



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

February 9, 2002
Cisco IOS Release 12.2(2)XA5
OL-1645-01 Rev CO



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(2)XA4. These release notes are updated as needed to describe new features, memory requirements, hardware support, software platform deferrals, and changes to the microcode or modem code and related documents.

For a list of software caveats that apply to Release 12.2(2)XA4, see the [“Caveats” section on page 30](#) 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 33](#).

Contents

These release notes describe the following topics:

- [Introduction, page 2](#)
- [System Requirements, page 5](#)
- [New and Changed Information, page 10](#)



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

Copyright © 2001. Cisco Systems, Inc. All rights reserved.

- [Limitations and Restrictions, page 21](#)
- [Important Notes, page 24](#)
- [Caveats, page 30](#)
- [Related Documentation, page 33](#)
- [Obtaining Documentation, page 38](#)
- [Obtaining Technical Assistance, page 39](#)

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(2)XA1. 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 Cisco IOS Release 12.2(2)XA4, the Cisco uBR905 and Cisco uBR925 cable access routers use the same software images. VoIP and USB support, however, is supported only on the Cisco uBR925 cable access router. All Cisco uBR905 and Cisco uBR925 cable access router images support DOCSIS Baseline Privacy Interface (BPI) encryption. BPI is subject to export restrictions.

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(2)XA4, which is an early deployment (ED) release based on Cisco IOS Release 12.2 T. Early deployment releases contain fixes for software caveats and support for new Cisco hardware and software features.

[Table 1](#) shows that Release 12.2(2)XA4 is the initial early deployment release for both the Cisco uBR905 and Cisco uBR925 cable access routers.



Note

Cisco IOS Release 12.2(2)XA and Cisco IOS Release 12.1(3a)XL1 were the initial early deployment releases for the Cisco uBR905 cable access router and should not be used on the Cisco uBR925 cable access router.

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

ED Release	Additional Software Features	Availability
12.2(2)XA4	Support for the [no] cable-modem qos drop-ack command.	Now
12.2(2)XA1	Support for the Cisco uBR925 cable access router was added, including the following features: <ul style="list-style-type: none"> • H.323v2 Protocol¹ • Cable-Modem VoIP Clock-Internal Command • NAT Support of H.323 RAS • Cisco H.323 Version 2 Phase 2 Gateway Features, which include: <ul style="list-style-type: none"> – 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 • MGCP Including NCS 	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(2)XA	<ul style="list-style-type: none"> • 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-SID² 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 • HSRP³ Support for ICMP⁴ 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 DES⁵ (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) • NAT—Support for NetMeeting Directory (Internet Locator Service—ILS) • Radio frequency interface • RFC 2233 support for link up/down traps and for the IF-MIB MIB⁶ • RFC 2669 and RFC 2670 Support • Routing (RIP V2) • Secure Shell (SSH) Version 1 Client and Server Support • VPN⁷ Enhancements—Dynamic Crypto Map 	Now

1. VoIP and USB support exist only when the Cisco IOS Release 12.2(2)XA1 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.

2. SID = Service ID

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(2)XA4 and includes the following sections:

- [Memory Recommendations, page 5](#)
- [Headend Interoperability, page 5](#)
- [Hardware Supported, page 6](#)
- [Determining the Software Version, page 7](#)
- [Upgrading to a New Software Release, page 7](#)
- [Feature Set Tables, page 7](#)

Memory Recommendations

[Table 2](#) lists the minimum memory recommendations for Cisco IOS Release 12.2(2)XA4 for the Cisco uBR905 and Cisco uBR925 cable access routers.

Table 2 Cisco IOS Release 12.2(2)XA Memory Recommendations

Feature Set	Image Name	Recommended Flash Memory	Recommended DRAM Memory	Runs from
Perf Small Office/Voice/FW IPSec 3DES	ubr925-k9o3sv4y5-mz	8 MB	24 MB	RAM
Perf Telecommuter/Voice IPSec 3DES	ubr925-k9sv4y5-mz	8 MB	24 MB	RAM
Value Small Office/Voice/FW IPSec 56	ubr925-k8o3sv4y5-mz	8 MB	24 MB	RAM
Value Telecommuter/Voice IPSec 56	ubr925-k8sv4y5-mz	8 MB	24 MB	RAM

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 the Cisco uBR7200 series 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(2)XA4 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, the Cisco uBR905 and Cisco uBR925 cable access routers and the destination endpoint must support IPSec encryption and be configured for the same encryption policy. The endpoint is typically an IPSec gateway 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 gateway.)



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-k8o3sv4y5-mz), Version 12.2(2)XA4, 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://tools.cisco.com/SupportFusion/FusionHome.do>

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 3 lists the features and feature sets supported by the Cisco uBR905 and Cisco uBR925 cable access routers in Cisco IOS Release 12.2(2)XA4 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(2)XA by using the Feature Navigator tool at <http://www.cisco.com/go/fn>.

Table 3 Feature List by Feature Set for the Cisco uBR905 and Cisco uBR925 Cable Access Routers

Features	Feature Set			
	Perf Small Office/Voice/FW IPSec 3DES	Perf Telecommuter/Voice/ IPSec 3DES	Value Small Office/ Voice/FW IPSec 56	Value Telecommuter/Voice IPSec 56
IPv6 for Cisco IOS Software	Yes	Yes	Yes	Yes
uBR905 Cable Access Router	Yes	Yes	Yes	Yes
uBR925 Cable Access Router	Yes	Yes	Yes	Yes
Cable Device MIB (RFC 2669)	Yes	Yes	Yes	Yes
Cable-Modem VoIP Clock-Internal Command	Yes	Yes	Yes	Yes
Cable Monitor	Yes	Yes	Yes	Yes
Cisco H.323 Version 2 Phase 2	Yes	Yes	Yes	Yes
Cisco IOS Firewall Software	Yes	No	Yes	No
Cisco Secure Intrusion Detection System (IDS)	Yes	No	Yes	No
Cisco Standard MIBs	Yes	Yes	Yes	Yes
DF Bit Override Functionality with IPSec Tunnels	Yes	Yes	Yes	Yes
DHCP Proxy Support	Yes	Yes	Yes	Yes
DOCSIS 1.0+ Extensions (Dynamic multi-SID assignment and concatenation)	Yes	Yes	Yes	Yes
DOCSIS Baseline Privacy Interface (BPI) Encryption	Yes	Yes	Yes	Yes
DOCSIS Baseline Privacy Interface (BPI) MIB	Yes	Yes	Yes	Yes
DOCSIS-Compliant Bridging	Yes	Yes	Yes	Yes
Easy IP	Yes	Yes	Yes	Yes

Table 3 Feature List by Feature Set for the Cisco uBR905 and Cisco uBR925 Cable Access Routers (continued)

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

New and Changed Information

New Hardware Features in Release 12.2(2)XA4

There are no new hardware features in Release 12.2(2)XA4.

New Software Features in Release 12.2(2)XA4

The following new software features are supported in Cisco IOS Release 12.2(2)XA4.

Cable-Modem QoS Drop-Ack Command

TCP traffic uses a packet-acknowledge algorithm, where a group of packets must be acknowledged before additional traffic can be sent. When a large number of packets is transmitted on the downstream, it can result in a large number of acknowledgements on the upstream. Because the downstream bandwidth is typically many times greater than the upstream bandwidth, certain applications can temporarily overrun the upstream with a large volume of acknowledgement packets.

If any of those acknowledgements are dropped or lost, traffic can be backed up, and data packets might have to be resent, even if those packets had in fact been successfully received. This can significantly impact real-time traffic, such as voice calls.

To optimize the TCP traffic on the upstream in these circumstances, the Cisco uBR905 and Cisco uBR925 cable access routers automatically analyze the upstream traffic and drop unnecessary packet acknowledgements when traffic begins backing up. This feature has been automatically enabled by default on the routers, starting with Cisco IOS Release 12.0(5)T.

In some situations, however, this feature can result in packets being dropped on the upstream, which could impact the performance of certain applications such as FTP transfers. If packet drops do occur on the upstream, this feature can be turned off with the **no cable-modem qos drop-ack** command, which is new to Cisco IOS Release 12.2(2)XA4.

New Hardware Features in Release 12.2(2)XA1

Cisco IOS Release 12.2(2)XA1 is the first release that supports both the Cisco uBR905 and Cisco uBR925 cable access routers.

**Note**

Cisco IOS Release 12.2(2)XA and Cisco IOS Release 12.1(3a)XL1 were the initial early deployment releases for the Cisco uBR905 cable access router and should not be used on the Cisco uBR925 cable access router.

New Software Features in Release 12.2(2)XA1

The following new software features are supported in Cisco IOS Release 12.2(2)XA1. All voice-related features apply only to the Cisco uBR925 cable access router. All other features apply to both the Cisco uBR905 and Cisco uBR925 cable access routers, unless otherwise noted.

Cable-Modem VoIP Clock-Internal Command

The **cable-modem voip clock-internal** command enables the cable access router's internal clock, allowing it to make VoIP calls over the Ethernet and USB interfaces even when the cable interface is down or disconnected. If the CMTS is a Cisco uBR7200 series router with a Cisco Cable Clock Card, this command disables the use of that clock.

Cisco H.323 Version 2 Phase 2 Gateway Features

Cisco H.323 Version 2 Phase 2 upgrades Cisco IOS software by adding the following optional features, and facilitates customized extensions to the Cisco gatekeeper:

- 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
- Translation of FXS Hookflash Relay
- H.235 Security

See the *Cisco H.323 Version 2 Phase 2* document on Cisco.com at <http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t1/h323v2p2.htm> for more information.

Czech Republic and Mexico Country Codes Supported

Cisco IOS Release 12.2(2)XA4 enhances the **cptone** voice-port configuration command with support for the Czech Republic (CZ) and Mexico (MX) country call progress codes.

H.323v2 Protocol

In architectures using the VoIP H.323v2 protocol stack, the session application manages two call legs for each call: a telephony leg managed by the voice telephony service provider, and the VoIP leg managed by the cable system operator—the VoIP service provider. Use of the H.323v2 protocol typically requires a dial plan and mapper at the Cisco uBR925 cable access router or other server location to map IP addresses to telephone numbers.

When both legs of the call have been set up, the session application creates a conference between them. The opposite leg's transmit routine for voice packets is given to each provider. The CMTS router passes data to the gateway and gatekeeper. The H.323v2 protocol stack provides signaling using H.225 and media negotiation using H.245.



Note

For more information on using H.323v2, see the document *H.323 Version 2 Support*, available on Cisco.com and the Documentation CD-ROM.

To make and receive H.323 calls, the Cisco uBR925 cable access router must be configured for the following:

- The IP address of the gateway for the destination dialed—In all situations, these IP addresses can be configured statically using the command-line interface (CLI) with voip dial peer group commands. If you are using Cisco gatekeeper products that are running Cisco IOS Release 12.0(5)T or higher images, the Cisco uBR925 cable access router can obtain these addresses dynamically from the gatekeeper using the Registration, Admission, and Status (RAS) protocol.
- The telephone numbers of the attached devices—In all situations, these IP addresses can be configured statically using the CLI pots port commands. When using Cisco Network Registrar (CNR) version 3.0 or higher, the IP addresses can be configured with the relay.tcl and setrouter.tcl scripts. If you are using Cisco gatekeeper products that are running Cisco IOS Release 12.0(5)T or higher images, you can obtain these addresses dynamically from CNR. The telephone numbers of attached devices are then sent in DHCP response messages. When the cable access router processes the DHCP response, it automatically creates the pots dial peer for each port, creates the voip dial peer for the RAS target, and starts the H.323v2 RAS gateway support.

**Note**

To support voice configurations using Cisco gatekeeper products with RAS, Cisco IOS Release 12.0(5)T or higher images with gatekeeper support are required. The headend must have IP multicast enabled. The cable interface must be designated as the default for RAS to discover the gatekeeper. The gatekeeper then resolves all dialed destinations sent to the RAS protocol.

H.323v2 Caller ID

Cisco IOS Release 12.2(2)XA4 adds support for caller ID over H.323v2 VoIP calls, using the **station-id name** and **caller-id enable** voice-port configuration commands. For example, to enable caller ID for voice port 0 on the Cisco uBR925 cable access router, enter the following commands:

```
Router# config t
Router(config)# voice-port 0
Router(voice-port)# station-id name myphonename
Router(voice-port)# caller-id enable
Router(voice-port)# exit
Router(config)#
```

**Tip**

For more information about these commands, see the *Cisco IOS Voice, Video, and Fax Command Reference, Release 12.2*, available on Cisco.com and the Customer Documentation CD-ROM.

H.323 Call Redirection Enhancements

The user-to-user information element (UUIE) of the H.323 Facility message is used primarily for call redirection. The UUIE contains a field, facilityReason, that indicates the nature of the redirection. The H.323 Call Redirection Enhancements feature adds support for two reasons: routeCallToGatekeeper and callForwarded. It also provides a non-standard method for using the Facility message to effect call transfer.

**Tip**

For more information, see the *H.323 Call Redirection Enhancements* document, available on Cisco.com and the Customer Documentation CD-ROM.

MGCP Including NCS

This feature implements the following MGCP protocols on the Cisco uBR925 cable access router:

- MGCP 1.0 (RFC2705)
- Network-based Call Signaling (NCS) 1.0, the PacketCable profile of MGCP 1.0 for residential gateways (RGWs)

Media Gateway Control Protocol (MGCP) 1.0 is a protocol for the control of Voice over IP (VoIP) calls by external call-control elements known as media gateway controllers (MGCs) or call agents (CAs). It is described in RFC2705.

PacketCable is an industry-wide initiative to develop interoperability standards for multimedia services over cable facilities using packet technology. PacketCable developed the NCS protocol, which contains extensions and modifications to MGCP while preserving basic MGCP architecture and constructs. NCS is designed for use with analog, single-line user equipment on residential gateways.

MGCP Model

MGCP bases its call control and intelligence in centralized call agents, also called media gateway controllers. The call agents issue commands to simple, low-cost endpoints, which are housed in media gateways (MGs), and they also receive event reports from the gateways. MGCP messages between call agents and media gateways are sent over IP/UDP. The messages between CA and gateways can be sent over IP/TCP as well. Typically, IP/UDP is the chosen norm.

The MGCP 1.0 Including NCS 1.0 provides protocols for residential gateways (RGWs), which sit at the border of the packet network to provide an interface between traditional, circuit-based voice services and the packet network. Residential gateways offer a small number of analog line interfaces.

Two basic MGCP constructs are endpoints and connections. An endpoint is a source or sink for call data (RTP/IP) that is flowing through the gateway. A common type of endpoint is found at the physical interface between the POTS or PSTN service and the gateway; this type of endpoint might be an analog voice port or a digital DS0 group. There are other types of endpoints as well, and some are logical rather than physical. An endpoint is identified by a two-part endpoint name that contains the name of the entity on which it exists (for example, an access server or router) and the local name by which it is known (for example, a port identifier).

A connection is a temporary allocation of resources that enables a call to be completed. One or more connections is necessary to complete a call. Connections have names that identify them with the call to which they belong. Connections can be one-to-one or multipoint. Calls and connections are initiated, modified, and deleted on instructions from call agents.

Call agents manage call flow through standard MGCP commands that are sent to the endpoints under their control. The commands are delivered in standard ASCII text, and may contain session descriptions transmitted in Session Description Protocol (SDP), a text-based protocol. These messages are sent over IP/UDP.

Call agents keep track of endpoint and connection status through the gateway's reporting of standard events that are detected from endpoints and connections. Call agents also direct gateways to apply certain standard signals when a POTS/PSTN connection expects them. For example, when someone picks up a telephone handset, an off-hook event is detected on an endpoint on the residential gateway to which the telephone is connected. The gateway reports the event to a call agent, which orders the gateway to apply the dial-tone signal to the endpoint reporting the off-hook event. The person picking up the handset hears dial tone.

Related events and signals are grouped into standard packages that apply to particular types of endpoints. For instance, the off-hook event is found in the line package, which is associated with analog-line endpoints, which in turn are associated with residential gateways.

NAT Support of H.323 RAS

Cisco IOS NAT supports all H.225 and H.245 message types, including those sent in the Registration, Admission, and Status (RAS) protocol. RAS provides a number of messages that are used by software clients and Voice over IP (VoIP) devices to register their location, request assistance in call setup, and control bandwidth. The RAS messages are directed toward an H.323 gatekeeper.

Some RAS messages include IP addressing information in the payload, typically meant to register a user with the gatekeeper or learn about another user already registered. If these messages are not known to NAT, they cannot be translated to an IP address that will be visible to the public network.

Previously, NAT did not support H.323 RAS messages. With this enhancement, embedded IP addresses can be inspected for potential address translation.



Tip

For more information, see the *NAT Support of H.323 RAS* document, available on Cisco.com and the Customer Documentation CD-ROM.

New Hardware Features in Release 12.2(2)XA

Cisco IOS Release 12.2(2)XA supports the Cisco uBR905 cable access router.

New Software Features in Release 12.2(2)XA

The following new software features are supported by the Cisco uBR905 cable access router for Release 12.2(2)XA. (The Cisco uBR925 cable access router inherits these features when running Cisco IOS Release 12.2(2)XA1.)

Cable Monitor Web Diagnostics Tool

The Cable Monitor is a web-based diagnostic tool to display the current status and configuration of the Cisco uBR905 and Cisco uBR925 cable access routers. The Cable Monitor can also be used when the cable network is down, providing an easy way for subscribers to provide necessary information to service technicians and troubleshooters.

Cisco IOS Firewall (Phase I and II)

The Cisco IOS Firewall feature set includes the following set of features:

- Context-Based Access Control (CBAC) that intelligently filters TCP and UDP packets based on the application-layer protocol. This includes Java applets, which can be blocked completely or allowed only from known and trusted sources.
- Detection and prevention of the most common denial of service (DoS) attacks, such as ICMP and UDP echo packet flooding, SYN packet flooding, half-open or other unusual TCP connections, and deliberate misfragmentation of IP packets.
- Support for a broad range of commonly used protocols, including H.323 and NetMeeting, FTP, HTTP, MS Netshow, RPC, SMTP, SQL*Net, and TFTP.
- Authentication Proxy for authentication and authorization of web clients on a per-user basis.

- Dynamic port mapping that maps the default port numbers for well-known applications to other port numbers. This can be done on a host-by-host basis or for an entire subnet, providing a large degree of control over which users can access different applications.
- Configurable alerts and audit trail.
- Intrusion Detection System (IDS) that recognizes the signatures of 59 common attack profiles. When an intrusion is detected, IDS can either send an alarm to a syslog server or to NetRanger Director, drop the packet, or reset the TCP connection.
- User-configurable audit rules.
- Configurable real-time alerts and audit trail logs.

For general information, see the description of the *Cisco IOS Firewall Feature Set* in the *Cisco Product Catalog*. For detailed information, see the *Cisco IOS Firewall Feature Set* documentation set, as well as the section *Traffic Filtering and Firewalls* in the *Security Configuration Guide* and the *Security Command Reference* (available on the Documentation CD-ROM and Cisco.com).

Cisco Secure Intrusion Detection System (IDS) Support

Cisco IOS Release 12.2(2)XA supports the Cisco Secure Intrusion Detection System (IDS), formerly known as Cisco NetRanger, which is composed of three parts:

- A management console (director) that is used to view the alarms and to manage the sensors.
- A sensor that monitors traffic. This traffic is matched against a list of known signatures to detect misuse of the network. This is usually in the form of scanning for vulnerabilities or of attacking systems. When a signature is matched, the sensor can track certain actions. In the case of the appliance sensor, it can reset the sessions (using the TCP/rst calls), or enable “shuns” of further traffic. In the case of the IOS-IDS, it can drop traffic. In all cases, the sensor can send alarms to the director.
- Communications through automated report generation of standardized and customizable reports and QoS/CoS monitoring capabilities.

DF Bit Override Functionality with IPSec Tunnels

The DF Bit Override Functionality with IPSec Tunnels feature allows customers to specify whether their router can clear, set, or copy the Don't Fragment (DF) bit from the encapsulated header. A DF bit is a bit within the IP header that determines whether a router is allowed to fragment a packet.

For more information, see the *DF Bit Override Functionality with IPSec Tunnels* document, available on Cisco.com and the Customer Documentation CD-ROM.

DOCSIS 1.0+ Extensions

In addition to the other quality of service (QoS) features, DOCSIS 1.1 supports a number of features that are required for the delivery of high-quality voice traffic. To use these features before the DOCSIS 1.1 specification is finalized, Cisco has created the DOCSIS 1.0+ extensions that contain the most important of these features:

- Concatenation—DOCSIS concatenation combines multiple upstream packets into one packet to reduce packet overhead and overall latency, and to increase transmission efficiency. Using concatenation, a DOCSIS cable modem makes only one bandwidth request for multiple packets, as opposed to making a different bandwidth request for each individual packet; this technique is especially effective for bursty real-time traffic, such as voice calls.

- **Dynamic Multi-SID Assignment**—To give priority to voice traffic, the Cisco uBR905 router assigns a different SID to each voice port. Without the DOCSIS 1.0+ extensions, the router creates these SIDs during the provisioning process, and the SIDs remain in effect until the router is rebooted with a different configuration. As part of this process, a minimum guaranteed bandwidth is permanently allocated to the voice ports; this bandwidth is reserved to the voice ports even if no calls are being made.

To avoid potentially wasting bandwidth in this manner, the DOCSIS 1.0+ extensions support the dynamic creation of multiple SIDs. New Media Access Control (MAC) messages dynamically add, delete, and modify SIDs when needed. When a phone connected to the router is taken off-hook, the Cisco uBR905 router creates a SID that has the QoS parameters needed for that particular voice call. When the call terminates, the router deletes the SID, releasing its bandwidth for use elsewhere.

The DOCSIS 1.0+ features are introduced in Cisco IOS Software Release 12.0(7) XR and 12.1(1) T.

**Note**

Both the Cisco uBR905 and Cisco uBR925 cable access routers and the CMTS must support the dynamic multi-SID and concatenation features for them to be used on the cable network. If you are using a Cisco CMTS universal broadband router as the CMTS, Cisco IOS Release 12.1(1) T (or later) is required on the Cisco CMTS router to use these features.

DOCSIS Baseline Privacy Interface (BPI)

The DOCSIS Baseline Privacy Interface (BPI) feature is based on the DOCSIS BPI Specification (SP-BPI-I02-990319 or later revision). It provides data privacy across the Hybrid Fiber-Coaxial (HFC) network by encrypting traffic flows between the Cisco uBR905 and Cisco uBR925 cable access routers and the cable operator's CMTS.

The BPI+ (BPI Plus) feature is an enhancement to the BPI feature and is based on the DOCSIS BPI+ Specification (SP-BPI+-I04-000407 or later revision), which is still in development. In addition to the regular BPI features, BPI+ provides more secure authentication of cable modems through the use of digital certificates. Also, a cable modem can use a digital signature to verify that the software image it has downloaded has not been altered or corrupted in transit.

**Note**

Cisco IOS Release 12.2(2)XA4 supports BPI encryption but not BPI+ encryption. The CMTS and Cisco uBR905 and Cisco uBR925 cable access routers must both support and enable BPI to use its features.

DOCSIS Baseline Privacy Management Information Base

The Baseline Privacy Management Information Base (MIB), as currently defined, is available in Cisco IOS Release 12.2(2)XA code. BPI allows a Simple Network Management Protocol (SNMP) manager to monitor and manage the BPI configuration of Cisco uBR905 and Cisco uBR925 cable access routers, including whether BPI is enabled, status of current authorization keys, current timeout values, real-time status counters, and additional information about authorization errors.

**Note**

The SNMP manager must load the DOCSIS-BPI-MIB.my MIB to access the BPI attributes. See the [“Cable-Specific MIBs” section on page 27](#) for details.

Dynamic Host Configuration Protocol Proxy Support

The DHCP Proxy Support feature helps to automate the configuration of the Cisco uBR905 and Cisco uBR925 cable access routers in two situations:

- When the Cisco uBR905 and Cisco uBR925 cable access routers is configured for routing mode, an IP address must be assigned to its Ethernet interface. The DHCP Proxy Support feature allows an external DHCP server to assign an IP address to the Ethernet interface, as opposed to having to assign it manually with the appropriate command line interface (CLI) commands.



Note The DHCP Proxy Support feature cannot be used to assign an IP address to the USB interface on the Cisco uBR925 cable access router.

- When network address translation (NAT) is used, an inside global address pool must be created on the Ethernet interface. The DHCP Proxy Support feature allows a DHCP server to assign an IP address that automatically creates the NAT address pool, as opposed to manually specifying a static IP address with the appropriate command line interface (CLI) commands.

When configured for DHCP Proxy Support, during startup the Cisco uBR905 and Cisco uBR925 cable access routers sends a proxy DHCP request to the DHCP server using the Ethernet interface's MAC address. The DHCP server replies with a second IP address that the router assigns to either the Ethernet interface or to the NAT pool, depending on which option was specified.

Easy IP—DHCP Server and NAT/PAT

The Easy IP feature set includes the following features to automate the assignment and use of IP addresses:

- The DHCP server feature on the Cisco uBR905 and Cisco uBR925 cable access routers includes both Intelligent DHCP Relay and DHCP Client functionality. A DHCP Relay Agent is any host that forwards DHCP packets between clients and servers—this enables the client and server to reside on separate subnets. If the Cisco uBR905 and Cisco uBR925 cable access routers DHCP server cannot satisfy a DHCP request from its own database, it can act as a DHCP proxy agent by forwarding the DHCP request to one or more secondary DHCP servers.
- Network address translation (NAT) and port address translation (PAT) frees a private network from needing a worldwide unique IP address for every computer connected to the Internet. Instead, the Cisco uBR905 and Cisco uBR925 cable access routers translates the IP addresses used on the private network into a global IP address that can be used on the Internet. One IP address can be used for multiple computers because a unique port address identifies the individual computers on the private network.



Note

NAT and PAT are defined in Requests for Comments (RFC) 1631.

Enhanced Bridging

The Cisco uBR905 and Cisco uBR925 cable access routers contains four RJ-45 (10BaseT Ethernet) hub ports, which can be connected to four computers directly or one of the four ports to an Ethernet hub. The Ethernet hub connects additional computers or devices at the site. A maximum of 254 devices can be bridged in DOCSIS bridging mode; no limit exists in routing mode.

Full and DOCSIS-Compliant Bridging

DOCSIS-compliant bridging allows the Cisco uBR905 and Cisco uBR925 cable access routers to operate as a DOCSIS 1.0 cable modem, so that it can interoperate with any DOCSIS-qualified CMTS. This is the default mode of operation for the Cisco uBR905 and Cisco uBR925 cable access routers.

HSRP Support for ICMP Redirects

The HSRP Support for ICMP Redirects feature enables Internet Control Message Protocol (ICMP) redirection on interfaces configured with the Hot Standby Router Protocol.

When running HSRP, it is important to prevent hosts from discovering the interface (or real) MAC addresses of routers in the HSRP group. If a host is redirected by ICMP to the real MAC address of a router, and that router later fails, then packets from the host will be lost. Previously, ICMP redirect messages were automatically disabled on interfaces configured with HSRP.

This feature now enables ICMP redirects on interfaces configured with HSRP. This functionality works by filtering outgoing ICMP redirect messages through HSRP, where the next-hop IP address may be changed to an HSRP virtual IP address.

IP Address Negotiation

The Cisco uBR905 and Cisco uBR925 cable access routers support the **ip address docsis** command on the cable interface. Older Cisco IOS releases used the **ip address negotiated** or **ip address dhcp** command for this purpose, but these commands cannot be used on cable interfaces.



Note

This change is cosmetic only and does not change how the cable access router obtains its IP address.

IPSec Encryption (56-bit and 3DES)

IPSec Network Security (IPSec) is an IP security feature that provides robust authentications and encryption of IP packets. IPSec is a framework of open standards developed by the Internet Engineering Task Force (IETF). IPSec provides security for transmission of sensitive information over unprotected networks such as the Internet. IPSec acts at the network layer, protecting and authenticating IP packets between participating IPSec devices (“peers”) such as the Cisco uBR905 and Cisco uBR925 cable access routers.

IPSec provides the following network security services:

- Privacy—IPSec can encrypt packets before transmitting them across a network.
- Integrity—IPSec authenticates packets at the destination peer to ensure that the data has not been altered during transmission.
- Authentication—Peers authenticate the source of all IPSec-protected packets.
- Anti-replay protection—Prevents capture and replay of packets; helps protect against denial-of-service attacks.
- 3DES—Triple DES (3DES) images increase the encryption/decryption from the 56-bit IPSec feature set to 168 bits.

Layer 2 Tunneling Protocol

Layer 2 Tunneling Protocol (L2TP) is an emerging Internet Engineering Task Force (IETF) standard that combines Cisco's Layer 2 Forwarding (L2F) and Microsoft's Point-to-Point Tunneling Protocol (PPTP). L2TP is an extension of the Point-to-Point Protocol (PPP), which is an important component for Access Virtual Private Networks (VPNs).

Traditional dial-up networking services only supported registered IP addresses, which limited the types of applications that could be implemented over VPNs. L2TP supports multiple protocols and unregistered and privately administered IP addresses over the Internet. This allows the existing access infrastructure, such as the Internet, modems, access servers, and ISDN terminal adapters (TAs), to be used.

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



Note

Cisco IOS Release 12.2(2)XA1, 12.2(2)T, or greater is required to support Generic routing encapsulation (GRE) IP tunnels.

Management Information Base (MIB) Features

Cisco IOS Release 12.2(2)XA supports the following MIB features:

- Baseline Privacy Interface (BPI) MIBs
- Cable Device MIBs
- Cisco Standard MIBs
- Radio Frequency Interface MIBs

NAT—Support for NetMeeting Directory (Internet Locator Service—ILS)

Microsoft NetMeeting is a Windows-based application that enables multiuser interaction and collaboration from a user's PC over the Internet or an intranet. Support for the NetMeeting Directory (ILS) allows connections by name from the directory built into the NetMeeting application. Destination IP addresses do not need to be known in order for a connection to be made.

Parser Cache

The Parser Cache feature optimizes the parsing (translation) of Cisco IOS software configuration command lines by remembering how to parse recently encountered command lines. This feature was developed to improve the scalability of the Cisco IOS software CLI parser when processing large configuration files. This improvement is especially useful for those cases in which thousands of virtual circuits must be configured for interfaces, or hundreds of access control lists (ACLs) are required. The parser chain cache can rapidly recognize and translate configuration lines that differ slightly from previously used configuration lines (for example, pvc 0/100, pvc 0/101, and so on). Testing indicates an improvement to load time of between 30% and 36% for large configuration files when using the parser cache.

A new global configuration command, **[no] parser cache**, allows the disabling or reenabling of parser cache.

RFC 2233 Support

In Cisco IOS Release 12.2(2)XA, the IF-MIB MIB supports RFC 2233, which obsoletes the previous RFC 1573. This change adds the “ifCounterDiscontinuityTime” attribute and changes the “ifTableLastChange attribute.”

In addition, this feature adds support for RFC 2233-compliant link up and link down traps. By default, link up and link down traps are implemented as given in the CISCO-IF-CAPABILITY.mib MIB. To generate link up and link down traps as defined by RFC 2233, use the **snmp-server trap link ietf** global configuration command.

RFC 2669 and RFC 2670 Support

RFC 2669 and RFC 2670 are supported on the DOCS-CABLE-DEVICE-MIB and DOCS-IF-MIB MIBs, respectively.

Routing (RIP V2)

When configured for routing mode, the Cisco uBR905 and Cisco uBR925 cable access routers supports the Routing Information Protocol Version 2 (RIPv2). In routing mode the Cisco uBR905 and Cisco uBR925 cable access routers automatically configures itself to use the headend's IP address as its IP default gateway. This allows the Cisco uBR905 and Cisco uBR925 cable access routers to send packets not intended for the private LAN to the headend for delivery to the Internet and other networks.



Note

The Cisco uBR905 and Cisco uBR925 cable access routers supports only static routes and the RIP routing protocol.

Secure Shell Version 1 Client Support

The Secure Shell (SSH) protocol provides for authentication and encryption at the application layer, providing a secure connection even when BPI or IPSec authentication and encryption are not used at the network layer.

By default, the SSH feature uses 56-bit DES encryption. Higher security 168-bit 3DES encryption is available when using Cisco IOS images that support 3DES IPSec encryption. (The SSH client must also support the same level of encryption.)

In Cisco IOS Release 12.2(2)XA, SSH support includes the following features:

- SSH server support allows users to use an SSH connection to log in to the Cisco uBR905 router.
- SSH client support allows a user logged in to the Cisco uBR905 and Cisco uBR925 cable access routers to log in to another router using SSH authentication and encryption.
- DES and 3DES encryption are supported, depending on the capabilities of the Cisco IOS image being used.
- RSA authentication. (RSA stands for Rivest, Shamir, and Adelman, inventors of a public-key cryptographic system.)



Note

For configuration and other information, see the *Secure Shell Version 1 Client* feature module, available on Cisco.com and the Documentation CD-ROM.

SNMP Enhancements

Cisco IOS Release 12.2(2)XA supports RFC 2669 and RFC 2670 for the DOCS-CABLE-DEVICE-MIB and DOCS-IF-MIB MIBs, respectively.

VPN Enhancement—Dynamic Crypto Map

Dynamic crypto map is one of the Cisco PIX IPSec network security commands. IPSec provides security for transmission of sensitive information over unprotected networks such as the Internet.

The **dynamic crypto map** command is used to create policy templates that are used when processing negotiation requests for new security associations from a remote IPSec peer, even if you do not know all of the crypto map parameters required to communicate with the remote peer (such as the peer's IP address). The dynamic crypto map allows you to accept requests for new security associations from previously unknown peers. These requests, however, are not processed until the Internet Security Association and Key Management Protocol (ISAKMP) Internet Key Exchange (IKE) authentication has completed successfully.

When the firewall receives a negotiation request via IKE from another IPSec peer, the request is examined to see if it matches a crypto map entry. If the negotiation does not match any explicit crypto map entry, it will be rejected unless the crypto map set includes a reference to a dynamic crypto map.

If the firewall accepts the peer's request, at the point that it installs the new IPSec security associations, it also installs a temporary crypto map entry. This entry is filled in with the results of the negotiation. At this point, the firewall performs normal processing, using this temporary crypto map entry as a normal entry, even requesting new security associations if the current ones are expiring (based on the policy specified in the temporary crypto map entry). After all of the corresponding security associations expire, the temporary crypto map entry is removed.

Dynamic crypto map sets are not used for initiating IPSec security associations. However, they are used for determining whether traffic should be protected.



Note

The only parameter required in a **dynamic crypto map** command is the **set transform-set**. All other parameters are optional.

Limitations and Restrictions

Cisco IOS Release 12.2(2)XA4 for the Cisco uBR905 and Cisco uBR925 cable access routers contains the following limitations and restrictions.

Bridging Support

The Cisco uBR905 and Cisco uBR925 cable access routers interoperate with DOCSIS cable networks. Cisco IOS Release 12.2(2)XA4 does not support bridging traffic across a non-DOCSIS cable network.

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 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)XA1, 12.2(2)T, 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 negotiated** 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(2)XA4 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(2)XA4, 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.

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(2)XA4, 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(2)XA4 software.

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-RF1v1.1-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 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 and Cisco uBR925 cable access routers. 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(2)XA4, 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 4 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 4 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 4 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
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	<p>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.</p> <p>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.</p>	—
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 5 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 5 Replacements for Deprecated MIBs

Deprecated MIB	Replacement MIBs	
	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	—	—
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 5 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(2)XA4. All caveats in Release 12.2 T are also in Release 12.2(2)XA4.

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(2)XA are listed in [Table 10](#) and [Table 11](#). 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 34](#).



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.

Resolved Caveats—Release 12.2(2)XA5

All caveats in this section have been resolved in Cisco IOS Release 12.2(2)XA5 but may be open in previous Cisco IOS releases.

- 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(2)XA4

This section documents possible unexpected behavior by Cisco IOS Release 12.2(2)XA4, and describes only severity 1 and 2 caveats and select severity 3 caveats.

Table 6 *Open Caveats for Release 12.2(2)XA4*

Caveat ID Number	Description
CSCdv79146	Inconsistent mem leak avg 650 Bytes/mibwalk
CSCdv81611	Crashdump w/ large docsis config file w/ BPI enabled

Table 6 *Open Caveats for Release 12.2(2)XA4 (continued)*

Caveat ID Number	Description
CSCdv82925	cm becomes stuck in ranging-2 state, cant clear c0 int, sram low
CSCdv84006	cm loses connectivity, DIX dwn
CSCdv86070	Hornet: Segv Exception crash with Ipsec
CSCdv87298	DTMF Digit Detection Failed to Meeting Specification
CSCdv89379	SEGV on cm during c0 interface init w/ cm remote-query on CMTS
CSCdw01104	ubr905: Non-repeatable crash while SNMP loading rboot image

Closed or Resolved Caveats—Release 12.2(2)XA4

Table 7 *Closed or Resolved Caveats for Release 12.2(2)XA4*

Caveat ID Number	Description
CSCdv88497	upstream TCP performance problems with ubr/cva
CSCdv77630	Ring frequency is incorrect for Denmark telephony
CSCdv77898	Suspend/Resume states missing for Denmark MGCP telephony
CSCdv48509	CVA does not play cptone call waiting
CSCdv50485	Quoted CID number & name strings not properly displayed by xGCP RGWs
CSCdv59255	cable modem sending RSIP for non-provisioned voice port
CSCdv23498	CD Mib memory leak of 0.5 KB per docsDev MibWalk
CSCdv31378	PHY07_ECW5: docsIfSqiQCorrecteds and docsIfSqiQUncorrectables wrong
CSCds26199	CW16_ETH-02:Blue fails eth-02 ATP because of MAX CPE
CSCdv50040	OSS-08_CW19: docsDev mibs not set corrected w/ CL config file
CSCdv50045	ETH-01_CW19: 10th ip filter not translated to an ACL entry
CSCdu82175	CVA122; problem with security command dwnld via DOCSIS and/or ios.tx
CSCdu27827	CM CMAC_LOG_OUTPUT_STUCK when CMTS clear IP route *
CSCdv45674	Blue & ubr925: Spurious memory access occurs when booting

Open Caveats—Release 12.2(2)XA1

This section documents possible unexpected behavior by Cisco IOS Release 12.2(2)XA1, and describes only severity 1 and 2 caveats and select severity 3 caveats.

Table 8 *Open Caveats for Release 12.2(2)XA1*

Caveat ID Number	Description
CSCdr48095	SNMP Copy with erase to bootflash erases flash
CSCdu32179	firewall dest inspec not working
CSCdu46795	MAC-14_ECW4: Mib sets in docsis config file ignored if upgrade fails

Table 8 *Open Caveats for Release 12.2(2)XA1 (continued)*

Caveat ID Number	Description
CSCdu48008	CMAC Control process memory leak w/ c0 interface reset
CSCdu56484	UBR925: SEGV is USB code
CSCdu27827	CM CMAC_LOG_OUTPUT_STUCK when CMTS clear IP route *
CSCdu50598	ubr925: If BPI ena, fails to get TOD and read config file on restart
CSCds17134	Slow SNMP Memory leak, not docsis specific

Closed or Resolved Caveats—Release 12.2(2)XA1

Table 9 *Closed or Resolved Caveats for Release 12.2(2)XA1*

Caveat ID Number	Description
CSCdu32179	firewall dest inspec not working

Open Caveats—Release 12.2(2)XA

This section documents possible unexpected behavior by Cisco IOS Release 12.2(2)XA, and describes only severity 1 and 2 caveats and select severity 3 caveats.

Table 10 *Open Caveats for Release 12.2(2)XA*

Caveat ID Number	Description
CSCdr48095	SNMP Copy with erase to bootflash erases flash
CSCdu32179	firewall dest inspec not working
CSCdu46795	MAC-14_ECW4: Mib sets in docsis config file ignored if upgrade fails
CSCdu48008	CMAC Control process memory leak w/ c0 interface reset
CSCdu56484	UBR925: SEGV is USB code
CSCdu27827	CM CMAC_LOG_OUTPUT_STUCK when CMTS clear IP route *
CSCdu50598	ubr925: If BPI ena, fails to get TOD and read config file on restart
CSCds17134	Slow SNMP Memory leak, not docsis specific

Closed or Resolved Caveats—Release 12.2(2)XA

Table 11 *Closed or Resolved Caveats for Release 12.2(2)XA*

Caveat ID Number	Description
CSCdt43223	MAX-CPE parameter in the DOCSIS configuration file
CSCdt01374	Display the version number of the USB driver running on the PC
CSCdu01820	MGCP: After embedded RQNT is sent next call did not get dial tone

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 33](#)
- [Platform-Specific Documents, page 34](#)
- [Feature Modules, page 34](#)
- [Feature Navigator, page 34](#)
- [Cisco IOS Software Documentation Set Contents, page 35](#)

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.

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

Feature Navigator is a web-based tool that enables you to quickly determine which Cisco IOS software images support a particular set of features and which features are supported in a particular Cisco IOS image.

Feature Navigator is available 24 hours a day, 7 days a week. To access Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, e-mail the Contact Database Administration group at cdbadmin@cisco.com. If you do not have an account on Cisco.com, go to <http://www.cisco.com/register> and follow the directions to establish an account.

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

Feature Navigator is updated when major Cisco IOS software releases and technology releases occur. It contains feature information about mainline-, T-, S-, and P-trains. You can access Feature Navigator 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
<ul style="list-style-type: none"> Cisco IOS Configuration Fundamentals Configuration Guide Cisco IOS Configuration Fundamentals Command Reference 	Cisco IOS User Interfaces File Management System Management
<ul style="list-style-type: none"> 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
<ul style="list-style-type: none"> 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
<ul style="list-style-type: none"> <i>Cisco IOS Interface Configuration Guide</i> <i>Cisco IOS Interface Command Reference</i> 	LAN Interfaces Serial Interfaces Logical Interfaces

Table 12 Cisco IOS Release 12.2 Documentation Set (continued)

Books	Major Topics
<ul style="list-style-type: none"> • 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
<ul style="list-style-type: none"> • Cisco IOS AppleTalk and Novell IPX Configuration Guide • Cisco IOS AppleTalk and Novell IPX Command Reference 	AppleTalk Novell IPX
<ul style="list-style-type: none"> • 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
<ul style="list-style-type: none"> • Cisco IOS Voice, Video, and Fax Configuration Guide • <i>Cisco IOS Voice, Video, and Fax Command Reference</i> 	Voice over IP Call Control Signaling Voice over Frame Relay Voice over ATM Telephony Applications Trunk Management Fax, Video, and Modem Support
<ul style="list-style-type: none"> • Cisco IOS Quality of Service Solutions Configuration Guide • <i>Cisco IOS Quality of Service Solutions Command Reference</i> 	Packet Classification Congestion Management Congestion Avoidance Policing and Shaping Signaling Link Efficiency Mechanisms
<ul style="list-style-type: none"> • Cisco IOS Security Configuration Guide • <i>Cisco IOS Security Command Reference</i> 	AAA Security Services Security Server Protocols Traffic Filtering and Firewalls IP Security and Encryption Passwords and Privileges Neighbor Router Authentication IP Security Options Supported AV Pairs
<ul style="list-style-type: none"> • 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

Table 12 Cisco IOS Release 12.2 Documentation Set (continued)

Books	Major Topics
<ul style="list-style-type: none"> • Cisco IOS Wide-Area Networking Configuration Guide • Cisco IOS Wide-Area Networking Command <i>Reference</i> 	ATM Broadband Access Frame Relay SMDS X.25 and LAPB
<ul style="list-style-type: none"> • Cisco IOS Mobile Wireless Configuration Guide • Cisco IOS Mobile Wireless Command Reference 	General Packet Radio Service
<ul style="list-style-type: none"> • Cisco IOS Terminal Services Configuration Guide • Cisco IOS Terminal Services Command Reference 	ARA LAT NASI Telnet TN3270 XRemote X.28 PAD Protocol Translation
<ul style="list-style-type: none"> • <i>Cisco IOS Configuration Guide Master Index</i> • <i>Cisco IOS Command Reference Master Index</i> • Cisco IOS Debug Command Reference • Cisco IOS Software System Error Messages • <i>New Features in 12.2 T-Based Limited Lifetime Releases</i> • 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 provide sources for obtaining documentation from Cisco Systems.

World Wide Web

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

- <http://www.cisco.com>
- <http://www-china.cisco.com>
- <http://www-europe.cisco.com>

Documentation CD-ROM

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

Ordering Documentation

Cisco documentation is available in the following ways:

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

Documentation Feedback

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

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

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

Attn Document Resource Connection
Cisco Systems, Inc.
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. For Cisco.com registered users, additional troubleshooting tools are available from the TAC website.

Cisco.com

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

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

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

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

<http://www.cisco.com>

Technical Assistance Center

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

Contacting TAC by Using the Cisco TAC Website

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

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

P3 and P4 level problems are defined as follows:

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

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

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

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

If you cannot resolve your technical issue by using the TAC online resources, Cisco.com registered users can open a case online by using the TAC Case Open tool at the following website:

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

Contacting TAC by Telephone

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

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

P1 and P2 level problems are defined as follows:

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

This document is to be used in conjunction with the documents listed in the [“Related Documentation” section on page 33](#).

AccessPath, AtmDirector, Browse with Me, CCIP, CCSI, CD-PAC, *CiscoLink*, the Cisco *Powered* Network logo, Cisco Systems Networking Academy, the Cisco Systems Networking Academy logo, Cisco Unity, Fast Step, Follow Me Browsing, FormShare, FrameShare, IGX, Internet Quotient, IP/VC, iQ Breakthrough, iQ Expertise, iQ FastTrack, the iQ Logo, iQ Net Readiness Scorecard, MGX, the Networkers logo, ScriptBuilder, ScriptShare, SMARTnet, TransPath, Voice LAN, Wavelength Router, and WebViewer are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and Discover All That's Possible are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, FastHub, FastSwitch, GigaStack, IOS, IP/TV, LightStream, MICA, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, SlideCast, StrataView Plus, Stratm, SwitchProbe, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0110R)

Copyright © 2001, Cisco Systems, Inc.
All rights reserved.

