezvpn xauth**
- **crypto ipsec client ezvpn** (global configuration)
- **crypto ipsec client ezvpn** (interface configuration)
- **show crypto ipsec client ezvpn**
- **show tech-support**
- **debug crypto ipsec client ezvpn**

Tip For complete information on this feature, see the Cisco Easy VPN Remote Feature document, available on Cisco.com and the Customer Documentation CD-ROM.

Limitations and Restrictions

Cisco IOS Release 12.2(8)YJ for the Cisco uBR905 and Cisco uBR925 cable access routers contains the following limitations and restrictions.

Cisco Easy VPN Remote Phase II

- Establishing Cisco Easy VPN Remote Phase II tunnels over sub-interfaces is not supported in Cisco IOS Release 12.2(8)YJ.
- The Cisco Easy VPN Remote Web Manager does not work with the cable -monitor web interface in Cisco IOS 12.2(8)YJ Release. To access the cable-monitor web interface, you must first disable the Cisco Easy VPN Remote web interface with the **no ip http ezvpn** command, and then enable the Cable Monitor with the **ip http cable-monitor** command.

Bridging Support

The Cisco uBR905 and Cisco uBR925 cable access routers interoperate with DOCSIS cable networks. Cisco IOS Release 12.2(8)YJ does not support bridging traffic across a non-DOCSIS cable network.

Detecting Carrier Sense Errors

The Cisco uBR905 and Cisco uBR925 cable access routers cannot detect carrier sense errors on the four Ethernet ports that connect the router to the subscriber's local area network. This is because the four Ethernet ports are provided by an internal hub that always provides a carrier sense signal to the Cisco IOS software, even if no Ethernet devices are connected to the external ports.

In particular, this means that the dot3StatsCarrierSenseErrors attribute in ETHERLIKE-MIB (RFC 2665) will never indicate any drops in carrier of the Ethernet interface.

DOCSIS CLI Commands are Removed

To comply with DOCSIS requirements that restrict access to commands that change DOCSIS parameters, Cisco IOS Release 12.2(1)T removed a number of commands from the CLI. The following commands and are now reserved exclusively for DOCSIS use:

- **cable-modem downstream saved channel**
- **cable-modem downstream symbol rate**
- **cable-modem fast-search**
- **cable-modem transmit-power**
- **cable-modem upstream preamble qpsk**

GRE IP Tunnels Support

Cisco IOS Release 12.2(2)XA, 12.2(2)T, 12.2(4)YA, or greater is required to support Generic routing encapsulation (GRE) IP tunnels.

IP Address Negotiation

The DOCSIS specifications require that a cable modem obtain its IP address at power-on or reset from a DHCP server that is available through the cable interface.

For this reason, the Cisco uBR905 and Cisco uBR925 cable access routers default to a configuration that uses the **ip address docsis** command for the cable interface. It is not possible to override this setting by specifying a static IP address using other forms of the **ip address** command. To assign a static IP address to the cable access router, configure the DHCP server so that it assigns the desired IP address on the basis of the unit MAC address.

Note The **ip address dhcp** and **ip address negotiated** commands cannot be used on the cable interface.

Layer 2 Tunneling Protocol

Implementation of L2TP in Cisco IOS Release 12.2(8)YJ is dependent on a PPP connection supported on one of the directly attached interfaces. A dial-up PPP connection is required in order to initiate an L2TP Tunnel connection. This is a requirement of the L2TP Access Concentrator (LAC). In Cisco IOS Release 12.2(8)YJ, the cable access router cannot function as the LAC; it can only function as the L2TP Network Server (LNS), which terminates a tunnel created elsewhere in the network.

Note Cisco IOS Release 12.2(2)XA, 12.2(2)T, 12.2(4)YA, or greater is required to support Generic routing encapsulation (GRE) IP tunnels.

Upgrading Software Images Using BPI

To enable BPI encryption, the Cisco uBR905 and Cisco uBR925 cable access routers must use a Cisco IOS image that supports BPI encryption. If the current software image of the router does not support BPI encryption (or if the current software image is corrupted), you must disable BPI encryption in the DOCSIS configuration file and reset the router before you will be able to download a new software image.

Using Access Lists

The DOCSIS processes onboard the Cisco uBR905 and Cisco uBR925 cable access routers automatically create a number of access lists at initial power-on provisioning to control which network management workstations are allowed SNMP access. This means that when you are creating access lists for use with IPSec VPN configurations, you must not configure the cable access router to use the same access lists that the DOCSIS processes are using.

In previous Cisco IOS software releases, the cable access routers used access lists 100, 101, and 102 for the cable, Ethernet, and USB interfaces to control this access. In Cisco IOS Release 12.2(8)YJ, the cable access router instead uses access lists 170, 171, and 172 to minimize the potential for conflict with user-configured access lists, but you must still be certain not to configure access lists 170–172 manually, either by using the CLI or a Cisco IOS configuration file.

Note See caveats CSCdr45850 and CSCdr46128 for more information about this situation.

Three-Way Calling

Three-way calling services are limited to using only the G.711 codec voice algorithms. Attempts to connect a call using a high complexity algorithm, such as G.729, will result in blocked calls.

Using Multiple PCs

The “MAX CPE” parameter in the DOCSIS configuration file determines how many PCs (or other CPE devices) are supported by the Cisco uBR905 and Cisco uBR925 cable access routers. The default value for the “MAX CPE” parameter is 1, which means only one PC can be connected to the cable access router.

The DOCSIS 1.0 specification states that a CMTS cannot age-out MAC addresses for CPE devices, so the first PC that is connected to the cable access router is normally the only one that the CMTS recognizes as valid. If a subscriber replaces an existing PC or changes its network interface card (NIC) to one that has a different MAC address, the CMTS will refuse to let the PC come online because the maximum number of CPE devices specified by the “MAX CPE” parameter would be exceeded. The CMTS will also refuse to let the PC come online if a user decides to move a PC from one cable access router to another.

To allow a subscriber to replace an existing PC or NIC, the following workarounds are possible:

- If using a Cisco CMTS router as the CMTS, enter the clear cable host MAC address command on the Cisco CMTS router to remove the MAC address from the internal address tables of the router from the PC. The new PC will be rediscovered and associated with the correct cable access router during the next DHCP lease cycle.
- Increase the value of the “MAX CPE” parameter in the cable access router’s DOCSIS configuration file so that it can accommodate the desired number of PCs. Reset the cable access router to force it to load the new configuration file.

Using the Reset Switch

The reset switch on the back panel of the Cisco uBR905 and Cisco uBR925 cable access routers is recessed to prevent accidental resets of the router. To depress the switch, use a blunt object, such as a pen or pencil point; do not use a sharp object, such as a knife or awl, because sharp objects could damage the switch and the circuitry of the router.

Important Notes

This section contains important information about using the Cisco uBR905 and Cisco uBR925 cable access routers with Cisco IOS Release 12.2(8)YJ software.

Cisco Easy VPN Remote Phase II

- Any changes to an active Cisco Easy VPN Remote Phase II configuration or IP address changes to the involved interfaces, such as adding or removing an inside interface, results in a reset of the Cisco Easy VPN Remote Phase II connection.
- For the uBR905 and uBR925 cable access routers and the Cisco 800 series routers, no configuration work is needed if you have a Phase I configuration and then upgrade to a Phase II image. 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 Remote Phase II image, you must configure the inside interfaces because there is no longer a default inside interface.

- Cisco Easy VPN Remote Phase II supports Cisco PIX Firewall Version 6.2. You can refer to *Cisco PIX Firewall and VPN Configuration Guide Version 6.2* documentation on Cisco.com at the following URL:

  http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_62/config/index.htm

- 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 Remote using hostname. You can either configure DNS on the client to resolve the peer hostname, or you can configure peer hostname locally on the client using the **ip host peer_hostname ip_address** command. As an example, you can configure peer hostname locally on an Easy VPN Remote with the **ip host crypto-gw.cisco.com 10.0.0.1** command. Or you can configure the Easy VPN Remote to use hostname with the **peer hostname** command, such as **peer crypto-gw.cisco.com**.
- The Interactive Hardware Client Authentication Version 3.5—Cisco Easy VPN Remote Phase II does not support the Interactive Hardware Client Authentication Version 3.5 feature. This feature must be disabled. This is configured on the VPN 3000 series concentrator by clicking the **HW Client** tab on the **Configuration | User Management | Base Group** screen.

Limitation on Vendor-Specific Information in the DOCSIS Configuration File

DOCSIS requires that when the cable modem sends its Registration Request (REG-REQ) message to the CMTS, it must include the configuration information found in the DOCSIS configuration file. This configuration information must include all vendor-specific information fields (VSIF). Because MAC-layer management messages, such as REG-REQ, have a maximum data size of 1522 bytes, this limits the amount of VSIF information that can be included in the DOCSIS configuration file.

In particular, the maximum packet size imposes a limit on the number of Cisco IOS CLI commands you can include as VSIF fields in the DOCSIS configuration file. The exact number of commands that will fit depends on the other information included in the file, as well as the length of each command.

If the REG-REQ message is larger than 1522 bytes, the cable modem will likely report errors similar to the following errors that appears on Cisco uBR900 series cable access routers:

```
%LINK-4-TOOBIG: Interface cable-modem0, Output packet size of 1545 bytes too big
%LINEPROTO-5-UPDOWN: Line protocol on Interface cable-modem0, changed state to down
```

In addition, the CMTS will also report that the cable modem timed out during the registration process. If this occurs, you can try the following steps:

- Reduce the length of the commands by using the abbreviated form of the command. For example, you can specify the **int c0** instead of the full command **interface cable-modem0**.
- SNMP MIB objects are not included in the Registration Request message, so wherever possible, replace the CLI commands with the corresponding SNMP MIB object statements in the DOCSIS configuration file.
- If a large number of CLI commands must be given, use VSIF option 128 to download a Cisco IOS configuration file to the cable modem.

For complete details on what is included in the REG-REQ message, see Chapter 6 of the current DOCSIS 1.1 specification (SP-RFIv1.1-I07-010829 or later).

Note This limitation is being tracked by caveat CSCdv83892 but is not expected to be resolved unless the DOCSIS specification is changed to remove the maximum size limit for MAC-layer management messages.

Cisco IOS Configuration File Download

The DOCSIS configuration file can contain an optional Vendor-Specific Information Field (VSIF) that instructs the Cisco uBR905/uBR925 cable access router to download a Cisco IOS configuration file before coming online. In Cisco IOS releases prior to Cisco IOS Release 12.2(4)T, the download of the Cisco IOS configuration file was optional—if the download failed, the router would go online anyway.

Starting with Cisco IOS Release 12.2(4)T and 12.2(4)YA, if the DOCSIS configuration file specifies a download of a Cisco IOS configuration file, that download is required—if the download of the Cisco IOS configuration file fails for any reason, the Cisco uBR905/uBR925 cable access router will reset with the error message "CMAC_LOG_CONFIG_FILE_CISCO_BAD_TYPE" and attempt to reregister again.

Cisco DOCSIS CPE Configurator Support

The DOCSIS specification requires that every cable modem download a DOCSIS configuration file before being allowed online. To support the creation of such files, Cisco has made available the Cisco DOCSIS CPE Configurator tool, a Java-based tool available for both Windows and Solaris systems.

Because of ongoing changes in the DOCSIS specification, you must use version 3.5 or greater of the Cisco DOCSIS CPE Configurator tool when generating DOCSIS configuration files for the Cisco uBR905 Cable Access Router. The current version of this tool is available on Cisco.com at http://www.cisco.com/cgi-bin/tablebuild.pl/cpe-conf.

CPE Device Filtering

In Cisco IOS Release 12.2(8)YJ, the "docsDevCpeIpMax" attribute defaults to –1 instead of the default of 1, which was used in previous releases. This attribute controls the maximum number of CPE devices that can pass traffic through the router from its Ethernet interface as follows:

- When "docsDevCpeIpMax" is set to –1, the Cisco uBR905 and Cisco uBR925 cable access routers do not filter any IP packets on the basis of their IP addresses, and CPE IP addresses are not added to the "docsDevFilterCpeTable" table.
- When "docsDevCpeIpMax" is set to 0, the Cisco uBR905 and Cisco uBR925 cable access routers do not filter any IP packets on the basis of the IP addresses. However, the source IP addresses are still entered into the "docsDevFilterCpeTable" table.
- When "docsDevCpeIpMax" is set to a positive integer, it specifies the maximum number of IP addresses that can be entered into the "docsDevFilterCpeTable" table. The Cisco uBR905 and Cisco uBR925 cable access routers compare the source IP address for packets it receives from CPE devices to the addresses in this table. If a match is found, the packet is processed; otherwise, the packet is dropped.

CPE IP address filtering is done as part of the following process:

1. MAC address filtering—Packets are filtered on the basis of the MAC address for the CPE device. The filter is controlled by the value of the "MAX CPE" parameter, which is set in the DOCSIS configuration file.
2. Logical Link Control (LLC) filtering—Packets are filtered on the basis of the protocol for the packets. The filter is controlled by the "docsDevFilterLLCTable" table.
3. CPE IP address filtering—Packets are filtered on the basis of the IP address for the CPE device, as controlled by the "docsDevCpeIpMax" attribute and the "docsDevFilterCpeTable" table.
4. Access list filtering—Packets are filtered on the basis of access lists. IP filtering is controlled by the "docsDevFilterIpTable" table, and SNMP access filters are controlled by the "docsDevNmAccessTable" table.

See the DOCS-CABLE-DEVICE-MIB.my MIB for more information on the attributes and tables listed.

Disabling the Finger Server

By default, the Cisco uBR905 and Cisco uBR925 cable access routers enable the onboard TCP/IP "finger" server to allow remote users to query the number and identities of any users that are logged in to the router. Unless your network operations center (NOC) requires this service, it should be disabled to prevent denial of service attacks that access the well-known port (TCP port 79) of the finger server. To disable the finger server, include the **no service finger** command in the Cisco IOS configuration file that the router downloads at initial power-on.

Supported MIBs

The Cisco uBR905 and Cisco uBR925 cable access routers support the following categories of MIBs:

- Cable device MIBs—These MIBs are for DOCSIS-compliant cable modems and CMTS to record statistics related to the configuration and status of the cable modem. These MIBs include support for the MIB attributes defined in RFC 2669.
- Cisco standard MIBs—These MIBs are common across most of the Cisco router platforms. If your network management applications are already configured to support other Cisco routers, such as the Cisco 2600 series or Cisco 7200 series, no further configuration is needed unless the version of Cisco IOS software being used has updated these MIBs.
- Radio Frequency Interface MIBs—These MIBs are for DOCSIS-compliant radio frequency interfaces in cable modems and CMTS. This MIB includes support for the MIB attributes defined in RFC 2670.
- SNMP standard MIBs—These are the MIBs required by any agent supporting SNMPv1 or SNMPv2 network management.
- Cable-specific MIBs—These MIBs provide information about the cable interface and related information on the Cisco uBR905 and Cisco uBR925 cable access routers. They include both DOCSIS-required MIBs and Cisco-specific enterprise MIBs. If your network management applications have not already been configured for the Cisco uBR905 cable access router, these MIBs must be loaded.
- Deprecated MIBs—These MIBs were supported in earlier releases of Cisco IOS software but have been replaced by more standardized, scalable MIBs. Network management applications and scripts should convert to the replacement MIBs as soon as possible.

Cable Device MIBs

The Cisco uBR905 and Cisco uBR925 cable access routers support the Cable Device MIB, which is defined by RFC 2669 and describes DOCSIS-compliant cable modems and CMTS. The Cable Device MIB records statistics related to the configuration and status of the cable modem. Statistics include an events log and device status. The following list details the components of the Cable Device MIB:

- **docsDevBase** group extends the MIB-II "system" group with objects needed for cable device system management.
- **docsDevNmAccess** group provides a minimum level of SNMP access security.
- **docsDevSoftware** group provides information for network downloadable software upgrades.
- **docsDevServer** group provides information about the progress of interaction with various provisioning servers.
- **docsDevEvent** group provides information about the progress of reporting.
- **docsDevFilter** group configures filters at the link layer and IP layer for bridge data traffic.

The Cable Device MIB is very similar to the Radio Frequency Interface (RFI) MIB in that both allow access to statistics; they are different in that the Cable Device MIB reports statistics on the cable modem, and the RFI MIB reports statistics on the radio frequency transmissions over the cable television line.

Cisco Standard MIBs

The Cisco uBR905 and Cisco uBR925 cable access routers support the Cisco Standard MIBs, which consist of the following components:

- CISCO-PRODUCT-MIB
- CISCO-SYSLOG-MIB
- CISCO-FLASH-MIB
- BRIDGE-MIB
- IF-MIB (RFC 2233)
- CiscoWorks/CiscoView support

Note The Cisco Management Information Base (MIB) User Quick Reference publication is no longer published. For the latest list of MIBs supported by Cisco, see the Cisco Network Management Toolkit on Cisco.com. From the Cisco.com home page, click this path: Service & Support: Software Center: Network Mgmt Products: Cisco Network Management Toolkit: Cisco MIB.

Radio Frequency Interface MIBs

The Cisco uBR905 and Cisco uBR925 cable access routers support the Radio Frequency Interface (RFI) MIB. The RFI MIB module is defined in RFC 2670 and describes DOCSIS-compliant radio frequency interfaces in cable modems and CMTS. On the cable modem, RFI MIB entries provide the following features:

- Upstream and downstream channel characteristics
- Class-of-service attributes

- Physical signal quality of the downstream channels
- Attributes of cable access router MAC interface
- Status of several MAC-layer counters

The RFI MIB includes tables describing both the CMTS and the cable modem side of the cable interface. All cable modem tables are implemented.

With IPSec, data can be sent across a public network without fear of observation, modification, or spoofing. IPSec enables applications such as VPNs, extranets, and remote user access.

IPSec services are similar to those provided by Cisco Encryption Technology, a proprietary Cisco security solution. However, IPSec provides a more robust security solution, and is standards based.

Cable-Specific MIBs

Table 5 shows the cable-specific MIBs that are supported on the Cisco uBR905 and Cisco uBR925 cable access routers. This table also provides a brief description of each of the MIB contents and the Cisco IOS software release in which the MIB was initially functional—earlier releases might have had unsupported prototype versions of the MIB; later releases might have added new attributes and functionality.

Note The names given in Table 5 are the filenames for the MIBs as they exist on the Cisco FTP site ftp://ftp.cisco.com/pub/mibs. Also see the Cisco Network Management Toolkit MIB page at http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml. Most MIBs are available in both SNMPv1 and SNMPv2 versions; the SNMPv1 versions have V1SMI as part of their filenames.

Table 5 Supported MIBs for the Cisco uBR905 and Cisco uBR925 Cable Access Routers

MIB Filename	Description	Release
SNMPv2-SMI.my SNMPv2-SMI-V1SMI.my	This module specifies the Structure of Management Information (SMI) for SNMPv2, as defined in RFC 1902.	12.1(3a)XL1
SNMPv2-TC.my SNMPv2-TC-V1SMI.my	This module defines the textual conventions as specified in pages 4, 10-11 of RFC 854.	12.1(3a)XL1
CISCO-SMI.my CISCO-SMI-V1SMI.my	This module specifies the Structure of Management Information (SMI) for the Cisco enterprise MIBs.	12.1(3a)XL1
CISCO-TC.my CISCO-TC-V1SMI.my	This module defines the textual conventions used in the Cisco enterprise MIBs.	12.1(3a)XL1
IF-MIB.my IF-MIB-V1SMI.my	This module describes generic objects for the Layer 3 network interface sublayers. This MIB is an updated version of the MIB-II if table, and incorporates the extensions defined in RFC 2233	12.1(3a)XL1
CISCO-CABLE-SPECTRUM-MIB.my CISCO-CABLE-SPECTRUM-MIB-V1SMI.my	This module describes the spectrum management flap list attributes.	12.1(3a)XL1
DOCS-IF-MIB.my DOCS-IF-MIB-V1SMI.my	This module describes the DOCSIS-compliant Radio Frequency (RF) interfaces in cable modems and cable modem termination systems, as described in RFC 2670.	12.1(3a)XL1

Table 5 Supported MIBs for the Cisco uBR905 and Cisco uBR925 Cable Access Routers (continued)

MIB Filename	Description	Release
DOCS-BPI-MIB.my DOCS-BPI-MIB-V1SMI.my	This module describes the attributes for the DOCSIS-specified Baseline Privacy Interface (BPI) on cable modems and the CMTS.	12.1(3a)XL1
CISCO-DOCS-EXT-MIB.my CISCO-DOCS-EXT-MIB-V1SMI.my	This module extends the DOCSIS standard RFI MIB (DOCS-IF-MIB) with Cisco-specific extensions, such as Quality of Service (QoS) attributes and connection status and other information regarding the cable modems and CPE devices supported by the CMTS. **Note** This MIB contains information about both the CMTS and CM, but it is supported only on the CMTS. If you are using the same manager for both CM and CMTS SNMP access, you must load this MIB in the order shown.	—
DOCS-CABLE-DEVICE-MIB.my DOCS-CABLE-DEVICE-MIB-V1SMI.my	This module was previously known as the CABLE-DEVICE-MIB and contains cable-related objects for DOCSIS-compliant cable modems, as specified in RFC 2669.	12.1(3a)XL1

Note Because of interdependencies, the MIBs must be loaded in the order given in the table.

Deprecated MIBs

A number of Cisco-provided MIBs have been replaced with more scalable, standardized MIBs; these MIBs have filenames that start with "OLD" and first appeared in Cisco IOS Release 10.2. The functionality of these MIBs has already been incorporated into replacement MIBs, but the old MIBs are still present to support existing Cisco IOS products or network management system (NMS) applications. However, because the deprecated MIBs will be removed from support, you should update your network management applications and scripts to refer to the table names and attributes that are found in the replacement MIBs.

Table 6 shows the deprecated MIBs and their replacements. In most cases, SNMPv1 and SNMPv2 replacements are available, but some MIBs are available only in one version. A few of the deprecated MIBs do not have replacement MIBs; support for these MIBs will be discontinued in a future release of Cisco IOS software.

Table 6 Replacements for Deprecated MIBs

	Replacement MIBs	
Deprecated MIB	**SNMPv1 MIB**	**SNMPv2 MIB**
OLD-CISCO-APPLETALK-MIB	RFC1243-MIB	—
OLD-CISCO-CHASSIS-MIB	ENTITY-MIB-V1SMI	ENTITY-MIB
OLD-CISCO-CPU-MIB	—	CISCO-PROCESS-MIB
OLD-CISCO-DECNET-MIB	—	—

Table 6 Replacements for Deprecated MIBs (continued)

Deprecated MIB	Replacement MIBs	
	SNMPv1 MIB	SNMPv2 MIB
OLD-CISCO-ENV-MIB	CISCO-ENVMON-MIB-V1SMI	CISCO-ENVMON-MIB
OLD-CISCO-FLASH-MIB	CISCO-FLASH-MIB-V1SMI	CISCO-FLASH-MIB
OLD-CISCO-INTERFACES-MIB	IF-MIB-V1SMI IF-MIB	CISCO-QUEUE-MIB-V1SMI CISCO-QUEUE-MIB
OLD-CISCO-IP-MIB	—	—
OLD-CISCO-MEMORY-MIB	CISCO-MEMORY-POOL-MIB-V1SMI	CISCO-MEMORY-POOL-MIB
OLD-CISCO-NOVELL-MIB	NOVELL-IPX-MIB	—
OLD-CISCO-SYS-MIB	(Compilation of other OLD* MIBS)	
OLD-CISCO-SYSTEM-MIB	CISCO-CONFIG-COPY-MIB-V1SMI	CISCO-CONFIG-COPY-MIB
OLD-CISCO-TCP-MIB	CISCO-TCP-MIB-V1SMI	CISCO-TCP-MIB
OLD-CISCO-TS-MIB	—	—
OLD-CISCO-VINES-MIB	CISCO-VINES-MIB-V1SMI	CISCO-VINES-MIB
OLD-CISCO-XNS-MIB	—	—

Note Some of the MIBs listed in Table 6 represent feature sets that are not supported on the Cisco uBR905 and Cisco uBR925 cable access routers.

Caveats

Caveats describe unexpected behavior in Cisco IOS software releases. Severity 1 caveats are the most serious caveats; severity 2 caveats are less serious. Severity 3 caveats are moderate caveats.

This section contains open and resolved caveats for Cisco IOS Release 12.2(8)YJ. All caveats in Release 12.2 T are also in Release 12.2(8)YJ.

For information on caveats in Cisco IOS Release 12.1 T, see *Caveats for Cisco IOS Release 12.1 T*, which lists severity 1 and 2 caveats and selected severity 3 caveats, and is located on Cisco.com and the Documentation CD-ROM.

Caveat numbers and brief descriptions for Release 12.2(8)YJ are listed in the following tables. For details about a particular caveat, go to Bug Toolkit at:

http://www.cisco.com/kobayashi/bugs/bugs.html

To access this location, you must have an account on Cisco.com. For information about how to obtain an account, go to the "Feature Navigator" section on page 32.

Note If you have an account with Cisco.com, you can use Bug Navigator II to find caveats of any severity for any release. To reach Bug Navigator II, go to Cisco.com and press **Login.** Then go to **Software Center: Cisco IOS Software: Cisco Bugtool Navigator II**. Another option is to go to http://www.cisco.com/support/bugtools/.

Note This document lists the caveats that were known at the time of publication. The Bug Navigator II site has the most current information about any caveat. Also, this document may be updated as needed with any new information about caveats; the most current version is always posted on Cisco.com.

Open Caveats—Release 12.2(8)YJ

There are no open caveats specific to Cisco IOS Release 12.2(8)YJ that require documentation in the release notes.

Closed or Resolved Caveats—Release 12.2(8)YJ

There are no closed or resolved caveats specific to Cisco IOS Release 12.2(8)YJ that require documentation in the release notes.

Open Caveats—Release 12.2(4)YA2

There are no open caveats specific to Cisco IOS Release 12.2(4)YA2 that require documentation in the release notes.

Closed or Resolved Caveats—Release 12.2(4)YA2

Table 7 lists the significant closed or resolved caveats that exist in Cisco IOS Release 12.2(4)YA2.

Table 7 Closed or Resolved Caveats for Release 12.2(4)YA2

Caveat ID Number	Description
CSCdv54349	aaa local authentication broken
CSCdv73238	DHCP client doesn't release BVI ip addr after no ip addr client
CSCdw57301	TPLUS: Select Error Invalid argument; inertmittent authen failure

Open Caveats—Release 12.2(4)YA1

This section documents possible unexpected behavior by Cisco IOS Release 12.2(4)YA1, and describes only severity 1 and 2 caveats and select severity 3 caveats. Table 8 lists the open caveats for Cisco IOS Release 12.2(4)YA1.

Table 8 Open Caveats for Release 12.2(4)YA1

Caveat ID Number	Description
CSCdw17297	Short pause in DTMF digit is erroneously recognized
CSCdw51353	dhcp-proxy nat pool: repeated cable flap; no CPE data

Closed or Resolved Caveats—Release 12.2(4)YA1

Table 9 lists the significant closed or resolved caveats that exist in Cisco IOS Release 12.2(4)YA1.

Table 9 Closed or Resolved Caveats for Release 12.2(4)YA1

Caveat ID Number	Description
CSCdw65903	An error can occur with management protocol processing. Please use the following URL for further information: http://www.cisco.com/cgi-bin/bugtool/onebug.pl?bugid=CSCdw65903

Open Caveats—Release 12.2(4)YA

This section documents possible unexpected behavior by Cisco IOS Release 12.2(4)YA, and describes only severity 1 and 2 caveats and select severity 3 caveats. Table 10 lists the open caveats for Cisco IOS Release 12.2(4)YA.

Table 10 Open Caveats for Release 12.2(4)YA

Caveat ID Number	Description
CSCdw17297	Short pause in DTMF digit is erroneously recognized
CSCdw51353	dhcp-proxy nat pool: repeated cable flap; no CPE data

Closed or Resolved Caveats—Release 12.2(4)YA

Cisco IOS Release 12.2(4)YA is the first release in the 12.2 YA train for the Cisco uBR905/uBR925 cable access routers but Table 11 lists the significant closed or resolved caveats that existed in previous releases for these platforms. Any caveats that were closed or resolved in Cisco IOS Release 12.2(4)T are also closed and resolved in Cisco IOS Release 12.2(4)YA.

Table 11 Closed or Resolved Caveats for Release 12.2(4)YA

Caveat ID Number	Description
CSCdv64020	Out of memory errors occur with IPSec configurations

Related Documentation

The following sections describe the documentation available for the cable access router. These documents consist of hardware and software installation guides, Cisco IOS configuration guides and command references, system error messages, feature modules, and other documents.

Most documentation is available as printed manuals or electronic documents, except for feature modules and select manuals, which are available online on Cisco.com and the Documentation CD-ROM.

Use these release notes with these documents:

- Release-Specific Documents, page 31
- Platform-Specific Documents, page 31

Release-Specific Documents

The following documents are specific to Release 12.2 and are located on Cisco.com and the Documentation CD-ROM:

- *Cross-Platform Release Notes for Cisco IOS Release 12.2*

  On Cisco.com at:

  Technical Documents: All Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 12.2: Release Notes: Cross-Platform Release Notes

  On the Documentation CD-ROM at:

  Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 12.2: Release Notes: Cross-Platform Release Notes

- Product bulletins, field notices, and other release-specific documents on Cisco.com at:

  Technical Documents

- *Caveats for Cisco IOS Release 12.2 T*

  As a supplement to the caveats listed in these release notes, see *Caveats for Cisco IOS Release 12.2*, which contains caveats applicable to all platforms for all maintenance releases of Release 12.2.

  On Cisco.com at:

  Technical Documents: All Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 12.2: Release Notes: Caveats

  On the Documentation CD-ROM at:

  Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS 12.2: Caveats

Note If you have an account with Cisco.com, you can use Bug Navigator II to find caveats of any severity for any release. To reach Bug Navigator II, go to Cisco.com and press **Login.** Then go to **Software Center: Cisco IOS Software: Cisco Bugtool Navigator II**. Another option is to go to http://www.cisco.com/support/bugtools/bugtool.shtml.

Platform-Specific Documents

These documents are available for the Cisco uBR905 and Cisco uBR925 cable access routers on Cisco.com and the Documentation CD-ROM:

- *Cisco uBR905 Hardware Installation Guide*
- *Cisco uBR925 Hardware Installation Guide*
- *Cisco uBR905/uBR925 Software Configuration Guide*
- *Cisco uBR905 Cable Access Router Subscriber Setup Quick Start Card*

- *Cisco uBR925 Cable Access Router Subscriber Setup Quick Start Card*
- *Cisco uBR925 Quick Start User Guide*

Note The *Cisco uBR905/uBR925 Software Configuration Guide* replaces the previous *Cisco uBR905 Software Configuration Guide*.

On Cisco.com at:

Technical Documents: All Product Documentation: Cisco Product Documentation: Broadband/Cable Solutions: Cisco uBR900 Series Cable Access Routers

On the Documentation CD-ROM at:

Cisco Product Documentation: Broadband/Cable Solutions: Cisco uBR900 Series Cable Access Routers

Feature Modules

Feature modules describe new features supported by Release 12.1, and are updates to the Cisco IOS documentation set. A feature module consists of a brief overview of the feature, benefits, and 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.

The Cisco Easy VPN feature is documented in the following feature modules:

- Cisco Easy VPN Remote Feature
- Cisco Easy VPN Remote Phase II

On Cisco.com at:

Technical Documents: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 12.2: New Feature Documentation

On the Documentation CD-ROM at:

Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 12.2: New Feature Documentation

Feature Navigator

Cisco Feature Navigator is a web-based tool that enables you to quickly determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image. You can search by feature or release. Under the release section, you can compare releases side by side to display both the features unique to each software release and the features in common.

Cisco Feature Navigator is available 24 hours a day, 7 days a week. To access Cisco Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions at http://www.cisco.com/register.

Cisco Feature Navigator is updated regularly when major Cisco IOS software releases and technology releases occur. For the most current information, go to the Cisco Feature Navigator home page at the following URL:

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

Cisco IOS Software Documentation Set Contents

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.

On Cisco.com and the Documentation CD-ROM, two master hot-linked documents provide information for the Cisco IOS software documentation set.

On Cisco.com, beginning under the **Service & Support** heading:

Technical Documents: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 12.2: Configuration Guides and Command References

On the Documentation CD-ROM:

Cisco IOS Software Configuration: Cisco IOS Release 12.2: Configuration Guides and Command References

Cisco IOS Release 12.2 Documentation Set

Table 12 lists the contents of the Cisco IOS Release 12.2 software documentation set, which is available in both electronic and printed form.

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.

On Cisco.com at:

Technical Documents: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 12.2

On the Documentation CD-ROM at:

Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 12.2

Table 12 Cisco IOS Release 12.2 Documentation Set

Books	Major Topics
• Cisco IOS Configuration Fundamentals Configuration Guide • Cisco IOS Configuration Fundamentals Command Reference	Cisco IOS User Interfaces File Management System Management
• Cisco IOS Bridging and IBM Networking Configuration Guide • Cisco IOS Bridging and IBM Networking Command Reference, Volume 1 of 2 • Cisco IOS Bridging and IBM Networking Command Reference, Volume 2 of 2	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
• Cisco IOS Dial Technologies Configuration Guide • Cisco IOS Dial Technologies Command Reference	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
• *Cisco IOS Interface Configuration Guide* • *Cisco IOS Interface Command Reference*	LAN Interfaces Serial Interfaces Logical Interfaces
• Cisco IOS IP Configuration Guide • Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services • Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols • Cisco IOS IP Command Reference, Volume 3 of 3: Multicast	IP Addressing and Services IP Routing Protocols IP Multicast
• Cisco IOS AppleTalk and Novell IPX Configuration Guide • Cisco IOS AppleTalk and Novell IPX Command Reference	AppleTalk Novell IPX

Table 12 Cisco IOS Release 12.2 Documentation Set (continued)

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

Table 12 Cisco IOS Release 12.2 Documentation Set (continued)

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

Obtaining Documentation

The following sections explain how to obtain documentation from Cisco Systems.

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at the following URL:

http://www.cisco.com

Translated documentation is available at the following URL:

http://www.cisco.com/public/countries_languages.shtml

Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which is shipped 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 through 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, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

If you are reading Cisco product documentation on Cisco.com, you can submit technical comments electronically. Click **Leave Feedback** at the bottom of the Cisco Documentation home page. After you complete the form, print it out and fax it to Cisco at 408 527-0730.

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

To submit your comments by mail, use the response card behind the front cover of your document, or write to the following address:

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

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools by using the Cisco Technical Assistance Center (TAC) Web Site. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC Web Site.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com is a highly integrated Internet application and a powerful, easy-to-use tool that provides a broad range of features and services to help you to

- Streamline business processes and improve productivity
- Resolve technical issues with online support

- Download and test software packages
- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

You can self-register on Cisco.com to obtain customized information and service. To access Cisco.com, go to the following URL:

http://www.cisco.com

Technical Assistance Center

The Cisco TAC is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two types of support are available through the Cisco TAC: the Cisco TAC Web Site and the Cisco TAC Escalation Center.

Inquiries to Cisco TAC are categorized according to the urgency of the issue:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration.
- Priority level 3 (P3)—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- Priority level 2 (P2)—Your production network is severely degraded, affecting significant aspects of business operations. No workaround is available.
- Priority level 1 (P1)—Your production network is down, and a critical impact to business operations will occur if service is not restored quickly. No workaround is available.

Which Cisco TAC resource you choose is based on the priority of the problem and the conditions of service contracts, when applicable.

Cisco TAC Web Site

The Cisco TAC Web Site allows you to resolve P3 and P4 issues yourself, saving both cost and time. The site provides around-the-clock access to online tools, knowledge bases, and software. To access the Cisco TAC Web Site, go to the following URL:

http://www.cisco.com/tac

All customers, partners, and resellers who have a valid Cisco services contract have complete access to the technical support resources on the Cisco TAC Web Site. The Cisco TAC Web Site requires a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to the following URL to register:

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

If you cannot resolve your technical issues by using the Cisco TAC Web Site, and you are a Cisco.com registered user, you can open a case online by using the TAC Case Open tool at the following URL:

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

If you have Internet access, it is recommended that you open P3 and P4 cases through the Cisco TAC Web Site.

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses issues that are classified as priority level 1 or priority level 2; these classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer will automatically open a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to the following URL:

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

Before calling, please check with your network operations center to determine the level of Cisco support services to which your company is entitled; for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). In addition, please have available your service agreement number and your product serial number.

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