



Release Notes for Cisco uBR924 Cable Access Router for Cisco IOS Release 12.1(5)T

November 27, 2000
Part Number: OL-0385-04 Rev.B0



Note

You can find the most current Cisco IOS documentation on Cisco Connection Online (CCO). These electronic documents may contain updates and modifications made after this document was published.

These release notes for the Cisco uBR924 Cable Access Router describe the enhancements provided in Cisco IOS Release 12.1(5)T. 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 12.1(5)T, see the “Caveats” section on page 26 and *Caveats for Cisco IOS Release 12.1 T*. The caveats document is updated for every maintenance release and is located on Cisco Connection Online (CCO) and the Documentation CD-ROM.

Use these release notes with *Cross-Platform Release Notes for Cisco IOS Release 12.1 T*, located on CCO and the Documentation CD-ROM.



Note

Cisco IOS Release 12.1 T does not support the Cisco uBR904 Cable Access Router, which is an end-of-life (EOL) product. However, Cisco IOS Release 12.1 images do support the Cisco uBR904 router and include the current caveat fixes.

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 © 2000. Cisco Systems, Inc. All rights reserved.

OL-0385-04 Rev. B0 (2/2001)

- Limitations and Restrictions, page 18
- Important Notes, page 20
- Caveats, page 26
- Related Documentation, page 34
- Obtaining Documentation, page 39
- Obtaining Technical Assistance, page 40

Introduction

The DOCSIS-based Cisco uBR924 Cable Access Router gives residential or small office/home office (SOHO) subscribers high-speed Internet or Intranet access. The Cisco uBR924 Cable Access Router supports both data traffic and packet voice and fax traffic via a shared two-way cable system and Internet Protocol (IP) backbone network. The Cisco uBR924 Cable Access Router connects computers and other customer premises devices at a subscriber site to the service provider's cable, hybrid-fiber coaxial (HFC), and IP backbone network.

The Cisco uBR924 Cable Access Router is based on Data-over-Cable Service Interface Specifications (DOCSIS) and interoperates with any bidirectional, DOCSIS-qualified cable modem termination system (CMTS). The Cisco uBR924 Cable Access Router ships from the Cisco factory with a Cisco IOS software image stored in nonvolatile Flash memory that supports DOCSIS-compliant bridging data operations. The Cisco uBR924 Cable Access Router functions as a cable modem at the subscriber site to convey data communications on the cable television system.

**Note**

For information on new features and Cisco IOS commands supported by Release 12.1 T, see the “New and Changed Information” section on page 10 and the “Related Documentation” section on page 34.

Based on the feature licenses your company purchased, other Cisco IOS images can be downloaded from Cisco Connection Online (CCO). Special operating modes, based on your service offering and the practices in place for your network, can be supported for the Cisco uBR924 router, based on the available images in Cisco IOS Release 12.1(5)T. The Cisco uBR924 Cable Access Router can also function as an advanced router, providing wide-area network (WAN) data connectivity in a variety of configurations.

**Note**

All Cisco uBR924 Cable Access Router images support DOCSIS Baseline Privacy Interface (BPI) encryption. BPI is subject to export restrictions.

Cisco uBR924 Cable Access Router

The Cisco uBR924 Cable Access Router features a single F-connector interface to the cable system, four RJ-45 (10BaseT Ethernet) hub ports, two RJ-11 Foreign Exchange Station (FXS) voice ports, one RJ-11 port for an optional backup analog telephone line connection, and one RJ-45 console port to connect to a laptop computer/console terminal for local Cisco IOS configuration. The Cisco uBR924 Cable Access Router supports voice and data Cisco IOS software images; available feature sets include Easy IP, Firewall Phase II (Cisco Secure Integrated Software), and IP security (IPSec).

Early Deployment Releases

These release notes describe the Cisco uBR924 Cable Access Router for Cisco IOS Release 12.1(5)T, which is an early deployment (ED) release based on Cisco IOS Release 12.1. Early deployment releases contain fixes for software caveats and support for new Cisco hardware and software features.

Table 1 shows recent early deployment releases of the Cisco uBR924 Cable Access Router:

Table 1 Early Deployment Releases for the Cisco uBR924 Cable Access Router



ED Release	Maintenance Release	Additional Software Features	Availability
Release 12.1 T	(5)	<ul style="list-style-type: none"> NAT¹—Support for NetMeeting Directory (Internet Locator Service—ILS) Parser Cache 	Now
	(3a)	<ul style="list-style-type: none"> HSRP² Support for ICMP³ Redirect Media Gateway Control Protocol Residential Gateway Support Secure Shell (SSH) Version 1 Client Support Support for the ip address dhcp command XGCP⁴ MIB⁵ support for both the MGCP and SGCP⁶ protocols 	Now
	(2)	<ul style="list-style-type: none"> Configurable H.225 Timers Ecosystem Gatekeeper Interoperability Enhancements, Phase 2 H.323 Support for Virtual Interfaces RFC 2233 support for link up/down traps and for the IF-MIB MIB 	Now
Release 12.1 T	(1)	<ul style="list-style-type: none"> Cable Monitor Web Diagnostics Tool Cisco Cable Clock Card Support DOCSIS 1.0+ Extensions—Dynamic Multi-SID⁷ Assignment and Concatenation Dynamic Host Configuration Protocol (DHCP) Proxy Support Ecosystem Gatekeeper Interoperability Enhancements H.323 Enhancements Secure Shell Server (SSH) Support SNMP⁸ Enhancements <p> Note Release 12.1 T also includes the features from Release 12.0 T and Release 12.0(7)XR.</p>	Now

Table 1 Early Deployment Releases for the Cisco uBR924 Cable Access Router (continued)

ED Release	Maintenance Release	Additional Software Features	Availability
Release 12.0 XR1	(7)	<ul style="list-style-type: none"> • DOCSIS 1.0+ Extensions—Dynamic Multi-SID Assignment and Concatenation • VPN⁹ Enhancements—Dynamic Crypto Map • NetRanger Support—Cisco IOS Intrusion Detection • Firewall (Phase II)—Cisco Secure Integrated Software • SGCP 1.1 and SGCP MIB 	Now
Release 12.0 XR	(7)	<ul style="list-style-type: none"> • DOCSIS 1.0+ Extensions—Dynamic Multi-SID Assignment and Concatenation <p> Note Excludes VPN, Firewall (Phase II) and Triple DES¹⁰ found in 12.0(7)T.</p>	Now
Release 12.0 T	(7)	<ul style="list-style-type: none"> • VPN Enhancements—Dynamic Crypto Map • NetRanger Support—Cisco IOS Intrusion Detection • Firewall (Phase II)—Cisco Secure Integrated Software • SGCP 1.1 and SGCP MIB 	Now
	(5)	<ul style="list-style-type: none"> • Fax support over the cable network • Advanced data feature sets: <ul style="list-style-type: none"> – DOCSIS Baseline Privacy (BPI) – IPSec—56-bit encryption/decryption at network layer (Phase I) – 3DES—Triple DES (Phase I): 168-bit encryption/decryption at network layer (Phase I) – L2TP—Layer 2 tunneling protocol (Phase I) – Firewall (Phase I)—Cisco Secure Integrated Software • Enhanced VoIP¹¹ feature integration • Enhanced bridging functionality 	Now
Release 12.0 XI1	(4)	<ul style="list-style-type: none"> • Full and DOCSIS-compliant bridging • Network address translation and port address translation (NAT¹²/PAT¹³) • Radio frequency interface • Routing (RIP V2¹⁴) 	Now

1. NAT = Network Address Translation
 2. HSRP = Hot Standby Router Protocol
 3. ICMP = Internet Control Message Protocol
 4. XGCP is meant to represent both Simple Gateway Control Protocol and Media Gateway Control Protocol.
 5. MIB = Management Information Base
 6. SGCP = Simple Gateway Control Protocol

7. SID = Service ID
8. SNMP = Simple Network Management Protocol
9. VPN = Virtual Private Network
10. DES = Data Encryption Standard
11. VoIP = Voice over Internet Protocol
12. NAT = Network Address Translation
13. PAT = Port Address Translation
14. RIP V2 = Routing Information Protocol version 2

System Requirements

This section describes the system requirements for Cisco IOS Releases 12.1(5)T:

- Memory Recommendations, page 5
- Headend Interoperability, page 6
- Hardware Supported, page 7
- Determining the Software Version, page 8
- Upgrading to a New Software Release, page 8
- Feature Set Tables, page 8

Memory Recommendations

Table 2 lists the memory recommendations for each of the feature sets available for the Cisco uBR924 Cable Access Router in Cisco IOS Release 12.1(5)T. The image subset legend for Table 2 is as follows:

- y5=Reduced IP image with Easy IP functionality (PAT/NAT/DHCP server)
- v4=Voice set
- o3=Firewall (Phase II) feature set
- k1=DOCSIS baseline privacy
- 56i=56-bit IPsec
- k2=Triple DES IPsec (Phase I)

Table 2 *Memory Recommendations for the Cisco uBR924 Cable Access Router, Release 12.1(5)T Feature Sets*

Feature Set Matrix Term ¹	Image Name	Minimum Flash Memory	Minimum DRAM Memory	Runs From
Home Office with Voice—Base image with Easy IP and Voice	ubr920-k1v4y5-mz	4 MB Flash	16 MB DRAM	RAM
Value Telecommuter—Easy IP, Voice, and IPsec 56	ubr920-k1v4y556i-mz	4 MB Flash	16 MB DRAM	RAM
Performance Telecommuter—Easy IP, Voice, and IPsec 3DES	ubr920-k1k2v4y5-mz	4 MB Flash	16 MB DRAM	RAM

Table 2 *Memory Recommendations for the Cisco uBR924 Cable Access Router, Release 12.1(5)T Feature Sets (continued)*

Feature Set Matrix Term ¹	Image Name	Minimum Flash Memory	Minimum DRAM Memory	Runs From
Value Small Office—Easy IP, Voice, FW ² , and IPSec 56	ubr920-k1o3v4y556i-mz	4 MB Flash	16 MB DRAM	RAM
Performance Small Office—Easy IP, Voice, FW ² , and IPSec 3DES	ubr920-k1k2o3v4y5-mz	4 MB Flash	16 MB DRAM	RAM

1. L2TP is not supported in any Cisco IOS Release 12.1(5)T images for the Cisco uBR924 Cable Access Router.

2. FW—Firewall (Cisco Secure Integrated Software)



Note

Cisco IOS Release 12.1 T supports fewer software images for the Cisco uBR924 Cable Access Router than Release 12.0 (which supported 14 separate images). The new simplified set of software images are a superset of the images supported in the previous releases, allowing for an easy upgrade path from Release 12.0 to Release 12.1. All of the images shown in Table 2 support both the Easy IP and Voice feature sets; the IPSec and Firewall feature sets are supported as shown.

Headend Interoperability

Cisco Cable Clock Card Support

When using Cisco IOS Release 12.1(1)T or greater, the Cisco uBR924 Cable Access Router automatically supports the Cisco Cable Clock Card feature for voice traffic when the CMTS is a Cisco uBR7200 series universal broadband router with the Cisco Cable Clock Card feature.

DOCSIS Concatenation

If using DOCSIS concatenation with a 16-QAM (quadrature amplitude modulation) symbol rate, 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. See caveats CSCdp76415 and CSCdp92139 on page 31 for more detail.

DOCSIS 1.0+ Extensions

Cisco IOS Release 12.1 T 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, both the Cisco uBR924 router and the CMTS router must support them. If you are using the Cisco uBR7200 series headend equipment as the CMTS router, Cisco IOS Release 12.0(7)XR, Release 12.1(1)T, or greater is required on both the Cisco uBR924 Cable Access Router and the CMTS router to ensure that these features are activated.

To configure the Cisco uBR924 Cable Access Router 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. 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 traffic.

IPSec Encryption Support

To use IPSec encryption, both the Cisco uBR924 Cable Access Router 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, 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 uBR924 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 Cisco uBR924 Cable Access Router and the CMTS. To use BPI encryption, both the Cisco uBR924 Cable Access Router and the CMTS must support and enable BPI encryption.

Voice Protocol Support

When using a voice-enabled Cisco IOS Release 12.1 image, the Cisco uBR924 Cable Access Router can packetize and transport voice in compliance with the H.323 protocol. H.323v2 is integrated in Cisco gatekeeper/gateway products, such as the Cisco 2600 series and Cisco 3600 series, using Cisco IOS Release 12.0(5)T. The gatekeeper must be running Cisco IOS Release 12.0(5)T or greater to support registration of the full E.164 address for each Cisco uBR924 Cable Access Router voice port.

The Cisco uBR924 Cable Access Router also supports the Simple Gateway Control Protocol (SGCP) when using voice-enabled Cisco IOS Release 12.1 images. SGCP is an alternative to the H.323 protocol that provides signaling and feature negotiation via a remote Call Agent. SGCP eliminates the need for a dial plan mapper. It also eliminates the need for static configuration on the router to map IP addresses to telephone numbers because this function is provided by the remote Call Agent.

Hardware Supported

The Cisco uBR924 Cable Access Router contains the following interfaces:

- A single F-connector interface to the cable system.
- Four RJ-45 (10BaseT Ethernet) hub ports to connect:
 - Up to 254 computers directly to the four Ethernet hub ports at the rear of the Cisco uBR924 router when operating in bridging mode. When operating in routing mode, all four Ethernet hub ports can be connected directly to four computers.



Note For releases earlier than Cisco IOS Release 12.0(5)T—not 12.1(5)T but 12.0(5)T—the four Ethernet hub ports only support a maximum of three computers when operating in bridging mode. (The maximum of three computers is for all four ports together— not three computers per port).

- One of the four Ethernet hub ports at the rear of the Cisco uBR924 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.
- Two RJ-11 Foreign Exchange Station (FXS) ports connect telephones and fax devices to the cable system and IP backbone; the router ships from the Cisco factory with the voice ports enabled. The FXS ports on the Cisco uBR924 router can be connected to analog telephones or fax machines but cannot be used for private branch exchange (PBX) extensions.
- One RJ-11 port connects to a standard, analog telephone line (optional) to provide a backup plain old telephone service (POTS) connection to the Public Switched Telephone Network (PSTN). The backup port becomes operational if the Cisco uBR924 router loses power or its connection to the cable network.
- One RJ-45 console port (optional) to connect to a laptop computer or console terminal when locally configuring the Cisco uBR924 router; the router ships from the Cisco factory with the console port enabled.

Determining the Software Version

To determine the version of Cisco IOS software running on your Cisco uBR924 Cable Access Router, log into the Cisco uBR924 Cable Access Router and enter the **show version EXEC** command:

For the Cisco uBR924 Cable Access Router:

```
router# show version
Cisco Internetwork Operating System Software
IOS (tm) 920 Software (ubr920-k1v4y5-mz), Version 12.1(5)T, 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 CCO at:

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

For other information about upgrading to Cisco IOS Release 12.1, see the product bulletin *Cisco IOS Software Release 12.1 Upgrade Paths and Packaging Simplification* on CCO at:

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

Under **Cisco IOS 12.1**, click **Cisco IOS Software Release 12.1 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 voice and data software images by feature sets for the Cisco uBR924 Cable Access Router. This table uses the following conventions:

- Yes—The feature is supported in the feature set.
- No—The feature is not supported in the feature set.

**Note**

These feature set tables might contain a selected list of features. These tables might not be cumulative—nor do they list all the features in each image.

Table 3 Feature List by Feature Set for the Cisco uBR924 Cable Access Router—Voice and Data

Features	Software Images by Feature Set Matrix Term				
	Home Office with Voice	Value Telecommuter	Performance Telecommuter	Value Small Office	Performance Small Office
Baseline Privacy Interface (BPI) Encryption	Yes	Yes	Yes	Yes	Yes
Baseline Privacy Interface (BPI) MIB	Yes	Yes	Yes	Yes	Yes
Cable Device MIB (RFC 2669)	Yes	Yes	Yes	Yes	Yes
Cable Monitor	Yes	Yes	Yes	Yes	Yes
Firewall (Cisco Secure Integrated Software)	No	No	No	Yes	Yes
Cisco Standard MIBs	Yes	Yes	Yes	Yes	Yes
Cisco Voice MIBs	Yes	Yes	Yes	Yes	Yes
Configurable H.225 Timers	Yes	Yes	Yes	Yes	Yes
DHCP Proxy Support	Yes	Yes	Yes	Yes	Yes
DOCSIS 1.0+ Extensions (Dynamic multi-SID assignment and concatenation)	Yes	Yes	Yes	Yes	Yes
DOCSIS-Compliant Bridging	Yes	Yes	Yes	Yes	Yes
Easy IP	Yes	Yes	Yes	Yes	Yes
Ecosystem Gatekeeper Interoperability Enhancements	Yes	Yes	Yes	Yes	Yes
HSRP Support for ICMP Redirect	Yes	Yes	Yes	Yes	Yes
H.323v2 Protocol	Yes	Yes	Yes	Yes	Yes
H.323 Support for Virtual Interfaces	Yes	Yes	Yes	Yes	Yes
IPSec Encryption with 56-bit DES	No	Yes	Yes	Yes	Yes
IPSec Encryption with Triple DES (3DES)	No	No	Yes	No	Yes

Table 3 Feature List by Feature Set for the Cisco uBR924 Cable Access Router—Voice and Data (continued)

Features	Software Images by Feature Set Matrix Term				
	Home Office with Voice	Value Telecommuter	Performance Telecommuter	Value Small Office	Performance Small Office
Layer 2 Tunneling Protocol (L2TP) ¹	No	No	No	No	No
Media Gateway Control Protocol (MGCP) Residential Gateway Support	Yes	Yes	Yes	Yes	Yes
NAT—Support for NetMeeting Directory (Internet Locator Service—ILS)	Yes	Yes	Yes	Yes	Yes
Parser Cache	Yes	Yes	Yes	Yes	Yes
RFC 2233 Support	Yes	Yes	Yes	Yes	Yes
Radio Frequency Interface MIB (RFC 2670)	Yes	Yes	Yes	Yes	Yes
Routing (RIP V2)	Yes	Yes	Yes	Yes	Yes
Secure Shell (SSH)—56-bit encryption	Yes	Yes	Yes	Yes	Yes
Secure Shell (SSH)—3DES encryption	No	No	Yes	No	Yes
Simple Gateway Control Protocol (SGCP)	Yes	Yes	Yes	Yes	Yes
XGCP MIB	Yes	Yes	Yes	Yes	Yes

1. The L2TP feature set is not supported in any Cisco IOS Release 12.1(3a)T1 images for the Cisco uBR924 Cable Access Router.

New and Changed Information

The following sections list the new hardware and software features supported by the Cisco uBR924 Cable Access Router.

No New Hardware Features in Release 12.1(5)T

Cisco IOS Release 12.1(5)T does not contain any new hardware features for the Cisco uBR924 Cable Access Router.

New Software Features in Release 12.1(5)T

The following new software features are supported by the Cisco uBR924 Cable Access Router for Cisco IOS Release 12.1(5)T.

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 command-line interface (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.

The parser cache is enabled by default on all platforms using Cisco IOS Release 12.1(5)T or later. A new global configuration command, **[no] parser cache**, allows the disabling or reenabling of this feature.

No New Hardware Features in Release 12.1(3a)T1

Cisco IOS Release 12.1(3a)T1 does not contain any new hardware features for the Cisco uBR924 Cable Access Router.

New Software Features in Release 12.1(3a)T1

The following new software features are supported by the Cisco uBR924 Cable Access Router for Cisco IOS Release 12.1(3a)T1.

IP Address Negotiation

Cisco IOS Release 12.1(3a)T1 for Cisco uBR900 series Cable Access Routers adds support for the **ip address dhcp** command on the cable interface. Previous releases used the **ip address negotiated** command for this purpose, but this command is now reserved for serial interfaces. This change is cosmetic only and does not change how the router obtains its IP address. See the “IP Address Negotiation” section on page 18 for additional information.

HSRP Support for ICMP Redirects (CSCdp37610)

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

When running HSRP, it is important to prevent hosts from discovering the interface (or real) Media Access Control (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.

Media Gateway Control Protocol Residential Gateway Support

Cisco IOS Release 12.1(3a)T1 for the Cisco uBR924 Cable Access Router supports version 0.1 of the Media Gateway Control Protocol (MGCP), a proposed IETF voice control protocol that is intended to eventually supersede the existing SCGP 1.1 protocol. The MGCP 0.1 and SGCP 1.1 protocols have been merged on the Cisco uBR924 router so that the router can respond efficiently to either protocol.

The Cisco uBR924 Cable Access Router functions as a Residential Gateway, providing an interface between analog FXS phone or fax systems and the Voice over IP (VoIP) network. The Residential Gateway uses a Trunking Gateway to contact the call agent, which in turn provides access to the public telephone switched network (PTSN).

The Cisco uBR924 Cable Access Router supports both call waiting and caller ID when using either MGCP or SGCP for call control. Each of the two voice ports on the Cisco uBR924 router can be configured with the IP address for a default call agent. SNMP management of both the MGCP and SNMP protocols is provided by a single MIB (XGCP-MIB).



Note

This feature is described in detail in the *Media Gateway Control Protocol Version 12.1.3 T* feature module, available on CCO and the Documentation CD-ROM.

Secure Shell Version 1 Client Support

Cisco IOS Release 12.1(3a)T1 enhances the router's support for the Secure Shell (SSH) protocol, which was introduced in Cisco IOS Release 12.1(1)T (see the "Secure Shell Server Support" section on page 16). SSH connections use encryption and user authentication to establish a secure communications channel over an insecure network, such as the Internet.

In Cisco IOS Release 12.1(3a)T1, SSH support now includes the following features:

- SSH server support enables users to use an SSH connection to log in to the Cisco uBR924 router.
- SSH client support enables a user logged in to the Cisco uBR924 Cable Access Router 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.



Note

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 CCO and the Documentation CD-ROM.

No New Hardware Features in Release 12.1(2)T

Cisco IOS Release 12.1(2)T does not contain any new hardware features for the Cisco uBR924 Cable Access Router.

New Software Features in Release 12.1(2)T

The following new software features are supported by the Cisco uBR924 Cable Access Router for Cisco IOS Release 12.1(2)T. For more information on these features, see the documentation listed in the “Related Documentation” section on page 34.

Configurable H.225 Timer

In previous Cisco IOS releases, the H.225 Transmission Control Protocol (TCP) connection timeout timer was fixed at 15 seconds. Cisco IOS Release 12.1(2)T adds the ability to configure this timer to a value between 1–30 seconds, or to disable it entirely.



Note

For more information on this feature, see the *Configuring the Configurable Timers in H.225* feature module, available on CCO and the Documentation CD-ROM.

Ecosystem Gatekeeper Interoperability Enhancements, Phase 2

This feature enhances the existing Ecosystem Gatekeeper Interoperability Enhancements feature to improve the ability of voice gateways to move between gatekeepers upon a failure or an outage. In addition to the existing features, phase 2 adds support for the alternate gatekeeper field (altGKInfo) to the admission rejection message. This allows a gateway to move between gatekeepers during the admission request phase.

Phase 2 of this feature is introduced in Cisco IOS Release 12.1(2)T.



Note

For more information on this feature, see the *Ecosystem Gatekeeper Interoperability Enhancements, Phase 2* feature module, available on CCO and the Documentation CD-ROM.

H.323 Support for Virtual Interfaces

Cisco IOS Release 12.1(2)T for the Cisco uBR924 Cable Access Router introduces a new interface command to control the IP address used for outgoing H.323 VoIP traffic:

h323-gateway voip bind srcaddr ip address

The **h323-gateway voip bind** command can be used with any interface, but its primary use is with the Cisco uBR924 router’s Ethernet interface when configuring a Virtual Private Network (VPN). In this configuration, the **h323-gateway voip bind** command configures the router so that VoIP traffic is sent and received using the IP address of the Ethernet interface (as opposed to the default behavior, which is to use the IP address of the default outgoing interface, which is the cable interface).

The **h323-gateway voip bind** command allows the enterprise network to maintain the H.323 gatekeeper and gateway in the enterprise network’s address space. Without the **h323-gateway voip bind** command, outgoing voice traffic uses the IP address of the cable interface. This requires that the H.323 gatekeeper and gateway be maintained in the cable service provider’s address space, which is not desirable if the enterprise needs to control the voice network and VPN configuration.

**Note**

The **h323-gateway voip bind** command should be used only when the Cisco uBR924 Cable Access Router is operating in routing mode. This command has no effect when the router is operating in DOCSIS bridging mode.

This feature was tracked as caveat CSCdp11931, and is introduced in Cisco IOS Release 12.1(2)T.

RFC 2233 Support

Cisco IOS Release 12.1(2)T updates the IF-MIB MIB with support for RFC 2233, which makes the previous RFC 1573 obsolete. 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.

This feature was tracked as caveats CSCdp41317 and CSCdp55546, and is introduced in Cisco IOS Release 12.1(2)T.

No New Hardware Features in Release 12.1(1)T

Cisco IOS Release 12.1(1)T does not contain any new hardware features for the Cisco uBR924 Cable Access Router.

New Software Features in Release 12.1(1)T

The following new software features are supported by the Cisco uBR924 Cable Access Router for Cisco IOS Release 12.1(1)T. For more information on these features, see the documentation listed in the “Related Documentation” section on page 34.

Cable Monitor Web Diagnostics Tool

The Cable Monitor is a web-based diagnostic tool to display the current status and configuration of the Cisco uBR924 router. 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.

The Cable Monitor is introduced in Cisco IOS Release 12.1(1)T.

Cisco Cable Clock Card Support

When using Cisco IOS Release 12.1(1)T or greater, the Cisco uBR924 Cable Access Router automatically supports the Cisco Cable Clock Card feature for voice traffic when the CMTS is a Cisco uBR7200 series universal broadband router with the Cisco Cable Clock Card feature. This feature can enhance reliability in a voice network and reduce delay and jitter in the voice traffic.

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 uBR924 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 MAC messages dynamically add, delete, and modify SIDs when needed. When a phone connected to the router is taken off-hook, the Cisco uBR924 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 uBR924 Cable Access Router 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 the Cisco uBR7200 series universal broadband router as the CMTS, Cisco IOS Release 12.0(7)XR or 12.1(1)T (or later) is required on both the Cisco uBR924 and Cisco uBR7200 series routers to use these features.

Dynamic Host Configuration Protocol Proxy Support

The Dynamic Host Configuration Protocol (DHCP) Proxy Support feature helps to automate the configuration of the Cisco uBR924 Cable Access Router in two situations:

- When the Cisco uBR924 Cable Access Router 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 CLI commands.
- 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 CLI commands.

When configured for DHCP Proxy Support, during startup the Cisco uBR924 Cable Access Router 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.

Ecosystem Gatekeeper Interoperability Enhancements

The Ecosystem Gatekeeper Interoperability Enhancements feature improves the ability of voice gateways to move between gatekeepers upon a failure or an outage. Currently, gateways can be configured to switch from their primary gatekeeper to an alternate gatekeeper if a failure or outage occurs.

However, moving gateways from one gatekeeper to another can create an imbalance in the number of gateways registered to each gatekeeper. The Ecosystem Gatekeeper Interoperability Enhancements feature helps to restore the balance by moving some of the gateways back to their proper gatekeepers after the outage has been corrected.

This feature adds support for the alternate gatekeeper field (altGKInfo) to the gatekeeper rejection and registration rejection messages. This allows a gateway to move between gatekeepers during the gatekeeper request and registration request phases.

This feature is introduced in Cisco IOS Release 12.1(1)T.



Note

For more information on this feature, see the *Ecosystem Gatekeeper Interoperability Enhancements* feature module, available on CCO and the Documentation CD-ROM.

H.323 Enhancements

Cisco IOS Release 12.1(1)T adds a number of H.323v2 features for voice support:

- Fast Connect—This H.323v2 feature allows connections for the most common types of calls to be created without establishing a separate H.245 control channel.
- H.245 Tunneling—Supports two H.245 features during a call without having to establish an H.245 channel:
 - DTMF digit relay—Dual-tone multifrequency (DTMF) tones are often used during a voice call to convey information, such as entering an account number voice-mail commands. Certain forms of compression (such as G.729 and G.723.1) might interfere with these tones, so they must be transmitted “out of band,” separated from the encoded voice stream.
 - Hookflash relay—Many types of PBX and telephone switches give a special meaning to a hookflash (quickly depressing and releasing the hook on your telephone). Because this creates a voltage change that cannot be transmitted across an IP network, the H.323 protocol can send an H.245 User Input Indication message to convey the hookflash to the remote end.

This feature is introduced in Cisco IOS Release 12.0(7)XR and Release 12.1(1)T.



Note

For information about these features, see *H.323 Version 2 Support*, available on CCO at <http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t5>.

Secure Shell Server Support

The Cisco uBR924 router supports the Secure Shell (SSH) Version 1 protocol, which allows network administrators to make a secure Telnet connection with the router. SSH 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.)

SSH client server is introduced in Cisco IOS Release 12.1(1)T.

SNMP Enhancements

Cisco IOS Release 12.1(1)T adds support for RFC 2669 and RFC 2670 to the DOCS-CABLE-DEVICE-MIB and DOCS-IF-MIB MIBs, respectively.

New Hardware Features in Release 12.1(1)

The following new hardware features are supported by the Cisco uBR924 Cable Access Router for Cisco IOS Release 12.1(1): FXS VoIP ports—V1+2 and V2—for uBR924 Cable Access Router only.

New Software Features in Release 12.1(1)

The following new software and MIB features are supported by the Cisco uBR924 Cable Access Router for Cisco IOS Release 12.1(1).

Software Features

- DOCSIS Baseline Privacy Interface (BPI)
- Easy IP—DHCP Server and NAT/PAT
- Enhanced Bridging
- Fax
- Firewall Phase I and II (Cisco Secure Integrated Software)
- Full and DOCSIS-Compliant Bridging
- IPsec Encryption (56-bit and 3DES)
- Layer 2 Tunneling Protocol
- NetRanger Support—Cisco IOS Intrusion Detection
- Routing (RIP V2)
- Simple Gateway Control Protocol (SGCP) 1.1
- Voice Support—using H.323 (V2) and SGCP protocols
- VPN Enhancement—Dynamic Crypto Map

Management Information Base (MIB) Features

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

- Radio Frequency Interface MIBs
- SGCP MIB

Limitations and Restrictions

This section describes warnings and cautions about using Cisco IOS Release 12.1(5)T software.

Bridging Support

The Cisco uBR924 Cable Access Router interoperates with DOCSIS cable networks. Cisco IOS Release 12.1 T 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 12.1(2)T has removed a number of commands from the CLI. These commands are now reserved exclusively for DOCSIS use. See the description of caveat CSCdr32984, page 32, for more details.

GRE IP Tunnels Are Not Supported

Generic routing encapsulation (GRE) IP tunnels cannot be built between two Cisco uBR924 Cable Access Routers because GRE IP tunnels are not supported in any Cisco IOS image for the Cisco uBR924 Cable Access Routers. IPsec tunnels, however, are supported when using Cisco IOS images that support IPsec encryption.

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 uBR924 Cable Access Router defaults to a configuration that uses the **ip address dhcp** command for the cable interface. It is not possible to override this setting by specifying a specific static IP address; to assign a static IP address to the Cisco uBR924 router, configure the DHCP server so that it assigns the desired IP address on the basis of the unit's MAC address. However, service providers should warn subscribers that changes in the cable network's topology—due to traffic levels, growth, or changes to the cable plant and other hardware—might still require changing the subnets and IP addresses assigned to a particular cable modem.



Note

The **ip address negotiated** command cannot be used on the cable interface because this command is reserved exclusively for the serial interface. However, in Cisco IOS Release 12.1(3a)T1 when the **ip address dhcp** command is used for cable interfaces, the configuration files still show the **ip address negotiated** command, which can generate an “invalid input” error during boot. This is only a cosmetic issue and does not affect the unit's functionality. See the description of caveat CSCdr61697, page 33, for more information.

Upgrading Software Images Using BPI

To enable BPI encryption, the Cisco uBR924 Cable Access Router must use a Cisco IOS image that supports BPI encryption. If the router's current software image 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 with IPSec Images

Access lists 100 and 101 should never be manually configured on the Cisco uBR924 Cable Access Router. Configuring these access lists with Cisco IOS Release 12.1 T images that support any form of IPSec encryption can crash the router. Use any access lists 102 through 199 instead. See the description of caveats CSCdr45850 and CSCdr46128 on page 28 for more information.

Using Multiple PCs with the Cisco uBR924 Cable Access Router

The “MAX CPE” parameter in a Cisco uBR924 Cable Access Router's DOCSIS configuration file determines how many PCs (or other customer premises equipment [CPE] devices) are supported by the Cisco uBR924 Cable Access Router. The default value for the “MAX CPE” parameter is 1, which means only one PC can be connected to the Cisco uBR924 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 Cisco uBR924 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 this would exceed the maximum number of CPE devices specified by the “MAX CPE” parameter. A similar thing would happen if a user decides to move a PC from one Cisco uBR924 router to another.

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

- If using a Cisco uBR7200 series router as the CMTS, enter the **clear cable host MAC address** command on the Cisco uBR7200 series router to remove the PC's MAC address from the router's internal address tables. The new PC will be rediscovered and associated with the correct Cisco uBR924 Cable Access Router during the next DHCP lease cycle.
- Increase the value of the “MAX CPE” parameter in the Cisco uBR924 Cable Access Router's DOCSIS configuration file so that it can accommodate the desired number of PCs. Reset the Cisco uBR924 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 uBR924 Cable Access Router 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 this could damage the switch and the router's circuitry.

Important Notes

This section contains important information about using Cisco IOS Release 12.1(5)T software.

CPE Device Filtering

In Cisco IOS Release 12.1(2)T and above, the “docsDevCpeIpMax” attribute defaults to -1 instead of the previous default of 1. 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 uBR924 Cable Access Router does 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 uBR924 Cable Access Router does not filter 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 uBR924 Cable Access Router compares 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 CPE device’s MAC address. This is controlled by the value of the “MAX CPE” parameter, which is set in the DOCSIS configuration file.
2. Link Level Control (LLC) filtering—Packets are filtered on the basis of the packet’s protocol. This is controlled by the “docsDevFilterLLCTable” table.
3. CPE IP address filtering—Packets are filtered on the basis of the CPE device’s IP address, 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 above.

Disabling the Finger Server

By default, the Cisco uBR900 series Cable Access Router enables its onboard TCP/IP “finger” server to allow remote users to query the number and identities of any users who 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 finger server’s well-known port (TCP port 79). 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.

Last Maintenance Release of Cisco IOS Release 12.1 T

The last maintenance release of the 12.1 T release train is 12.1(5)T. The migration path for customers who need bug fixes for the 12.1 T features is the 12.2 mainline release. The 12.2 mainline release has the complete feature content of 12.1 T and will eventually reach general deployment (GD).

The last maintenance release was renamed from 12.1(4)T to 12.1(5)T to synchronize with its parent software base, the 12.1(5) mainline release, and to reflect that 12.1(5)T has all the bug fixes of the 12.1(5) mainline release. The 12.1 T release train is a superset of the 12.1 mainline release; hence any defect fixed in the 12.1 mainline is also fixed in 12.1 T. The set of features for 12.1(4)T is the same as that for 12.1(5)T. There was no change in the feature content of the release. The release was renamed so that the releases would be consistent with the Cisco release process.

Supplemental and Corrected Text for the Online Feature Module

Troubleshooting Tips for the uBR924 Cable Access Router, page 15, indicates:

“Some CATV systems use alternative frequency plans such as the IRC (Incrementally Related Carrier) and HRC (Harmonically Related Carrier) plans. Most of the IRC channel slots overlap the EIA plan. The HRC plan is not supported by Cisco’s cable access routers since so few cable plants are using this plan.”

The correction should read:

“For the Cisco uBR924 Cable Access Router, both the IRC (Incrementally Related Carrier) and HRC (Harmonically Related Carrier) plans are supported. Most of the IRC channel slots overlap the EIA plan. For the Cisco uBR924 Cable Access Router, both the IRC and HRC plans are supported.

“The list of downstream search bands added for HRC have appropriate center frequencies and step values for an HRC channel plan. The expanded search band list may increase the amount of time required by the Cisco uBR924 Cable Access Router to acquire the downstream signal on the HRC channel plan, which can add to the total time for complete registration of the modem the very first time it is added to the cable system.”

Supported MIBs

The Cisco uBR924 Cable Access Router supports 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’s standard MIBs—These MIBs are common across most of Cisco’s 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.
- Cisco Voice MIBs—These MIBs are common across Cisco’s router platforms that support Voice over IP (VoIP). These MIBs provide access to voice-related parameters and statistics, including the SGCP protocol.
- 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 uBR924 Cable Access Router. They include both DOCSIS-required MIBs and Cisco-specific enterprise MIBs. If your network management applications have not already been configured for the Cisco uBR924 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 uBR924 Cable Access Router supports 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.
- “docsDevServe” group provides information about the progress of interaction with various provisioning servers.
- “docsDevEven” group provides information about the progress of reporting.
- “docsDevFilter” group configures filters at link layer and IP layer for bridge data traffic.

The Cable Device MIB is very similar to the 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 uBR924 Cable Access Router supports 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 Connection Online (CCO). From the CCO home page, click on this path: **Service & Support: Software Center: Network Mgmt Products: Cisco Network Management Toolkit: Cisco MIB**

Cisco Voice MIBs

The Cisco uBR924 Cable Access Router supports the Cisco Voice MIBs are supported, which consist of the following components:

- CISCO-VOICE-IF-MIB
- CISCO-VOICE-DIAL-CONTROL-MIB
- CISCO-VOICE-ANALOG-MIB
- CISCO-DIAL-CONTROL-MIB
- DIAL-CONTROL-MIB
- SGCP-MIB
- XGCP-MIB

Radio Frequency Interface MIBs

The Cisco uBR924 Cable Access Router supports 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:

- 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 transmitted across a public network without fear of observation, modification, or spoofing. This 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.

SGCP and MGCP MIBs

The Cisco uBR924 Cable Access Router supports the Simple Gateway Control Protocol (SGCP) and Media Gateway Control Protocol (MGCP) through a single MIB (XGCP-MIB). This MIB supports configuration, performance, and fault management of the SGCP and MGCP interfaces.

The key attributes of this MIB are as follows:

- `xgcplnBadVersions`—Number of incoming messages delivered to the protocol entity and that are for an unsupported protocol version
- `xgcpRequestTimeOut`—Timeout value used for retransmitting an unacknowledged message
- `xgcpRequestRetries`—Number of retries for a request that exceeds timeout
- `xgcpAdminStatus`—Desired state of the protocol entity
- `xgcpOperStatus`—Current operational status of the protocol entity
- `xgcpUnRecognizedPackets`—Number of unrecognized packets since reset

- `xgcpMsgStatTable`—Table that contains SGCP statistics information since reset
- `xgcpMsgStatEntry`—Row in the “`xgcpMsgStatTable`” that contains information about SGCP message statistics per IP address of the Media Gateway Controller (MGC)
- `xgcpIPAddress`—IP address of the MGC
- `xgcpSuccessMessages`—Number of successful messages that communicate with the MGC on that IP address
- `xgcpFailMessages`—Number of failed messages that communicate with the MGC on that IP address
- `xgcpUpDownNotification`—Notification sent when the protocol status changes between up and down



Note

For complete details on the SGCP and MGCP MIB, see the `XGCP-MIB.my` file on the CCO MIB web site.

Cable-Specific MIBs

Table 4 shows the cable-specific MIBs that are supported on the Cisco uBR924 Cable Access Router. This table also provides a brief description of each MIB’s 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 Cisco’s FTP site (<ftp://ftp.cisco.com/pub/mibs/>). Most MIBs are available in both SNMPv1 and SNMPv2 versions; the SNMPv1 versions have *V1SMI* as part of their filenames. Also see the Cisco MIBs home page at <http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>.

Table 4 Supported MIBs for the Cisco uBR924 Cable Access Router

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.	12.0(4)XI
SNMPv2-TC.my SNMPv2-TC-V1SMI.my	This module defines the textual conventions as specified in pages 4 and 10-11 of RFC 854.	12.0(4)XI
CISCO-SMI.my CISCO-SMI-V1SMI.my	This module specifies the SMI for Cisco’s enterprise MIBs.	12.0(4)XI
CISCO-TC.my CISCO-TC-V1SMI.my	This module defines the textual conventions used in Cisco’s enterprise MIBs.	12.0(4)XI
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 MIB-II’s <i>if</i> table, and incorporates the extensions defined in RFC 2233.	12.0(4)XI RFC 2233 support: 12.1(2)T

Table 4 Supported MIBs for the Cisco uBR924 Cable Access Router (continued)

MIB Filename	Description	Release
CISCO-CABLE-SPECTRUM-MIB.my CISCO-CABLE-SPECTRUM-MIB-V1SMI.my	This module describes the spectrum management flap list attributes.	12.0(5)T1
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.	12.0(4)XI RFC 2670 support: 12.1(1)T
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.	12.0(5)T
CISCO-DOCS-EXT-MIB.my CISCO-DOCS-EXT-MIB-V1SMI.my	This module extends the DOCSIS standard RFI MIB (DOCS-IF-MIB) with Cisco-specific extensions, such as QoS attributes and connection status and other information regarding the cable modems and CPE devices supported by the CMTS.  Note Cisco IOS releases prior to 12.0(5)T1 provide only partial support for the attributes in this MIB.	partial support: 12.0(4)XI full support: 12.0(5)T1
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.	12.0(4)XI RFC 2669 support: 12.1(1)T

**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 in the future, 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 CISCO-QUEUE-MIB-V1SMI	IF-MIB 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 uBR924 Cable Access Router.

Troubleshooting uBR Cable Modems Not Coming Online

The tech note *Troubleshooting uBR Cable Modems Not Coming Online* is available on CCO:

http://www-tac.cisco.com/Teams/esupport/Cable/troubleshooting_cm_online_from_ac.html

This tech note discusses the different states that CMs go through before coming online and establishing IP connectivity. The tech note highlights the most commonly used IOS troubleshooting commands to verify what state the CM is in and the reasons that can cause the modem to arrive at that state. This is illustrated by debugs and show commands at both the CMTS and the CM. The tech note also discusses some of steps that can be taken to arrive at the correct status, online.

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 12.1(5)T.

For more information on caveats in Cisco IOS Release 12.1 T, see the *Caveats for Cisco IOS Release 12.1 T* document. All caveats in Cisco IOS Release 12.1 are also in Cisco IOS Release 12.1 T. For information on caveats in Cisco IOS Release 12.1, see *Caveats for Cisco IOS Release 12.1*. These documents list severity 1 and 2 caveats and only selected severity 3 caveats, and are located on CCO and the Documentation CD-ROM.

**Note**

If you have an account with CCO, you can use Bug Navigator II to find caveats of any severity for any release. To reach Bug Navigator II, go to CCO 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> (you must have an account on CCO to access this site).

Open Caveats—Release 12.1(5)T

All the caveats listed in this section are open in Release 12.1(5)T:

- CSCdp03592

This caveat affects the Cisco uBR924 router when it is configured as an H.323 gateway using the following cable interface configuration commands:

- h323-gateway voip interface
- h323-gateway voip id gklocal ipaddr x.x.x.x 1719
- h323-gateway voip h323-id xxxxx@xxxx.xxx

When the Cisco uBR924 router reboots, this configuration will fail if these commands are executed before the cable interface acquires a valid IP address from the DHCP server. In this situation, the h323-gateway commands will be ignored, and voice calls that use that gateway will fail.

The workaround is to either reenter the gateway commands manually or to reload the entire configuration using the **copy start-config running-config** command.

- CSCdm38753

The Cisco uBR924 router, when running the NAT and firewall features, crashes if establishing roughly 150 Telnet sessions (using the *solaris_telnet* client). The workaround is to avoid creating that many Telnet sessions.

- CSCdm75295

The Cisco uBR924 Cable Access Router can stop responding to CMTS requests when upstreams are configured with different minislot sizes. The workaround is to configure the upstreams on the CMTS with the same minislot size.

- CSCdp03177

When running Cisco IOS Release 11.3(11)NA, the Cisco uBR924 Cable Access Router does not come up when all four downstreams are combined through the upconverter and all of the upstreams of the four cards are combined. When the Cisco uBR924 router is instructed to go to a different downstream, it obtains the correct IP address for the new downstream, but fails to update the default gateway according to the DHCP reply; it subsequently fails to obtain the time-of-day (TOD) or to download the DOCSIS configuration file. The default gateway address must be corrected manually before the router succeeds in obtaining the configuration file and in getting the current time-of-day.

- CSCdp13089 and CSCdp90276
The **voice-port cptone** command does not support the set of telephony tones used in the Czech Republic or in Switzerland. There is no workaround.
- CSCdr28707
The **show interface** command can show an impossible number of CRC errors on the cable interface when transmitting VoIP traffic. When this error occurs, the number of cyclic redundancy check (CRC) errors typically exceeds a billion errors and is greater than the total number of packets transmitted on the interface. The workaround is to use the **show interface cable 0 counters** command to display the correct number of errors.
- CSCdr45850 and CSCdr46128
The Cisco uBR924 Cable Access Router can crash when using an access list numbered 100 or 101 while running Cisco IOS Release 12.1 T images that support any form of IPSec encryption. Other access lists, however, can be used without problem.
Workaround: Do not configure access list numbers 100 and 101 for any purpose. Use access lists 102 through 199 instead.
- CSCdr74817
Using the **ip pim** interface command on the cable interface can force the Cisco uBR924 to go off-line. The workaround is to avoid enabling IP multicast on the cable interface using the **ip pim** interface command.
- CSCdr76711
Upstream performance for data traffic on a DOCSIS 1.0 cable modem is limited to approximately 1.7 megabits per second, due to the limits of using one SID for data traffic, as required by the DOCSIS 1.0 specification. This caveat cannot be resolved until the implementation of the DOCSIS 1.1 specification, which provides for multiple SIDs for data traffic. There is no workaround.
- CSCds74274
The Value Small Office image (ubr920-k1o3v4y556i-mz) should be used only if BPI is disabled; otherwise, the cable access router might reload, requiring power cycling and reconfiguration before it can come back online. There is no workaround.

Closed or Resolved Caveats—Release 12.1(5)T and Earlier Releases

All the caveats listed in this section are closed or resolved in Release 12.1(5)T:

- CSCdp04541
Previously, the Cisco uBR924 Cable Access Router would age out a CPE device's MAC address after one week of inactivity. This behavior did not conform to the DOCSIS specification, which prohibits aging out of CPE devices.
This is resolved in Cisco IOS Release 12.1(1), so that CPE devices are no longer aged out.
- CSCdp25025 and CSCdr11675
These caveats improve the Cisco uBR924 router's error handling when it does not receive a valid response from the time-of-day (ToD) server during its power-on provisioning; an error message is also displayed when a ToD failure occurs. These caveats also add support for using multiple ToD servers when the DHCP server returns a list of two or more ToD servers.
This caveat is resolved in Cisco IOS Release 12.1(1)T.

- CSCdp37677 and CSCdp38842

The DOCS-CABLE-DEVICE-MIB.my MIB has been updated to be compliant with RFC 2669, *DOCSIS Cable Device MIB Cable Device Management Information Base for DOCSIS Compliant Cable Modems and Cable Modem Termination Systems*. This includes the following changes:

The root object “docsDevMIB” has become “docsDev”. The Object Identifier (OID) for the root has changed from 83 (experimental) to 69 (mib-2).

The following attributes have been added:

- docsDevFilterPolicyStatus
- docsDevFilterPolicyPtr

The following attributes have been removed:

- docsDevFilterPolicyType
- docsDevFilterPolicyAction

The following attributes have been renamed:

Old Name	New Name
docsDevEvCount	docsDevEvCounts
docsDevFilterLLCDefault	docsDevFilterLLCUnmatchedAction
docsDevCpeMax	docsDevCpeIpMax

The following attributes were changed as noted:

Attribute	Change
docsDevSerialNumber	The syntax has changed from DisplayString to SnmpAdminString.
docsDevSwFilename	The syntax has changed from DisplayString to SnmpAdminString.
docsDevSwCurrentVers	The syntax has changed from DisplayString to SnmpAdminString.
docsDevServerConfigFile	The syntax has changed from DisplayString to SnmpAdminString.
docsDevEvText	The syntax has changed from DisplayString to SnmpAdminString.
All attributes of the RowStatus type	Values can now be changed when the row is active.
Various attributes	The syntax has changed from Integer to Integer32.
Various attributes	The syntax has changed from Display String to Octet String.
Various attributes	The syntax has changed from Octet String to Bits.

This caveat is resolved in Cisco IOS Release 12.1(1)T.

- CSCdm93891 and CSCdp39237

The DOCS-IF-MIB has been updated to support RFC 2670, *Radio Frequency (RF) Interface Management Information Base for MCNS/DOCSIS Compliant RF Interfaces*. This change is in the DOCS-IF-MIB file with a LAST-UPDATED field of “9908190000Z” or later.

The following attributes have been added:

- docsIfCmRangingTimeout
- docsIfSigQEqualizationData
- docsIfCmtsInsertInterval
- docsIfCmtsMacToCmTable

The following attributes have been added but currently return an empty string:

- docsIfSigQEqualizationData
- docsIfCmtsCmStatusUnerrored
- docsIfCmtsCmStatusCorrected
- docsIfCmtsCmStatusUncorrectable
- docsIfCmtsCmStatusSignalNoise
- docsIfCmtsCmStatusMicroreflections

The following attributes have been deleted:

- docsIfCmtsInsertionInterval
- docsIfCmRangingRespTimeout

The following attributes have been renamed:

Old Name	New Name
docsIfCmStatusInvalidRangingResp	docsIfCmStatusInvalidRangingResponses
docsIfCmStatusInvalidRegistrationResp	docsIfCmStatusInvalidRegistrationResponses
docsIfCmServiceTxExceeded	docsIfCmServiceTxExceededs
docsIfCmServiceRqExceeded	docsIfCmServiceRqExceededs

The following attributes were changed as noted:

Attribute	Change
docsIfUpChannelWidth	The maximum value has changed from 16000000 to 20000000.
docsIfSigQSignalNoise	The syntax has changed from TenthdBmV to TenthdB.
docsIfCmCapabilities	The syntax has changed from OCTET STRING to BITS.
docsIfCmtsCapabilities	The syntax has changed from OCTET STRING to BITS.
docsIfCmtsServiceQosProfile	A range has been added: (0–16383).

Attribute	Change
docsIfCmtsServiceCreateTime	The syntax has changed from TimeTicks to TimeStamp.
docsIfCmtsQosProfilePermissions	The syntax has changed from OCTET STRING to BITS.

This caveat is resolved in Cisco IOS Release 12.1(1)T.

- CSCdp41317

This caveat 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.

This caveat is resolved in Cisco IOS Release 12.1(2)T.

- CSCdp55546

This caveat updates the IF-MIB MIB with support for RFC 2233, which makes the previous RFC 1573 obsolete. This change adds the “ifCounterDiscontinuityTime” attribute and changes the “ifTableLastChange attribute”.

This caveat is resolved in Cisco IOS Release 12.1(2)T.

- CSCdp76415 and CSCdp92139

Packets can be unexpectedly dropped on the upstream channel when the Cisco uBR924 is configured to use DOCSIS concatenation and the upstream is using 16 QAM symbol rate. The workaround is to configure the CMTS for a preamble with Unique Word 16 for both the short and long data burst profile. On the Cisco uBR7200 series universal broadband routers, this can be done with the **cable modulation-profile** global configuration command, specifying “uw16” for both the long and short modulation profiles.

This caveat is resolved in Cisco IOS Release 12.1(2)T.

- CSCdp80746

The Cisco uBR924 Cable Access Router could not upgrade its software image if the fully qualified filename for the new image was longer than 48 characters. The workaround was to rename the image with a shorter filename or to move it higher in the Trivial File Transfer Protocol (TFTP) server’s directory structure so that the fully qualified pathname was shorter than 48 characters.

This caveat is resolved in Cisco IOS Release 12.1(1)T.

- CSCdp95187 and CSCdp97141

The Cisco uBR924 Cable Access Router, when running one of the Small Office feature sets, can crash with an exception when changing the running configuration. The crash occurs when using a specific configuration designed for test networks and is unlikely to occur when using configurations for real-life networks. This caveat is resolved in Cisco IOS Release 12.1(1)T.

- CSCdp97839

This caveat described a problem with GRE IP tunnels that were built between two Cisco uBR900 series Cable Access Routers, using BPI encryption. The resulting tunnels experienced intermittent operation, going down after a few minutes of use. Tunnels built using IPsec encryption were successfully used.

This caveat was closed without modification because GRE tunnels are not currently supported on any software image for the Cisco uBR924 Cable Access Routers. IPSec tunnels, however, are supported when using Cisco IOS images that support IPSec encryption.

- CSCdr11723

This caveat described a situation in which two Cisco uBR924 Cable Access Routers could no longer establish voice calls. The routers needed to be reloaded before being able to make additional voice calls.

This caveat is resolved in Cisco IOS Release 12.1(2)T.

- CSCdr32984

To comply with DOCSIS regulations that restrict access to commands that change DOCSIS parameters, the following commands have been removed from the CLI:

- **[no] cable-modem downstream saved channel**
- **[no] cable-modem fast-search**
- **[no] cable-modem downstream symbol rate**
- **[no] cable-modem transmit-power**
- **[no] cable-modem upstream preamble qpsk**

In Cisco IOS Release 12.1(2)T, these commands are now reserved exclusively for DOCSIS use.

- CSCdr36952

A defect could cause a Cisco router to crash and hang when the Cisco web server was enabled with the **ip http server** command and a browser connects to *http://<router-ip>/%%*. The defect could be exploited to produce a denial of service (DoS) attack. This fact was announced on public Internet mailing lists, which are widely read both by security professionals and by security “crackers”, and should be considered public information.

The workaround to this defect was to disable the Cisco web server with the command:

```
no ip http server
```

Alternatively, the administrator could choose to block port 80 connections to the router via access lists or other firewall methods. For further information, a Security Advisory will be posted to <http://www.cisco.com/warp/public/707/advisory.html>.

This caveat is resolved in Cisco IOS Release 12.1(2)T.



Note Although CSCdr36952 has been resolved in Release 12.1(2)T, Cisco recommends that the Cisco web server be disabled on any Cisco uBR900 series router installed in a subscriber environment using the **no ip http server** command.

- CSCdr40540

The Cisco uBR924 Cable Access Router reverses the order in which it should obtain the IP address of its default gateway from the information that the DHCP server supplies during power-on provisioning. If both the router and giaddr fields are present, the Cisco uBR924 Cable Access Router should use the value from the router field as the address for the default gateway, but instead it uses the value from the giaddr field.

This caveat is resolved in Cisco IOS Release 12.1(2)T so that the Cisco uBR924 Cable Access Router uses the router field, if present, as its default gateway. If the DHCP server does not provide the router field, the Cisco uBR924 Cable Access Router then uses the giaddr field.

- CSCdr43824

In Cisco IOS Release 12.1(2)T, if two (or more) dial-peers were configured with destination patterns terminated by T, then calls with a dial number that was completed by the # key were routed only to the first matching dial-peer, even if other dial-peers are a better match. There was no workaround.

- CSCdr61697

The Cisco uBR924 Cable Access Router defaults to using the **ip address dhcp** command to set the IP address for the cable interface during power-on provisioning. However, the start-up and running configurations show that the cable interface uses the **ip address negotiated** command instead. Because only the serial interface can use the **ip address negotiated** command, this generates an “invalid input” error during start-up. This is only a cosmetic error, however, and does not affect any functionality. There is no workaround.

This caveat is resolved in Cisco IOS Release 12.1(5)T.

- CSCdr77182

The Cisco uBR924 router can eventually crash with “out of memory” errors after making several thousand phone calls if the configuration includes the **req-qos controlled-load** dial-peer configuration command. The workaround is to remove the **req-qos controlled-load** dial-peer configuration command.

This caveat is resolved in Cisco IOS Release 12.1(5)T.

- CSCdr88376

When voice and data are both running in the Frame Relay Low Latency Queuing (FR LLQ) configuration, some of the data packets are being classified as voice. This will result in police (that is, bandwidth limit) and consequent drops for the packets in the priority queue and hence cause bad voice quality.

Workaround: Turn on process-switching on the incoming interfaces for voice and data.

This caveat is resolved in Cisco IOS Release 12.1(5)T.

- CSCdr91706 and Cisco IOS HTTP Vulnerability

A defect in multiple releases of Cisco IOS software will cause a Cisco router or switch to halt and reload if the Cisco IOS HTTP service is enabled, browsing to [http://router-ip/anytext/?/](http://router-ip/anytext?/) is attempted, and the enable password is supplied when requested. This defect can be exploited to produce a denial of service (DoS) attack.

The vulnerability, identified as Cisco bug ID CSCdr91706, affects virtually all mainstream Cisco routers and switches running Cisco IOS software releases 12.0 through 12.1, inclusive. This is not the same defect as CSCdr36952.

The vulnerability has been corrected and Cisco is making fixed releases available for free to replace all affected Cisco IOS releases. Customers are urged to upgrade to releases that are not vulnerable to this defect as shown in detail below.

This vulnerability can only be exploited if the enable password is known or not set.

You are strongly encouraged to read the complete advisory, which is available at <http://www.cisco.com/warp/public/707/ioshttpserverquery-pub.shtml>.

This caveat is resolved in Cisco IOS Release 12.1(5)T.

- CSCds24499

RIP V2 updates stop after the Cisco uBR924 router attempts a renewal of its DHCP lease, which happens at approximately the half-life of the DHCP lease.

Workaround: Restart the RIP process on the router by issuing the **no router rip** and **router rip** commands. However, this restores the RIP updates only until the next DHCP lease renewal; restarting the routing process also forces the cable interface to go down and come back up.

This caveat is resolved in Cisco IOS Release 12.1(5)T.

Related Documentation

The following sections describe the documentation available for the Cisco uBR924 Cable Access Router. These documents consist of hardware and software installation guides, Cisco IOS configuration 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 CCO and the Documentation CD-ROM.

Use these release notes with these documents:

- Release-Specific Documents, page 34
- Platform-Specific Documents, page 35
- Feature Modules, page 35
- Cisco IOS Software Documentation Set, page 36

Release-Specific Documents

The following documents are specific to Release 12.1 and are located on CCO and the Documentation CD-ROM:

- *Cross-Platform Release Notes for Cisco IOS Release 12.1*

On CCO at:

Technical Documents: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 12.1

On the Documentation CD-ROM at:

Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 12.1: Release Notes: Cross-Platform Release Notes

- Product bulletins, field notices, and other release-specific documents on CCO at:

Technical Documents

- *Caveats for Cisco IOS Release 12.1*

As a supplement to the caveats listed in these release notes, see *Caveats for Cisco IOS Release 12.1*, which contains caveats applicable to all platforms for all maintenance releases of Release 12.1.

On CCO at:

Technical Documents: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 12.1: Caveats

On the Documentation CD-ROM at:

Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS 12.1: Caveats



Note If you have an account with CCO, you can use Bug Navigator II to find caveats of any severity for any release. To reach Bug Navigator II, go to CCO 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> (you must have an account on CCO to access this site).

Platform-Specific Documents

These documents are available for the Cisco uBR924 Cable Access Router on CCO and the Documentation DC-ROM:

- *Cisco uBR924 Cable Access Router Hardware Installation Guide*
- *Cisco uBR924 Cable Access Router Software Configuration Guide*
- *Cisco uBR924 Cable Access Router Subscriber Setup Quick Start Guide*
- *Cisco uBR924 Cable Access Router Quick Start Guide (Service Provider Job Aid)*
- *Troubleshooting Tips for the Cisco uBR924 Cable Access Router*
- *Regulatory Compliance and Safety Information for the Cisco uBR924 Cable Access Router*
- *DOCSIS CPE Configurator* online help



Note The *Cisco uBR924 Cable Access Router Installation and Configuration Guide* is still available on CCO but has been made obsolete by the hardware and software guides listed above.

On CCO at:

Technical Documents: Documentation Home Page: 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, 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 CCO at:

Technical Documents: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 12.1: New Feature Documentation

On the Documentation CD-ROM at:

Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 12.1: New Feature Documentation

Cisco IOS Software Documentation Set

The Cisco IOS software documentation set consists of the Cisco IOS configuration guides, Cisco IOS command references, and several other supporting documents that are available in electronic form on the Documentation CD-ROM and CCO and in printed form on request.

Documentation Modules

Each module in the Cisco IOS documentation set consists of two books: a configuration guide and a corresponding command reference. Chapters in a configuration guide describe protocols, configuration tasks, and Cisco IOS software functionality, and contain comprehensive configuration examples. Chapters in a command reference provide complete command syntax information. Use each configuration guide with its corresponding command reference.

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

On CCO at:

Technical Documents: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 12.1: Configuration Guides and Command References

On the Documentation CD-ROM at:

Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 12.1: Configuration Guides and Command References

Release 12.1 Documentation Set

Table 6 describes the contents of the Cisco IOS Release 12.1 software documentation set, which is available in electronic form and in printed form upon request.



Note

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

On CCO at:

Technical Documents: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 12.1

On the Documentation CD-ROM at:

Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 12.1

Table 6 Cisco IOS Software Release 12.1 Documentation Set

Books	Major Topics
<ul style="list-style-type: none"> • <i>Cisco IOS Configuration Fundamentals Configuration Guide</i> • <i>Cisco IOS Configuration Fundamentals Command Reference</i> 	Configuration Fundamentals Overview Cisco IOS User Interfaces Cisco IOS File Management Cisco IOS System Management Cisco IOS User Interfaces Commands Cisco IOS File Management Commands Cisco IOS System Management Commands
<ul style="list-style-type: none"> • <i>Cisco IOS Bridging and IBM Networking Configuration Guide</i> • <i>Cisco IOS Bridging and IBM Networking Command Reference, Volume I</i> • <i>Cisco IOS Bridging and IBM Networking Command Reference, Volume II</i> 	Transparent Bridging Source-Route Bridging Token Ring Inter-Switch Link Remote Source-Route Bridging DLSw+ Serial Tunnel and Block Serial Tunnel Commands LLC2 and SDLC Commands IBM Network Media Translation Commands SNA Frame Relay Access Support Commands NCIA Client/Server Commands Airline Product Set Commands
<ul style="list-style-type: none"> • <i>Cisco IOS Dial Services Configuration Guide: Terminal Services</i> • <i>Cisco IOS Dial Services Configuration Guide: Network Services</i> • <i>Cisco IOS Dial Services Command Reference</i> 	Preparing for Dial Access Modem Configuration and Management ISDN and Signalling Configuration PPP Configuration Dial-on-Demand Routing Configuration Dial-Backup Configuration Terminal Service Configuration Large-Scale Dial Solutions Cost-Control Solutions Virtual Private Networks X.25 on ISDN Solutions Telco Solutions Dial-Related Addressing Services Dial Access Scenarios
<ul style="list-style-type: none"> • <i>Cisco IOS Interface Configuration Guide</i> • <i>Cisco IOS Interface Command Reference</i> 	Interface Configuration Overview Configuring LAN Interfaces Configuring Serial Interfaces Configuring Logical Interfaces
<ul style="list-style-type: none"> • <i>Cisco IOS IP and IP Routing Configuration Guide</i> • <i>Cisco IOS IP and IP Routing Command Reference</i> 	IP Overview IP Addressing and Services IP Routing Protocols IP Multicast
<ul style="list-style-type: none"> • <i>Cisco IOS AppleTalk and Novell IPX Configuration Guide</i> • <i>Cisco IOS AppleTalk and Novell IPX Command Reference</i> 	AppleTalk and Novell IPX Overview Configuring AppleTalk Configuring Novell IPX

Table 6 Cisco IOS Software Release 12.1 Documentation Set (continued)

Books	Major Topics
<ul style="list-style-type: none"> • <i>Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS, and XNS Configuration Guide</i> • <i>Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS, and XNS Command Reference</i> 	<ul style="list-style-type: none"> Overview Configuring Apollo Domain Configuring Banyan VINES Configuring DECnet Configuring ISO CLNS Configuring XNS
<ul style="list-style-type: none"> • <i>Cisco IOS Multiservice Applications Configuration Guide</i> • <i>Cisco IOS Multiservice Applications Command Reference</i> 	<ul style="list-style-type: none"> Multiservice Applications Overview Voice Video Broadband
<ul style="list-style-type: none"> • <i>Cisco IOS Quality of Service Solutions Configuration Guide</i> • <i>Cisco IOS Quality of Service Solutions Command Reference</i> 	<ul style="list-style-type: none"> Quality of Service Overview Classification Congestion Management Congestion Avoidance Policing and Shaping Signalling Link Efficiency Mechanisms Quality of Service Solutions
<ul style="list-style-type: none"> • <i>Cisco IOS Security Configuration Guide</i> • <i>Cisco IOS Security Command Reference</i> 	<ul style="list-style-type: none"> Security Overview Authentication, Authorization, and Accounting (AAA) Security Server Protocols Traffic Filtering and Firewalls IP Security and Encryption Configuring Passwords and Privileges Neighbor Router Authentication Configuring IP Security Options
<ul style="list-style-type: none"> • <i>Cisco IOS Switching Services Configuration Guide</i> • <i>Cisco IOS Switching Services Command Reference</i> 	<ul style="list-style-type: none"> Cisco IOS Switching Services Overview Cisco IOS Switching Paths Cisco Express Forwarding NetFlow Switching Multiprotocol Label Switching Multilayer Switching Multicast Distributed Switching Virtual LANs LAN Emulation
<ul style="list-style-type: none"> • <i>Cisco IOS Wide-Area Networking Configuration Guide</i> • <i>Cisco IOS Wide-Area Networking Command Reference</i> 	<ul style="list-style-type: none"> Introduction: Wide-Area Networking Overview Configuring ATM Configuring Frame Relay Configuring Frame Relay-ATM Interworking Configuring SMDS Configuring X.25 and LAPB

Table 6 Cisco IOS Software Release 12.1 Documentation Set (continued)

Books	Major Topics
<ul style="list-style-type: none"> • <i>Cisco IOS Configuration Master Index</i> • <i>Cisco IOS Command Reference Master Index</i> • <i>Cisco IOS Debug Command Reference</i> • <i>Cisco IOS Dial Services Quick Configuration Guide</i> • <i>Cisco IOS Software System Error Messages</i> • <i>Cisco IOS Configuration Guide Master Index</i> • <i>New Features in 12.1-Based Limited Lifetime Releases</i> • <i>New Features in Release 12.1 T</i> • Release Notes (Release note and caveat documentation for 12.1-based releases and various platforms) 	

**Note**

Cisco Management Information Base (MIB) User Quick Reference is no longer published. If you have an account with CCO, you can find the latest list of MIBs supported by Cisco. To reach the *Cisco Network Management Toolkit*, press **Login** at CCO and go to **Software Center: Network Mgmt Products: Cisco Network Management Toolkit: Cisco MIB**.

Obtaining Documentation

World Wide Web

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

Documentation CD-ROM

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

Ordering Documentation

Registered CCO users can order the Documentation CD-ROM and other Cisco Product documentation through our online Subscription Services at <http://www.cisco.com/cgi-bin/subcat/kaojump.cgi>.

Nonregistered CCO users can order documentation through a local account representative by calling Cisco's corporate headquarters (California, USA) at 408 526-4000 or, in North America, call 800 553-NETS (6387).

Obtaining Technical Assistance

Cisco provides Cisco Connection Online (CCO) as a starting point for all technical assistance. Warranty or maintenance contract customers can use the Technical Assistance Center. All customers can submit technical feedback on Cisco documentation using the Web, e-mail, a self-addressed stamped response card included in many printed documents, or by sending mail to Cisco.

Cisco Connection Online

Cisco continues to revolutionize how business is done on the Internet. Cisco Connection Online 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.

CCO's broad range of features and services helps customers and partners to streamline business processes and improve productivity. Through CCO, you will find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online support services, 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 CCO to obtain additional personalized information and services. Registered users may order products, check on the status of an order, and view benefits specific to their relationships with Cisco.

You can access CCO in the following ways:

- WWW: www.cisco.com
- Telnet: cco.cisco.com
- Modem using standard connection rates and the following terminal settings: VT100 emulation; 8 data bits; no parity; and 1 stop bit.
 - From North America, call 408 526-8070
 - From Europe, call 33 1 64 46 40 82

You can e-mail questions about using CCO to cco-team@cisco.com.

Technical Assistance Center

The Cisco Technical Assistance Center (TAC) is available to warranty or maintenance contract customers who need technical assistance with a Cisco product that is under warranty or covered by a maintenance contract.

To display the TAC web site that includes links to technical support information and software upgrades and for requesting TAC support, use www.cisco.com/techsupport.

To contact TAC by e-mail, use one of the following:

Language	E-mail Address
English	tac@cisco.com
Hanzi (Chinese)	chinese-tac@cisco.com
Kanji (Japanese)	japan-tac@cisco.com

Language	E-mail Address
Hangul (Korean)	korea-tac@cisco.com
Spanish	tac@cisco.com
Thai	thai-tac@cisco.com

In North America, TAC can be reached at 800 553-2447 or 408 526-7209. For other telephone numbers and TAC e-mail addresses worldwide, consult the following web site:
<http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml>.

Software Configuration Tips on the Cisco Technical Assistance Center Home Page

If you have a CCO login account, you can access the following URL, which contains links and tips on configuring your Cisco products:

http://www.cisco.com/kobayashi/technotes/serv_tips.shtml

This URL is subject to change without notice. If it changes, point your Web browser to CCO, press **Login**, and click on this path: **Technical Assistance Center: Technical Tips**.

The following sections are provided from the Technical Tips page:

- Configuration Cookbooks—Contains common configurations or recipes for configuring various access routes and dial technologies.
- Field Notices—Notifies you of any critical issues regarding Cisco products and includes problem descriptions, safety or security issues, and hardware defects.
- Frequently Asked Questions—Describes the most frequently asked technical questions about Cisco hardware and software.
- Hardware—Provides technical tips related to specific hardware platforms.
- Hot Tips—Describes popular tips and hints gathered from the Cisco Technical Assistance Center (TAC). Most of these documents are available from the TAC Fax-on-demand service. To reach Fax-on-demand and receive documents at your fax machine from the United States, call 888-50-Cisco (888-502-4726). From other areas, call 650-596-4408.
- Internetworking Features—Lists tips on using Cisco IOS software features and services.
- Sample Configurations—Provides actual configuration examples that are complete with topology and annotations.
- Miscellaneous—Provides other documents and technical tips.

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

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

We appreciate and value your comments.

This document is to be used in conjunction with the documents listed in the “Related Documentation” section on page 34

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

All other brands, names, or trademarks mentioned in this document or website 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. (0101R)

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