



# Release Notes for Cisco uBR900 Series for Cisco IOS Release 12.1(5)

---

**October 30, 2000**

**Part Number: OL-0384-05**

These release notes for the Cisco uBR900 series cable access router support Cisco IOS Release 12.1, up to and including Cisco IOS Release 12.1(5). These release notes are updated as needed to describe new features, memory requirements, hardware support, software deferrals, and changes to the microcode and related documents.

For a list of software caveats that apply to Release 12.1(5), see the “Caveats” section on page 25 and *Caveats for Cisco IOS Release 12.1*. The caveats document is updated for every maintenance release and is located on CCO and the Documentation CD-ROM.

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



**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.

---

## Contents

These release notes describe the following topics:

- Introduction, page 2
- System Requirements, page 3
- New and Changed Information, page 9
- Limitations and Restrictions, page 11
- Important Notes, page 12
- Caveats, page 25
- Related Documentation, page 28



---

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

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

**OL-0384-05 (10/2000)**

- Obtaining Documentation, page 34
- Obtaining Technical Assistance, page 34

## Introduction

The DOCSIS-based Cisco uBR900 series cable access routers—Cisco uBR924 and Cisco uBR904—give residential or small office/home office (SOHO) subscribers high-speed Internet or Intranet access. The Cisco uBR924 cable access router also supports both data traffic and packet telephone and fax services using a shared two-way cable system and IP backbone network. The Cisco uBR900 series 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 uBR900 series 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 uBR900 series 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 uBR900 series cable access router functions as a cable modem (CM)—a modulator/demodulator at the subscriber site that conveys data communications on the cable television system.

**Note**

---

For information on new features and Cisco IOS commands supported by Release 12.1, see the “New and Changed Information” section on page 9 and the “Related Documentation” section on page 28.

---

Based on the feature licenses your company purchased, other Cisco IOS images can be downloaded from CCO. Special operating modes, based on your service offering and the practices in place for your network, can be supported for the Cisco uBR900 series router, based on the images available in Cisco IOS Release 12.1(5). The Cisco uBR900 series 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 IOS images for the Cisco uBR900 series 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 Cisco IOS Firewall, Easy IP, Layer 2 Tunneling Protocol (L2TP), and 56-bit and 168-bit IP security (IPSec) encryption.

## Cisco uBR904 Cable Access Router

The Cisco uBR904 cable access router features a single F-connector interface to the cable system, four RJ-45 (10BaseT Ethernet) hub ports, and one RJ-45 console port to connect to a laptop computer/console terminal for local Cisco IOS configuration. The Cisco uBR904 cable access router supports data-only Cisco IOS software images; available feature sets include Firewall (Phase I), Easy IP, and 56-bit IPsec.



### Note

The Cisco uBR904 cable access router is an end-of-life (EOL) product, and is no longer available for orders as of October 1999. Software images for the Cisco uBR904 router will continue to be available until November 2000 but will not contain any new feature sets. However, software images for the Cisco uBR904 router do include current caveat fixes.

## System Requirements

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

- Memory Recommendations, page 3
- Headend Interoperability, page 5
- Hardware Supported, page 5
- Determining the Software Version, page 7
- Upgrading to a New Software Release, page 7
- Feature Set Tables, page 7

## Memory Recommendations

Table 1 lists the memory recommendations for the Cisco IOS Release 12.1 image sets for the Cisco uBR924 cable access router. Table 2 lists the memory recommendations for the Cisco IOS Release 12.1 image sets for the Cisco uBR904 cable access router.

The image subset legend for Table 1 and Table 2 is as follows:

- y5=Reduced IP image with Easy IP functionality (Dynamic Host Configuration Protocol/Network Address Translation/Port Address Translation server)
- v4=Voice set (available for Cisco uBR924 only)
- s=Plus set includes L2TP
- o=Firewall (Phase I) feature set
- o3=Firewall (Phase II) feature set
- k1=DOCSIS baseline privacy
- 56i=56-bit IPsec
- k2=Triple DES (Phase I)

**Table 1** *Memory Recommendations for the Cisco uBR924 Cable Access Router, Release 12.1(5) Feature Sets*

Feature Set Matrix Term	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, L2TP, and IPSec 56	ubr920-k1sv4y556i-mz	4 MB Flash	16 MB DRAM	RAM
Performance Telecommuter—Easy IP, Voice, L2TP, and IPSec 3DES	ubr920-k1k2sv4y5-mz	4 MB Flash	16 MB DRAM	RAM
Value Small Office—Easy IP, Voice, FW <sup>1</sup> , L2TP, and IPSec 56	ubr920-k1o3sv4y556i-mz	4 MB Flash	16 MB DRAM	RAM
Performance Small and Branch Office—Easy IP, Voice, FW <sup>1</sup> , L2TP, and IPSec 3DES	ubr920-k1k2o3sv4y5-mz	4 MB Flash	16 MB DRAM	RAM

1. FW—Cisco IOS Firewall

**Note**

Cisco IOS Release 12.1 supports fewer software images (five separate images) for the Cisco uBR924 cable access router than previous releases (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 1 support both the Easy IP and Voice feature sets; the IPSec, L2TP, and Firewall feature sets are supported as shown.

**Table 2** *Memory Recommendations for the Cisco uBR904 Cable Access Router, Release 12.1(5) Feature Sets*

Feature Set Matrix Term	Image Name	Minimum Flash Memory	Minimum DRAM Memory	Runs From
Home Office	ubr900-k1y5-mz	4 MB Flash	8 MB RAM	RAM
Small Office/FW <sup>1</sup>	ubr900-k1oy5-mz	4 MB Flash	8 MB RAM	RAM
Small Office+/FW <sup>1</sup> /IPSec 56	ubr900-k1oy556i-mz	4 MB Flash	8 MB RAM	RAM
Telecommuter/IPSec 56	ubr900-k1y556i-mz	4 MB Flash	8 MB RAM	RAM

1. FW—Cisco IOS Firewall

## Headend Interoperability

### Cisco Cable Clock Card Support

When using Cisco IOS Release 12.1(1) 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 uBR7246 VXR universal broadband router with the Cisco Cable Clock Card feature. The Cisco uBR904 cable access router does not support this feature.

### IPSec Encryption Support

To use IPSec encryption, both the Cisco uBR900 series 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 acting as an IPSec gateway.)



**Note**

---

The IPSec feature set encrypts traffic sent between endpoints, such as between two Cisco uBR900 series 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 uBR900 series cable access router and the CMTS. To use BPI encryption, both the Cisco uBR900 series cable access router and the CMTS must support and enable BPI encryption.

---

### Voice Protocol Support (Cisco uBR924 only)

When using a 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 or higher images. The gatekeeper must be running Cisco IOS Release 12.0(5)T or higher in order 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 Cisco IOS Release 12.1(5) images. SGCP is an alternative to the H.323 protocol that provides signaling and feature negotiation using a remote call agent (CA). 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

This section discusses the hardware supported by the Cisco uBR924 and Cisco uBR904 cable access routers.

### Cisco uBR924 Cable Access Router

The Cisco uBR924 cable access router contains:

- A single F-connector interface to the cable system.

- Four RJ-45 (10BaseT Ethernet) hub ports to connect the following CPE devices:
  - 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 12.1(1), 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.

## Cisco uBR904 Cable Access Router

The Cisco uBR904 cable access router contains:

- 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 12.1(1), 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 uBR904 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. (A maximum of three computers are supported in bridging mode.)
- One RJ-45 console port (optional) to connect to a laptop computer or console terminal when locally configuring the Cisco uBR900 series cable access 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 uBR900 series cable access router, log in to the Cisco uBR900 series 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), RELEASE SOFTWARE
```

### For the Cisco uBR904 cable access router:

```
router# show version
Cisco Internetwork Operating System Software
IOS (tm) 900 Software (ubr900-k1y5-mz), Version 12.1(5), 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 located 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/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 are likely to require an export license. Customer orders may be denied or subject to delay due to United States government regulations. When applicable, purchaser/user must obtain local import and use authorizations for all encryption strengths. Please contact your sales representative or distributor for more information, or send an e-mail to [export@cisco.com](mailto:export@cisco.com).

---

Table 3 lists the voice and data software images by feature sets for the Cisco uBR924 cable access router. Table 4 lists the data-only software images by feature sets for the Cisco uBR904 cable access router. These tables use 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				
	Base Image with Voice	Value Telecommuter	Performance Telecommuter	Value Small Office	Performance Small and Branch Office
Baseline Privacy Interface (BPI) Encryption	Yes	Yes	Yes	Yes	Yes
Baseline Privacy Interface (BPI) MIB <sup>1</sup>	Yes	Yes	Yes	Yes	Yes
Cable Device MIB	Yes	Yes	Yes	Yes	Yes
Cisco IOS Firewall	No	No	No	Yes	Yes
Cisco Standard MIBs	Yes	Yes	Yes	Yes	Yes
Cisco Voice MIBs	Yes	Yes	Yes	Yes	Yes
DOCSIS-Compliant Bridging	Yes	Yes	Yes	Yes	Yes
Easy IP	Yes	Yes	Yes	Yes	Yes
H.323 Protocol	Yes	Yes	Yes	Yes	Yes
IPSec Encryption 56-bit DES	No	Yes	Yes	Yes	Yes
IPSec Encryption Triple DES (3DES)	No	No	Yes	No	Yes
Layer 2 Tunneling Protocol (L2TP)	No	Yes	Yes	Yes	Yes
Radio Frequency Interface MIB	Yes	Yes	Yes	Yes	Yes
Routing (RIP V2)	Yes	Yes	Yes	Yes	Yes
Simple Gateway Control Protocol (SGCP)	Yes	Yes	Yes	Yes	Yes
SGCP MIB	Yes	Yes	Yes	Yes	Yes

1. MIB = Management Information Base

**Table 4 Feature List by Feature Set for the Cisco uBR904 Cable Access Router—Data Only**

Features	Software Images by Feature Set Matrix Term			
	Home Office	Small Office/ FW	Small Office+/ FW/IPSec 56	Telecommuter/ IPSec 56
Baseline Privacy Interface (BPI) Encryption	Yes	Yes	Yes	Yes
Baseline Privacy Interface (BPI) MIB	Yes	Yes	Yes	Yes
Cable Device MIB	Yes	Yes	Yes	Yes
Cisco IOS Firewall	No	Yes	Yes	No
Cisco Standard MIBs	Yes	Yes	Yes	Yes
DOCSIS-Compliant Bridging	Yes	Yes	Yes	Yes
Easy IP	Yes	Yes	Yes	Yes
IPSec Encryption 56-bit DES	No	No	Yes	Yes

**Table 4** Feature List by Feature Set for the Cisco uBR904 Cable Access Router—Data Only (continued)

Features	Software Images by Feature Set Matrix Term			
	Home Office	Small Office/ FW	Small Office+/ FW/IPSec 56	Telecommuter/ IPSec 56
Radio Frequency Interface MIB	Yes	Yes	Yes	Yes
Routing (RIP V2)	Yes	Yes	Yes	Yes

## New and Changed Information

This section lists the new hardware and software features supported by the Cisco uBR900 series cable access router.

### No New Hardware Features in Release 12.1(5)

Cisco IOS Release 12.1(5) does not contain any new hardware features for the Cisco uBR900 series cable access router.

### No New Software Features in Release 12.1(5)

Cisco IOS Release 12.1(5) does not contain any new software features for the Cisco uBR900 series cable access router.

### No New Hardware Features in Release 12.1(4)

Cisco IOS Release 12.1(4) does not contain any new hardware features for the Cisco uBR900 series cable access router.

### No New Software Features in Release 12.1(4)

Cisco IOS Release 12.1(4) does not contain any new software features for the Cisco uBR900 series cable access router.

### No New Hardware Features in Release 12.1(3)

Cisco IOS Release 12.1(3) does not contain any new hardware features for the Cisco uBR900 series cable access router.

### No New Software Features in Release 12.1(3)

Cisco IOS Release 12.1(3) does not contain any new software features for the Cisco uBR900 series cable access router.

## No New Hardware Features in Release 12.1(2)

Cisco IOS Release 12.1(2) does not contain any new hardware features for the Cisco uBR900 series cable access router.

## No New Software Features in Release 12.1(2)

Cisco IOS Release 12.1(2) does not contain any new software features for the Cisco uBR900 series cable access router.

## New Hardware Features in Release 12.1(1)

The following hardware feature is supported by the Cisco uBR924 router for Release 12.1(1):

- FXS VoIP ports—V1+2 and V2 (Cisco uBR924 router only)

## New Software Features in Release 12.1(1)

The following software features are supported by the Cisco uBR900 series cable access router for Release 12.1(1). For more information on these features, see the documentation listed in the “Related Documentation” section on page 28.

### Software Features

- DOCSIS Baseline Privacy Interface (BPI)
- Easy IP—Dynamic Host Configuration Protocol (DHCP) Server and Network Address Translation/Port Address Translation (NAT/PAT)
- Enhanced Bridging
- Fax (Cisco uBR924 only)
- Cisco IOS Firewall
- Full and DOCSIS-Compliant Bridging
- IPsec Encryption with 56-bit DES
- IPsec Encryption with Triple DES (3DES)
- Layer 2 Tunneling Protocol (L2TP)
- NetRanger Support—Cisco IOS Intrusion Detection
- Routing (RIP V2)
- Simple Gateway Control Protocol (SGCP) 1.1 (Cisco uBR924 only)
- Voice Support—Using H.323 (V2) and SGCP protocols (Cisco uBR924 only)
- Virtual Private Network (VPN) Enhancement—Dynamic Crypto Map

## Management Information Base (MIB) Features

- Baseline Privacy Interface (BPI) MIBs
- Cable Device MIBs
- Cisco Standard MIBs
- Cisco Voice MIBs (Cisco uBR924 only)
- Radio Frequency Interface MIBs
- SGCP MIB

## Limitations and Restrictions

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

### Access Lists 100 and 101

Access lists 100 and 101 are reserved for DOCSIS use only and should not be configured for use with IPSec encryption or any other purpose. Access lists that use any other numbers can be used without restriction.

### Bridging Support

The Cisco uBR900 series cable access router interoperates with DOCSIS cable networks. Cisco IOS Release 12.1 does not support bridging traffic across a non-DOCSIS cable network.

### Debug Commands

All **debug** commands should be used only when needed for troubleshooting and testing, and then turned off when no longer needed. Each **debug** display consumes system resources; turning on too many **debug** commands can negatively affect system performance.

### GRE IP Tunnels Are Not Supported

Generic routing encapsulation (GRE) IP tunnels cannot be built between two Cisco uBR900 series cable access routers because GRE IP tunnels are not supported in any Cisco IOS image for the Cisco uBR900 series cable access routers. IPSec tunnels, however, are supported when using Cisco IOS images that support IPSec encryption.

## Using Multiple PCs with the Cisco uBR900 Series Cable Access Router

The “MAX CPE” parameter in a Cisco uBR900 series cable access router’s DOCSIS configuration file determines how many PCs (or other customer premises equipment [CPE] devices) are supported by the Cisco uBR900 series cable access router when operating in bridging mode. The default value for the “MAX CPE” parameter is 1, which means only one PC can be connected to the Cisco uBR900 series cable access router when operating in bridging mode.

The DOCSIS 1.0 specification states that a CMTS cannot age-out Media Access Control (MAC) addresses for CPE devices, so the first PC that is connected to the Cisco uBR900 series 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 uBR900 series cable access router to another.

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

- If using a Cisco 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 uBR900 series cable access router’s DOCSIS configuration file so that it can accommodate the desired number of PCs. Reset the Cisco uBR900 series 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 uBR900 series 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) software.

### Caveat 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?/` 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>.

## Cisco uBR904 Cable Access Router End of Life

The Cisco uBR904 cable access router is an end-of-life (EOL) product, and is no longer available for orders as of October 1999. Software images for the Cisco uBR904 router will continue to be available until November 2000 but will not contain any new feature sets. However, the software images for the Cisco uBR904 router do include the current caveat fixes.

## Configuring the Cisco uBR904 Router for Routing Mode

To change the operating mode of the Cisco uBR904 cable access router from its default bridging state, complete the following procedure:

	Command	Purpose
Step 1	<code>ubr904(config)#int c 0</code>	Enter interface configuration mode for the cable interface.
Step 2	<code>ubr904(config-if)# no cable-modem compliant bridge</code>	Disable DOCSIS-compliant bridging.
Step 3	<code>ubr904(config-if)# no bridge group number</code>	Remove the bridge group.
Step 4	<code>ubr904(config-if)# ip address ip-address subnet-mask</code>	Enter the cable interface's IP address and subnet mask.
Step 5	<code>ubr904(config-if)# exit</code>	Return to global configuration mode.
Step 6	<code>ubr904(config)#int e 0</code>	Enter interface configuration mode for Ethernet 0.
Step 7	<code>ubr904(config-if)# no bridge group number</code>	Remove the bridge group.
Step 8	<code>ubr904(config-if)# ip address ip-address subnet-mask</code>	Enter the Ethernet interface's IP address and subnet mask.
Step 9	<code>ubr904(config-if)# exit</code>	Return to global configuration mode.
Step 10	<code>ubr904(config)# ip routing</code>	Enable IP routing for the router.
Step 11	<b>To use RIPv2:</b> <code>ubr904(config)#router rip</code> <code>ubr904(config-router)# version 2</code> <code>ubr904(config-router)# network cable-network-number</code> <code>ubr904(config-router)# network Ethernet-network-number</code> <code>ubr904(config-router)# exit</code>	Enter router configuration mode. Enable RIP version 2 routing. Enable routing on the cable interface's IP network. Enable routing on the Ethernet interface's IP network. Return to global configuration mode.
Step 12	<code>ubr904(config)# no cdp run</code>	(Optional) Disable the Cisco Discovery Protocol (CDP) on the router. (CDP is a proprietary protocol for the discovery of Cisco routers running protocols other than TCP/IP; because DOCSIS cable data networks are primarily TCP/IP networks, CDP is not necessary on the Cisco uBR904 router.)

	Command	Purpose
Step 13	ubr904(config)# <b>ip default-gateway</b> <i>ip-address</i>	Set the default gateway for routing (typically, this is the CMTS).
Step 14	ubr904(config)# <b>ip classless</b>	(Optional) Enable the forwarding of packets that are destined for unrecognized subnets to the best supernet route.
Step 15	ubr904(config)# <b>ip route 0.0.0.0 0.0.0.0</b> <i>ip-address</i>	(Optional) Establish a static route so that all packets without an established route are forwarded to the default gateway (typically the <i>ip-address</i> should be the IP address for the CMTS), regardless of any routing metrics.
Step 16	ubr904(config-if)# <b>Ctrl-z</b>	Return to privileged EXEC mode.
Step 17	ubr904# <b>copy running-config startup-config</b> Building configuration...	Save the configuration to nonvolatile memory so that it will not be lost in the event of a reset, power cycle, or power outage.
Step 18	ubr904# <b>show startup-config</b>	Display the configuration file that was just created.

## Downloading a Cisco IOS Configuration File to the Cisco uBR904 Router

The vendor-specific information field in the DOCSIS configuration file supports a vendor-defined attribute (type = 43) that lets the system administrator define the name of a Cisco IOS configuration file to download to a remote Cisco uBR904 cable access router. This requires a unique DHCP policy for the Cisco uBR904 cable access router, a unique DOCSIS configuration file to be sent by the DOCSIS process, and a unique Cisco IOS configuration filename—such as “ios.cfg” file—located in the same TFTP server directory supported by the DOCSIS process.

The Cisco uBR904 router automatically downloads the DOCSIS configuration file during initialization. If the DOCSIS configuration file contains the name of a Cisco IOS configuration file, the router automatically downloads that file and processes its Cisco IOS commands. This also automatically disables the router’s console port to prevent remote configuration of the router.

Use the following procedure to enter the filename for a Cisco IOS configuration file in the router’s DOCSIS configuration file:



**Note**

The following steps can be accomplished through the Cisco DOCSIS CPE Configurator, which is available on CCO at <http://www.cisco.com/support/toolkit/CableModem>.

- Step 1** Create a Cisco IOS configuration file that should be sent to the Cisco uBR904 router. This file should contain any of the Cisco IOS commands that are needed to configure the router for proper operation.
- Step 2** Give the file a short filename such as “ios.cfg” and place that file in the appropriate directory on the TFTP server used by the Cisco uBR904 router.
- Step 3** Ensure that file permissions allow the file to be sent by TFTP.



**Note**

On a standard UNIX workstation, put the IOS configuration file in the */tftpboot* directory. Enter the following command: **chmod 775 filename**, where *filename* is the image filename.

- Step 4** Using a DOCSIS configuration editor, such as the Cisco DOCSIS CPE Configurator, create a DOCSIS configuration file and populate the file with the correct provisioning values. (If using version 2.0 of the DOCSIS CPE Configurator, you can simply enter the Cisco IOS configuration filename when prompted for it.)



**Note** DOCSIS configuration files work on the “TLV” basis—meaning Type, Length, Value. However, the Cisco DOCSIS CPE Configuration tool allows you to enter just the desired value, such as the filename; the tool then calculates the appropriate type and length fields.

If using another DOCSIS configuration file editor, enter the following information in the Vendor Specific Information Field (the following uses a file named “ios.cfg”—replace this value with the actual filename being used):

- For Cisco products, specify “00C” as the Vendor ID field.
- The option for downloading a Cisco IOS configuration file is “128”—this downloads the configuration file to the Cisco uBR904 router and disables the console port to prevent further configuration of the router at the remote site.
- Convert the Cisco IOS configuration filename to the decimal equivalent of the filename’s ASCII characters. Use the following ASCII-to-decimal conversion chart as needed. See the sample below:

Decimal - Character												
0 NUL	1 SOH	2 STX	3 ETX	4 EOT	5 ENQ	6 ACK	7 BEL					
8 BS	9 HT	10 NL	11 VT	12 NP	13 CR	14 SO	15 SI					
16 DLE	17 DC1	18 DC2	19 DC3	20 DC4	21 NAK	22 SYN	23 ETB					
24 CAN	25 EM	26 SUB	27 ESC	28 FS	29 GS	30 RS	31 US					
32 SP	33 !	34 "	35 #	36 \$	37 %	38 &	39 '					
40 (	41 )	42 *	43 +	44 ,	45 -	46 .	47 /					
48 0	49 1	50 2	51 3	52 4	53 5	54 6	55 7					
56 8	57 9	58 :	59 ;	60 <	61 =	62 >	63 ?					
64 @	65 A	66 B	67 C	68 D	69 E	70 F	71 G					
72 H	73 I	74 J	75 K	76 L	77 M	78 N	79 O					
80 P	81 Q	82 R	83 S	84 T	85 U	86 V	87 W					
88 X	89 Y	90 Z	91 [	92 \	93 ]	94 ^	95 _					
96 `	97 a	98 b	99 c	100 d	101 e	102 f	103 g					
104 h	105 i	106 j	107 k	108 l	109 m	110 n	111 o					
112 p	113 q	114 r	115 s	116 t	117 u	118 v	119 w					
120 x	121 y	122 z	123 {	124	125 }	126 ~	127 DEL					

For example, “ios.cfg” converts to the string of decimal digits shown:

**i**            **o**            **s**            **.**            **c**            **f**            **g**  
**105**            **111**            **115**            **46**            **99**            **102**            **103**

- Enter the Type, Length, and Value fields into the DOCSIS configuration file. For example, the filename “ios.cfg” would require the following values:

```
128.6.105.111.115.46.99.102.103 \
```

- Save your changes using the configuration file editor.

- Step 5** After you have saved the DOCSIS configuration file, save both the DOCSIS configuration file and the Cisco IOS configuration file on the TFTP file server in the appropriate directory (such as */tftpboot* or the equivalent).

- Step 6** Ensure that the configuration files have the proper permissions to allow TFTP to download the files to the Cisco uBR904 router. For example, on a UNIX workstation, give the following commands:

```
chmod 775 filename1
chmod 775 filename2
```

- Step 7** If necessary, reconfigure your DHCP server so that it downloads the new DOCSIS configuration file. (Cisco supplies a number of products, such as Cisco Network Register [CNR], to configure DHCP servers.)
- Step 8** Reset the Cisco uBR904 router to force it to reinitialize. If using a Cisco uBR7200 series router as the CMTS, you can give the following command on the Cisco uBR7200 series command-line console:

```
clear cable modem x.x.x.x reset
```

The Cisco uBR904 cable access router reregisters with the CMTS. When it processes the new DOCSIS configuration file, it downloads the new Cisco IOS configuration file from the TFTP server.

The console port of the Cisco uBR904 cable access router is completely disabled.

## 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.

## Downloading a Cisco IOS Image to the Cisco uBR904 Router

The CMTS system administrator can download an updated Cisco IOS image to a Cisco uBR904 router installed in the field by specifying the updated image filename in the router’s DOCSIS configuration file. The Cisco uBR904 router automatically downloads the DOCSIS configuration file during initialization. If the software upgrade option is present in the DOCSIS configuration file and if the name of the Cisco IOS image in the DOCSIS configuration file differs from the image that is currently running on the Cisco uBR904 router, the router automatically downloads the new Cisco IOS image from the Trivial File Transfer Protocol (TFTP) server and reboots.

The image filename must be entered as the fully qualified file and path name for the file, as it exists on a TFTP server. For example, if the **ubr900-k1y5-mz** software image is available on the TFTP server in the **12.1** directory, enter the following as the filename:

```
/12.1/ubr900-k1y5-mz
```



### Note

If using the DOCSIS CPE Configurator tool, v2.0 or greater, you can enter the software filename and the TFTP server’s IP address in the Software Upgrade fields.

## PPP IPCP Enhancements

The PPP IPCP command, which supplies Domain Name System (DNS) or Windows Internet Naming Service (WINS) addresses during IP Control Protocol (IPCP) negotiation, has been enhanced with the reject and accept keywords. These keywords allow enabling or disabling support for the Microsoft IPCP extensions defined by RFC 1877.

## Supplemental and Corrected Text for the Cisco uBR904 Cable Access Router

The following is updated information to the *Cisco uBR904 Cable Modem Installation and Configuration Guide*.

Data transmitted to a Cisco uBR904 cable access router from the CMTS shares a 26- or 27-Mbps, 6-MHz data channel in the 88- to 860-MHz range. The Cisco uBR904 cable access router shares an upstream data rate of up to 10 Mbps on a 200-kHz-wide to 3.2-MHz-wide channel in the 5- to 42-MHz range.



### Note

End-to-end throughput varies based on the design and loading of network components, the mix of traffic, the processing speed and interface of the host servers, the processing speed and local Ethernet performance of the subscriber's computer, and other parameters.


The Cisco uBR904 cable access router supports 64 or 256 quadrature amplitude modulation (QAM) downstream, and Quadrature Phase-Shift Keying (QPSK) or 16-QAM upstream transmission.

Table 5 lists the upstream and downstream data specifications for the Cisco uBR904 cable access router.

**Table 5** *Cisco uBR904 Cable Access Router Data Specifications*

Description	Downstream Values	Upstream Values
Frequency Range	88 to 860 MHz	5 to 42 MHz
Modulation	64 QAM 256 QAM	QPSK 16 QAM
Data Rate	30 Mbps/64 QAM (27 Mbit/sec after FEC overhead) 42.8 Mbps/256 QAM (36 Mbit/sec after FEC overhead)	QPSK—320 Kbit/sec to 5 Mbit/sec 16 QAM—640 Kbit/sec to 10 Mbit/sec
Bandwidth	6 MHz	200K, 400K, 800K, 1.6M, 3.2 MHz
FEC	RS (122, 128) Trellis	Reed Solomon
One Channel	Receive level of digital signal -15 to +15 dBmV	QPSK— +8 to +58 dBmV 16 QAM— +8 to +55 dBmV
	 <b>Note</b> Most field measurements are of nearby or adjacent analog signal, which is normally +6 to +10 dB (system specific) above the digital signal level.	

**Table 5 Cisco uBR904 Cable Access Router Data Specifications (continued)**

Description	Downstream Values	Upstream Values
Security	DES decryption: DOCSIS Baseline Privacy (BPI), 40-bit- and 56-bit-encryption, as controlled by the headend and configuration files.   <b>Note</b> Cisco IOS images must contain encryption software at both the CMTS router and the Cisco uBR904 router. Enable and configure both routers to support encryption.	DES encryption.
Signal-to-Noise Ratio (SNR) <sup>1</sup>	64 QAM: >23.5 dB @ BER<10 <sup>-8</sup>  256 QAM*: >30 dB @ BER <10 <sup>-8</sup> (For input levels between +15 and -8 dBmV, SNR must be greater than 30 dB. For input levels between -8 and -15 dBmV, SNR must be greater than 33 dB.)	QPSK: <sup>2</sup> >15 dB @ BER<10 <sup>-8</sup> (QPSK will work at 98% successful ping rate for SNR>13 dB. An SNR of 15 dB is needed to get almost optimal packets per minute transition.)  16 QAM: >22 dB @ BER <10 <sup>-8</sup> (For 16 QAM, an SNR>22 dB creates a grade that is for 98% ping efficiency. To get a good packet rate, you need SNR>25 dB).

1. These performance numbers are in laboratory-controlled conditions, against statistically pure noise sources (AWGN). Because such conditions do not exist in practice, an SNR margin of 6 dB or more is required for reliable operation. Check with your local system guidelines.
2. These measurements were done for 0 and -10 dBmV input to the CMTS, 1280 ksym/sec and 64-byte packet size with a Cisco uBR904 cable access router and laboratory-controlled conditions.

DOCSIS configuration files typically are created at the headend by using a configuration file editor of your choice. Using the FastStep utility at a subscriber site to locally configure the unit is not supported. The DOCSIS configuration file defines the Cisco uBR904 cable access router’s operating mode, such as the provisioned downstream and upstream service assignments, including assigned frequencies, data rates, modulation schemes, class of service (CoS), type of services to support, and other parameters.



**Note**

An incorrect configuration file can cause the Cisco uBR904 cable access router to constantly cycle offline. Such errors include: wrong downstream frequency, wrong Upstream Channel Descriptor (UCD), wrong downstream Channel ID, invalid CoS, and incorrect BPI privacy configurations or shared secret strings.

The Cisco uBR904 cable access router supports the following service classes:

- The first CoS in the DOCSIS configuration file is configured as the “Tiered Best Effort Type Class” used by the Cisco uBR904 cable access router as the primary quality-of-service (QoS) for all regular data traffic. The class has no minimum upstream rate specified for the channel.

This service class assigns a primary Service ID (SID) for the unit. In addition to being used as a data SID, the router uses this SID for all MAC message exchanges with the CMTS. Any Simple Network Management Protocol (SNMP) management traffic from the network to the Cisco uBR904 cable access router also uses this SID.

While this class is strictly “best effort,” you can prioritize data traffic within this class into eight different priority levels.




---

**Note** The CMTS system administrator must define the supported upstream traffic priority levels and include the traffic priority fields in the DOCSIS configuration file downloaded to the Cisco uBR904 router.

---

- The CMTS system administrator, when creating a DOCSIS configuration file for the Cisco uBR904 cable access router, can configure extra classes of service. These secondary classes of service are expected to be high QoS classes and are used by high-priority traffic. These classes have a minimum upstream rate specified for the channel.

## Supplemental and Corrected Text for the Online Feature Module

### For the Cisco uBR924 Cable Access Router

*Troubleshooting Tips for the Cisco 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 Incrementally Related Carrier (IRC) and Harmonically Related Carrier (HRC) plans are supported. Most of the IRC channel slots overlap the EIA plan.

“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 might increase the 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 first time it is added to the cable system.”



**Note**

---

For the most current information about the Cisco uBR924 cable access router, see the documents listed in the “Related Documentation” section on page 28.

---

### For the Cisco uBR904 Cable Access Router

*Troubleshooting Tips for the Cisco uBR904 Cable Modem, page 11, 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 modems since so few cable plants are using this plan.”

The correction should read:

“For the Cisco uBR904 cable access router, both the Incrementally Related Carrier (IRC) and Harmonically Related Carrier (HRC) plans are supported. Most of the IRC channel slots overlap the EIA plan.

“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 might increase the time required by the Cisco uBR904 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 Cisco uBR904 cable access router the first time it is added to the cable system.”

## Supported MIBs

The Cisco uBR900 series cable access router supports the following categories of Management Information Bases (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.
- 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 only supported by the Cisco uBR924 cable access router.
- Radio Frequency Interface MIBs—These MIBs are for DOCSIS-compliant radio frequency interfaces in cable modems and CMTS.
- SGCP MIBs—These MIBs support configuration, performance, and fault management of the SGCP interface. These MIBs are only supported by the Cisco uBR924 cable access router.
- 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 uBR900 series 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

For the Cisco uBR900 series cable access router, the Cable Device MIB is supported. The Cable Device MIB is for DOCSIS-compliant cable modems and CMTS. The Cable Device MIB records statistics related to the configuration and status of the cable modem. Statistics include an events log and device status. The following list details the components of the Cable Device MIB:

- “docsDevBase” group extends the MIB-II “system” group with objects needed for cable device system management.
- “docsDevNmAccess” group provides a minimum level of SNMP access security.
- “docsDevSoftware” group provides information for network downloadable software upgrades.
- “docsDevServer” group provides information about the progress of interaction with various provisioning servers.
- “docsDevEvent” group provides information about the progress of reporting.
- “docsDevFilter” group configures filters at 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. However, the Cable Device MIB reports statistics on the cable modem, while the RFI MIB reports statistics on the radio frequency transmissions over the cable television line.

## Cisco Standard MIBs

For the Cisco uBR900 series cable access router, the Cisco Standard MIBs are supported. The Cisco Standard MIBs consist of the following components:

- CISCO-PRODUCT-MIB
- CISCO-SYSLOG-MIB
- CISCO-FLASH-MIB
- BRIDGE-MIB
- IF-MIB
- 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 (Cisco uBR924 only)

The Cisco Voice MIBs are supported only on the Cisco uBR924 cable access router. The Cisco Voice MIBs consist of the following components:

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

## Radio Frequency Interface MIBs

For the Cisco uBR900 series cable access router, the Radio Frequency Interface (RFI) MIB is supported. The RFI MIB module is for 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 MIBs (Cisco uBR924 only)

The Simple Gateway Control Protocol (SGCP) Management Information Bases (MIBs) are supported only on the Cisco uBR924 cable access router. The SGCP MIBs support configuration, performance, and fault management of the SGCP interface. The SGCP MIBs components are as follows:

- `xgcpInBadVersions`—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

## Cable-Specific MIBs


Table 6 shows the cable-specific MIBs that are supported on the Cisco uBR900 series 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 6 are the filenames for the MIBs as they exist on Cisco’s FTP site (<ftp://ftp.cisco.com/pub/mibs/> or <http://www.cisco.com/public/mibs>). Most MIBs are available in both SNMPv1 and SNMPv2 versions; the SNMPv1 versions have *V1SM1* 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 6 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 Structure of Management Information (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 1229.	12.0(4) XI
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.	12.0(4) XI
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.   <b>Note</b> 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.	12.0(4) XI

**Note**

Because of interdependencies, the MIBs must be loaded in the order given in Table 6.

## 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 7 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 7** 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 7 represent feature sets that are not supported on the Cisco uBR900 series 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](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, and only select severity 3 caveats are included in the caveats document.

For information on caveats in Cisco IOS Release 12.1, see *Caveats for Cisco IOS Release 12.1*, which lists severity 1 and 2 caveats and select severity 3 caveats for Cisco IOS Release 12.1 and is 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)

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

- CSCdm38753

The Cisco uBR924 cable access 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 uBR904 cable access router can stop responding to CMTS requests when upstreams are configured with different minislot sizes. The workaround is to configure the upstreams with the same minislot size.

- CSCdp03177

When running Cisco IOS Release 11.3(11) NA, the Cisco uBR900 series 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 uBR900 series 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.

- CSCdr11723

When two Cisco uBR924 cable access routers have established a working voice call, a particular situation might prevent the two routers from establishing any additional voice calls. The workaround is to reload each router before making additional voice calls.

- 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?/` 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>.

## Closed or Resolved Caveats—Release 12.1(5)

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

- CSCdp04541

Previously, the Cisco uBR900 series 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 cable access 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).

- CSCdp64558

Cisco IOS Release 12.1(2) updates the Cisco uBR924 cable access router so that the "docsDevCpeIpMax" attribute defaults to -1, which allows any number of CPE devices to access the cable network through the Cisco uBR924 cable access router.

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

- CSCdp80746 and CSCdr23760

The Cisco uBR900 series 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 TFTP server's directory structure so that the fully-qualified pathname was shorter than 48 characters.

- CSCdp89376

The Cisco uBR900 series cable access router could crash with an exception if the **debug all** command is given to turn on all debugging statements. This caveat was closed because the problem cannot be reproduced in production software images.




---

**Note** All **debug** commands should be used only when needed for troubleshooting and testing, and then turned off when no longer needed. Each **debug** display consumes system resources; turning on too many **debug** commands can negatively affect system performance.

---

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

- CSCdp95187 and CSCdp97141

The Cisco uBR924 cable access router, when running the Small Office feature set, could crash (with an exception) when changing the running configuration. The crash occurred when using a specific configuration designed for test networks and was unlikely to occur when using configurations for real-life networks.

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

- 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 uBR900 series cable access routers. IPSec tunnels, however, are supported when using Cisco IOS images that support IPSec encryption.

- 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).

**Note**

Although CSCdr36952 has been resolved in Release 12.1(2), 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.

## Related Documentation

The following sections describe the documentation available for the Cisco uBR900 series 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 28
- Platform-Specific Documents, page 29
- Feature Modules, page 30
- Cisco IOS Software Documentation Set, page 30

## 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

### Cisco uBR924 Cable Access Router

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

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**




---

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

---

### Cisco uBR904 Cable Access Router

These documents are available for the Cisco uBR904 cable access router on CCO and the Documentation CD-ROM:

- *Cisco uBR904 Cable Access Router Installation and Configuration Guide*
- *Update to the uBR904 Cable Access Router Installation and Configuration Guide*
- *Cisco uBR904 Cable Access Router Subscriber Setup Quick Reference Card*
- *Bridging and Routing Features for the Cisco uBR904 Cable Access Router*
- *Troubleshooting Tips for the Cisco uBR904 Cable Access Router*

- *Regulatory Compliance and Safety Information for the Cisco uBR904*
- *DOCSIS CPE Configurator* online help

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 8 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 8 Cisco IOS Software Release 12.1 Documentation Set**

Books	Major Topics
<ul style="list-style-type: none"> <li><i>Cisco IOS Configuration Fundamentals Configuration Guide</i></li> <li><i>Cisco IOS Configuration Fundamentals Command Reference</i></li> </ul>	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"> <li><i>Cisco IOS Bridging and IBM Networking Configuration Guide</i></li> <li><i>Cisco IOS Bridging and IBM Networking Command Reference, Volume I</i></li> <li><i>Cisco IOS Bridging and IBM Networking Command Reference, Volume II</i></li> </ul>	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

**Table 8 Cisco IOS Software Release 12.1 Documentation Set (continued)**

Books	Major Topics
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Dial Services Configuration Guide: Terminal Services</i></li> <li>• <i>Cisco IOS Dial Services Configuration Guide: Network Services</i></li> <li>• <i>Cisco IOS Dial Services Command Reference</i></li> </ul>	<ul style="list-style-type: none"> <li>Preparing for Dial Access</li> <li>Modem Configuration and Management</li> <li>ISDN and Signalling Configuration</li> <li>PPP Configuration</li> <li>Dial-on-Demand Routing Configuration</li> <li>Dial-Backup Configuration</li> <li>Terminal Service Configuration</li> <li>Large-Scale Dial Solutions</li> <li>Cost-Control Solutions</li> <li>Virtual Private Networks</li> <li>X.25 on ISDN Solutions</li> <li>Telco Solutions</li> <li>Dial-Related Addressing Services</li> <li>Dial Access Scenarios</li> </ul>
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Interface Configuration Guide</i></li> <li>• <i>Cisco IOS Interface Command Reference</i></li> </ul>	<ul style="list-style-type: none"> <li>Interface Configuration Overview</li> <li>Configuring LAN Interfaces</li> <li>Configuring Serial Interfaces</li> <li>Configuring Logical Interfaces</li> </ul>
<ul style="list-style-type: none"> <li>• <i>Cisco IOS IP and IP Routing Configuration Guide</i></li> <li>• <i>Cisco IOS IP and IP Routing Command Reference</i></li> </ul>	<ul style="list-style-type: none"> <li>IP Overview</li> <li>IP Addressing and Services</li> <li>IP Routing Protocols</li> <li>IP Multicast</li> </ul>
<ul style="list-style-type: none"> <li>• <i>Cisco IOS AppleTalk and Novell IPX Configuration Guide</i></li> <li>• <i>Cisco IOS AppleTalk and Novell IPX Command Reference</i></li> </ul>	<ul style="list-style-type: none"> <li>AppleTalk and Novell IPX Overview</li> <li>Configuring AppleTalk</li> <li>Configuring Novell IPX</li> </ul>
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS, and XNS Configuration Guide</i></li> <li>• <i>Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS, and XNS Command Reference</i></li> </ul>	<ul style="list-style-type: none"> <li>Overview</li> <li>Configuring Apollo Domain</li> <li>Configuring Banyan VINES</li> <li>Configuring DECnet</li> <li>Configuring ISO CLNS</li> <li>Configuring XNS</li> </ul>
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Multiservice Applications Configuration Guide</i></li> <li>• <i>Cisco IOS Multiservice Applications Command Reference</i></li> </ul>	<ul style="list-style-type: none"> <li>Multiservice Applications Overview</li> <li>Voice</li> <li>Video</li> <li>Broadband</li> </ul>
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Quality of Service Solutions Configuration Guide</i></li> <li>• <i>Cisco IOS Quality of Service Solutions Command Reference</i></li> </ul>	<ul style="list-style-type: none"> <li>Quality of Service Overview</li> <li>Classification</li> <li>Congestion Management</li> <li>Congestion Avoidance</li> <li>Policing and Shaping</li> <li>Signalling</li> <li>Link Efficiency Mechanisms</li> <li>Quality of Service Solutions</li> </ul>

**Table 8 Cisco IOS Software Release 12.1 Documentation Set (continued)**

Books	Major Topics
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Security Configuration Guide</i></li> <li>• <i>Cisco IOS Security Command Reference</i></li> </ul>	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"> <li>• <i>Cisco IOS Switching Services Configuration Guide</i></li> <li>• <i>Cisco IOS Switching Services Command Reference</i></li> </ul>	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"> <li>• <i>Cisco IOS Wide-Area Networking Configuration Guide</i></li> <li>• <i>Cisco IOS Wide-Area Networking Command Reference</i></li> </ul>	Introduction: Wide-Area Networking Overview Configuring ATM Configuring Frame Relay Configuring Frame Relay-ATM Interworking Configuring SMDS Configuring X.25 and LAPB
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Configuration Master Index</i></li> <li>• <i>Cisco IOS Command Reference Master Index</i></li> <li>• <i>Cisco IOS Debug Command Reference</i></li> <li>• <i>Cisco IOS Dial Services Quick Configuration Guide</i></li> <li>• <i>Cisco IOS Software System Error Messages</i></li> <li>• <i>Cisco IOS Configuration Guide Master Index</i></li> <li>• <i>New Features in 12.1-Based Limited Lifetime Releases</i></li> <li>• <i>New Features in Release 12.1 T</i></li> <li>• Release Notes (Release note and caveat documentation for 12.1-based releases and various platforms)</li> </ul>	

**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](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](http://www.cisco.com)
- Telnet: [cco.cisco.com](http://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](mailto: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](http://www.cisco.com/techsupport).

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

Language	E-mail Address
English	<a href="mailto:tac@cisco.com">tac@cisco.com</a>
Hanzi (Chinese)	<a href="mailto:chinese-tac@cisco.com">chinese-tac@cisco.com</a>
Kanji (Japanese)	<a href="mailto:japan-tac@cisco.com">japan-tac@cisco.com</a>
Hangul (Korean)	<a href="mailto:korea-tac@cisco.com">korea-tac@cisco.com</a>
Spanish	<a href="mailto:tac@cisco.com">tac@cisco.com</a>
Thai	<a href="mailto:thai-tac@cisco.com">thai-tac@cisco.com</a>

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](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:

- Access Dial Cookbook—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.

## 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](mailto: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 28.

Access Registrar, AccessPath, Are You Ready, ATM Director, 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, Fast Step, FireRunner, Follow Me Browsing, FormShare, GigaStack, IGX, Intelligence in the Optical Core, Internet Quotient, IP/VC, iQ Breakthrough, iQ Expertise, iQ FastTrack, iQuick Study, iQ Readiness Scorecard, The iQ Logo, Kernel Proxy, MGX, Natural Network Viewer, Network Registrar, the Networkers logo, *Packet*, PIX, Point and Click Internetworking, Policy Builder, RateMUX, ReyMaster, ReyView, ScriptShare, Secure Script, Shop with Me, SlideCast, SMARTnet, SVX, TrafficDirector, TransPath, VlanDirector, Voice LAN, Wavelength Router, Workgroup Director, and Workgroup Stack 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 Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Collision Free, Enterprise/Solver, EtherChannel, EtherSwitch, FastHub, FastLink, FastPAD, IOS, IP/TV, IPX, LightStream, LightSwitch, MICA, NetRanger, Post-Routing, Pre-Routing, Registrar, StrataView Plus, Stratm, SwitchProbe, TeleRouter, 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/website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any of its resellers. (0008R)

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