



Text Part Number: 78-6482-04

Release Notes for Cisco uBR904 Cable Access Router for Cisco IOS Release 12.0(7)T

December 13, 1999

These release notes for the Cisco uBR904 cable access router support Cisco IOS Release 12.0 T, up to and including Release 12.0(2)XC, 12.0(3)T, 12.0(4)T, 12.0(5)T, 12.0(7)T, or higher interim images. 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 the software caveats that apply to Release 12.0(7)T, see the “Caveats” section on page 22 and *Caveats for Cisco IOS Release 12.0 T*. The caveats document is updated for every maintenance release and is located on Cisco Connection Online (CCO).

Use these release notes with *Cross-Platform Release Notes for Cisco IOS Release 12.0* located on CCO.

Contents

These release notes describe the following topics:

- Introduction, page 2
- System Requirements, page 2
- New and Changed Information, page 5
- Important Notes, page 12
- Caveats, page 22
- Related Documentation, page 22
- Service and Support, page 27
- Cisco Connection Online, page 28
- Documentation CD-ROM, page 29

Corporate Headquarters

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

Copyright © 1999
Cisco Systems, Inc.
All rights reserved.

Introduction

The Cisco uBR904 cable access router gives residential or small office/home office (SOHO) subscribers, high-speed Internet or Intranet access via a shared two-way cable system and IP backbone network. The router connects computers and other customer premises devices at a subscriber site to the service provider's hybrid/fiber coax (HFC) and IP backbone network.

The Cisco uBR904 cable access router interoperates with any bidirectional, DOCSIS-qualified Cable Modem Termination System (CMTS). The Cisco uBR904 cable access router ships from the Cisco factory with a Cisco IOS software image stored in nonvolatile memory (NVRAM) that supports DOCSIS-compliant bridging data operations. The Cisco uBR904 cable access router functions as a cable modem—a modulator/demodulator at a subscriber site to convey data communications on the cable television system.

Based on the feature licenses your company purchased, you can download other Cisco IOS images from CCO. You can configure each Cisco uBR904 cable access router in your network to support special operating modes based on your cable plant's service offering and the practices in place for your network. The Cisco uBR904 cable access router can function as an advanced router, providing wide area network (WAN) data connectivity in a variety of configurations.

System Requirements

This section describes the system requirements for Release 12.0 T:

- Memory Requirements, page 2
- Headend Interoperability, page 3
- Hardware Supported, page 3
- Determining the Software Version, page 4
- Upgrading to a New Software Release, page 4
- Feature Set Tables, page 4

Memory Requirements

Table 1 Memory Requirements for the Cisco uBR904 Cable Access Router

| Feature Set Matrix Term | Image Name | Required Flash Memory | Required DRAM Memory | Runs From | Feature Status |
|---|--------------------|-----------------------|----------------------|-----------|--|
| IP Routing Standard Feature Sets | | | | | |
| 12.0(7)T | | | | | |
| Home Office | ubr900-k1y5-mz | 4 MB Flash | 8 MB DRAM | RAM | Added in Release 12.0(7)T |
| Telecommuter/IPSec 56 | ubr900-k1y556i-mz | 4 MB Flash | 8 MB DRAM | RAM | Encryption image added in Release 12.0(7)T |
| Small Office/FW | ubr900-k1oy5-mz | 4 MB Flash | 8 MB DRAM | RAM | Added in Release 12.0(7)T |
| Small Office+/FW/IPSec 56 | ubr900-k1oy556i-mz | 4 MB Flash | 8 MB DRAM | RAM | Added in Release 12.0(7)T |

Table 1 Memory Requirements for the Cisco uBR904 Cable Access Router (continued)

| Feature Set Matrix Term | Image Name | Required Flash Memory | Required DRAM Memory | Runs From | Feature Status |
|-----------------------------|---------------------|-----------------------|----------------------|-----------|--|
| 12.0(3)T to 12.0(5)T | | | | | |
| Home Office | ubr900-k1y5-mz | 4 MB Flash | 8 MB DRAM | RAM | Added in Release 12.0(3)T |
| Telecommuter/IPSec 56 | ubr900-k1sy556i-mz | 4 MB Flash | 8 MB DRAM | RAM | Encryption image added in Release 12.0(3)T |
| Small Office/FW | ubr900-k1oy5-mz | 4 MB Flash | 8 MB DRAM | RAM | Added in Release 12.0(3)T |
| Small Office+/FW/IPSec 56 | ubr900-k1osy556i-mz | 4 MB Flash | 8 MB DRAM | RAM | Encryption image added in Release 12.0(3)T |

The image subset legend for Table 1 appears below:

- k1=DOCSIS baseline privacy
- s=Plus set includes L2TP—Available in Cisco IOS Releases 12.0(3)T to 12.0(5)T; not available in Cisco IOS Release 12.0(7)T
- o=Firewall (Phase I) feature set
- y5=Reduced IP image with easy IP functionality (PAT/NAT/DHCP server)
- 56i=56-bit IPSec

Note The L2TP feature is removed in Cisco IOS Release 12.0(7)T.

Headend Interoperability

Note Starting with Cisco IOS Release 12.0(5)T, all Cisco uBR904 cable access router images support DOCSIS Baseline Privacy (BPI) encryption/decryption. BPI is subject to export restrictions.

To support encryption/decryption, Cisco IOS images must contain encryption/decryption software at both the CMTS router and the Cisco uBR904 cable access router. Both the CMTS router and the Cisco uBR904 cable access router must be enabled and configured per the software feature set.

If you are using Cisco 7200 series equipment, also refer to applicable release notes for the corresponding images at the headend that support the encryption/decryption software.

Hardware Supported

There are no new hardware features supported by the Cisco uBR904 cable access router for Cisco IOS Release 12.0 T.

Determining the Software Version

To determine the version of Cisco IOS software running on your Cisco uBR904 cable access router, log in to the Cisco uBR904 cable access router and enter the **show version EXEC** command:

```
router>show version
Cisco Internetwork Operating System Software
IOS (tm) 904 Software (UBR900-kly5-mz), Version 12.0(7)T, RELEASE SOFTWARE
```

Upgrading to a New Software Release

For information about upgrading to a new software release, see the product bulletin *Cisco IOS Software Release 12.0 Upgrade Paths and Packaging Simplification* located at:

http://www.cisco.com/warp/public/cc/cisco/mkt/ios/rel/120/prodlit/819_pp.htm

If you do not have an account on CCO and want general information about upgrading to a new software release, see the product bulletin *Cisco IOS Software Release 12.0 T Upgrade Paths and Packaging Simplification (#819: 1/99)* on CCO at:

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

Under **Cisco IOS 12.0**, click **Cisco IOS Software Release 12.0 T Upgrade (#819: 1/99)**.

Feature Set Tables

The Cisco IOS software is packaged in feature sets consisting of software images—depending on the platform. Each feature set contains a specific set of Cisco IOS features. (See Table 2.)

Release 12.0 T supports the same feature sets as Release 12.0, but Release 12.0 T can include new features supported by the Cisco uBR904 cable access router.

The Cisco uBR904 cable access router IP routing capabilities conserve IP addresses by using port-level multiplexed Network Address Translation (NAT) and Port Address Translation (PAT). Dynamic Host Configuration Protocol (DHCP) is used to distribute these or real IP addresses to the devices the Cisco uBR904 cable access router supports. NAT/PAT is bundled with DHCP server into a feature referred to as “Easy IP.”



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 or the user must obtain local import and use authorizations for all encryption strengths. Contact your sales representative or distributor for more information, or send e-mail to export@cisco.com.

Table 2 lists the features and feature sets supported by the Cisco uBR904 cable access router in Cisco IOS Release 12.0 T and uses the following conventions:

- Yes—The feature is supported in the feature set.
- No—The feature is not supported in the feature set.
- In—The number in the “In” column indicates the Cisco IOS release in which the feature was first introduced.

Note This feature set table only contains a selected list of features. This table is not cumulative—nor does it list all the features in each image.

Table 2 Feature List by Feature Set

| Features | Feature Sets | | | | |
|-------------------------------------|--------------|---|--|--|---|
| | In | Home Office, DOCSIS Baseline Privacy, Easy IP | Telecommuter, DOCSIS Baseline Privacy, Easy IP, IPSec 56 | Small Office, DOCSIS Baseline Privacy, Firewall, Easy IP | Small Office+, DOCSIS Baseline Privacy, Firewall, Easy IP, IPSec 56 |
| Full and DOCSIS-compliant Bridging | (2)XC | Yes | Yes | Yes | Yes |
| Routing (RIP V2) | (2)XC | Yes | Yes | Yes | Yes |
| Network Management | | | | | |
| DOCSIS 1.0 Baseline Privacy MIB | (5) | Yes | Yes | Yes | Yes |
| Cable Device MIB | (2)XC | Yes | Yes | Yes | Yes |
| Cisco Standard MIBs | (2)XC | Yes | Yes | Yes | Yes |
| Radio Frequency Interface (RFI) MIB | (2)XC | Yes | Yes | Yes | Yes |

New and Changed Information

The following section lists the new hardware and software features supported in Cisco IOS Release 12.0 T.

No New Hardware Features in Release 12.0(7)T

There are no new hardware features supported by the Cisco uBR904 cable access router for Release 12.0(7)T.

New Software Features in Release 12.0(7)T

The following new software features are supported by the Cisco uBR904 cable access router for Release 12.0(7)T.

VPN Enhancement—Dynamic Crypto Map

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

The **dynamic crypto map** command is used to create policy templates that are used when processing negotiation requests for new security associations from a remote IPSec peer, even if you do not know all of the crypto map parameters required to communicate with the remote peer (such

as the peer's IP address). The dynamic crypto map allows you to accept requests for new security associations from previously unknown peers. These requests, however, are not processed until the ISAKMP (IKE) authentication has completed successfully.

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

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

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

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

No New Hardware Features In Release 12.0(5)T

There are no new hardware features supported by the Cisco uBR904 cable access router for Release 12.0(5)T.

New Software Features in Release 12.0(5)T

Enhanced Bridging

Using previous Cisco IOS images, only three PCs can be directly connected to three of the four Ethernet hub ports at the rear of the Cisco uBR904 cable access router and operate correctly in bridging mode. The three-node directly-connected bridge limit existed due to the MAC chip contained in the unit. The MAC chip reserved one filter for the Cisco uBR904 cable access router's MAC address, leaving three available for Ethernet devices.

Cisco IOS 12.0(5)T images contain enhanced software, allowing 1 to 254 PCs to operate in bridging mode. Using Cisco IOS 12.0(5)T images, four PCs can be directly connected to four Ethernet hub ports or one of the four ports can be connected to an Ethernet hub, which then connects additional computers or devices at the site. For additional information regarding the bridging operation, see "Bridging Mode" in "Limitations and Restrictions."

No New Hardware Features In Release 12.0(4)T

There are no new hardware features supported by the Cisco uBR904 cable access router in Cisco IOS Release 12.0(4)T.

No New Software Features In Release 12.0(4)T

There are no new software features supported by the Cisco uBR904 cable access router in Cisco IOS Release 12.0(4)T.

No New Hardware Features In Release 12.0(3)T

There are no new hardware features supported by the Cisco uBR904 cable access router in Cisco IOS Release 12.0(3)T.

New Software Features In Release 12.0(3)T

Firewall (Phase I)

The Firewall (Phase I) feature set extends the security technology currently available in Cisco IOS software to the Cisco uBR904 cable access router, providing firewall-specific capabilities. Firewall (Phase I) features include stateful, application-based filtering, dynamic per-user authentication and authorization, defense against network attacks, Java blocking, and real-time alerts. Firewall (Phase I) is interoperable with Cisco IOS software features including NAT, VPN tunneling protocols, Cisco Express Forwarding (CEF), AAA extensions, Cisco encryption technology, and Cisco IOS IPsec.

New Software Features In Release 12.0(2)XC

Cable Device MIB

The Cable Device MIB is for DOCSIS-compliant cable modems and Cable Modem Termination Systems (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; 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 Standard MIBs consist of the following components:

- CISCO-PRODUCT-MIB

- CISCO-SYSLOG-MIB
- CISCO-FLASH-MIB
- BRIDGE-MIB
- IF-MIB
- CiscoWorks/CiscoView

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**

DOCSIS Baseline Privacy

The DOCSIS Baseline Privacy feature is based on the DOCSIS Baseline Privacy Interface Specification. It provides data privacy across the HFC network by encrypting traffic flows between the Cisco uBR904 cable access router and the cable operator's CMTS.

Baseline Privacy security services are defined as a set of extended services within the DOCSIS MAC sublayer. Two new MAC management message types, BPKM-REQ and BPKM-RSP, are employed to support the Baseline Privacy Key Management (BPKM) protocol.

The BPKM protocol does not use authentication mechanisms such as passwords or digital signatures; it provides basic protection of service by ensuring that a cable modem, uniquely identified by its 48-bit IEEE MAC address, can only obtain keying material for services it is authorized to access. The Cisco uBR904 cable access router is able to obtain two types of keys from the CMTS: the Traffic Exchange Key (TEK), which is used to encrypt and decrypt data packets, and the Key Exchange Key (KEK), which is used to decrypt the TEK.

For more information on this feature, refer to the DOCSIS Baseline Privacy Interface Specification (SP-BPI-IO1-970922).

Easy IP

Dynamic Host Configuration Protocol (DHCP) Server:

With the introduction of Easy IP, Cisco IOS Release 12.0(3)T supports Intelligent DHCP Relay and DHCP Client functionality. A DHCP Relay Agent is any host that forwards DHCP packets between clients and servers. A DHCP Relay Agent enables the client and server to reside on separate subnets. If the Cisco IOS DHCP server cannot satisfy a DHCP request from its own database, it can forward the DHCP request to one or more secondary DHCP servers defined by the network administrator using standard Cisco IOS IP helper-address functionality.

Network Address Translation and Port Address Translation (NAT/PAT):

- Allows customers to maintain their own private networks while giving them full Internet access through the use of one or more global IP addresses
- Allows several private IP addresses to use the same global IP address by using address overloading
- Facilitates configuration and permits a large network of users to reach the network by using one Cisco uBR904 cable access router and the same DOCSIS cable interface IP address

- Eliminates the need to readdress all hosts with existing private network addresses (one-to-one translation) or by enabling all internal hosts to share a single registered IP address (many-to-one translation, also known as Port Address Translation [PAT])
- Enables packets to be routed correctly to and from the outside world by using the Cisco uBR904 cable access router
- Allows personal computers on the Ethernet interface to have IP addresses to be mapped to the cable interface's IP address

Routing protocols will run on the Ethernet interface instead of the cable interface, and all packets received will be routed out the Ethernet interface or use the default gateway to reach the CMTS. This eliminates the need to run RIP on the cable interface.

To implement NAT on the Cisco uBR904 cable access router, the Ethernet interface is configured with an “inside” address and the cable interface is configured with an “outside” address. The Cisco uBR904 cable access router also supports configuration of static connections, dynamic connections, and address pools.

Full and DOCSIS-Compliant Bridging

Full and DOCSIS-Compliant Bridging allows the Cisco uBR904 cable access router to operate with any DOCSIS-qualified CMTS.

IPSec Network Security

IPSec Network Security (IPSec) is an IP security feature that provides robust authentications and encryption of IP packets. IPSec is a framework of open standards developed by the Internet Engineering Task Force (IETF). IPSec provides security for transmission of sensitive information over unprotected networks such as the Internet. IPSec acts at the network layer, protecting and authenticating IP packets between participating IPSec devices (“peers”) such as Cisco uBR904 cable access routers.

IPSec provides the following network security services:

- Privacy—IPSec can encrypt packets before transmitting them across a network.
- Integrity—IPSec authenticates packets at the destination peer to ensure that the data has not been altered during transmission.
- Authentication—Peers authenticate the source of all IPSec-protected packets.
- Anti-replay protection—Prevents capture and replay of packets; helps protect against denial-of-service attacks.

Layer 2 Tunneling Protocol

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

Note The L2TP feature is removed in Cisco IOS Release 12.0(7)T.

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

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

Refer to the “Limitations and Restrictions” section for information regarding the functionality of the Cisco uBR904 cable access router in L2TP applications.

Radio Frequency Interface MIB

The Radio Frequency Interface (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 security solution introduced in Cisco IOS Software Release 11.2. However, IPSec provides a more robust security solution, and is standards based.

Routing (RIP V2)

A routing configuration for the Cisco uBR904 cable access router is most likely used when the cable access router is being added to an existing personal computer network. When configured in routing mode, the Cisco uBR904 cable access router will automatically configure the headend's IP address as its IP default gateway. When the IP host-routing is being configured, this automatic configuration of the headend's IP address as its IP default gateway will allow the Cisco uBR904 cable access router to send packets not intended for the Ethernet interface to the headend.

RIP V2 routing is useful for small internetworks in that it enables optimization of Network Interface Center (NIC)-assigned IP addresses by defining VLSMs for network addresses, and it allows Classless Interdomain Routing (CIDR) addressing schema.

Limitations and Restrictions

This section describes warnings and cautions about using Cisco IOS Release 12.0 T software.

Using Multiple PCs with a Cisco uBR904 Cable Access Router

The MAX CPE parameter in a Cisco uBR904 cable access router's DOCSIS configuration file determines how many PCs (or other CPE devices) are supported by that Cisco uBR904 cable access router. The default value for the MAX CPE parameter is 1, which means only one PC can be connected to the Cisco uBR904 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 uBR904 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.

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 PC's MAC address will be rediscovered and associated with the correct Cisco uBR904 cable access router during the next DHCP lease cycle.
- Increase the value of the MAX CPE parameter in the Cisco uBR904 cable access router's DOCSIS configuration file so that it can accommodate the desired number of PCs. Reset the Cisco uBR904 cable access router to force it to load the new configuration file.

Bridging Mode

The Cisco uBR904 cable access router ships from the Cisco factory with the console port enabled. Based on the standard practices in place for your network, disable the console port as appropriate via the DOCSIS configuration file downloaded to the Cisco uBR904 cable access router. This prohibits network configuration access at the remote site.

Note Downloading a Cisco IOS image disables the console port by default and erases all previously saved configurations.

For software enhancements when operating in bridging mode, see the "Enhancements to Bridging Operation" section of the New Software Features in Release 12.0(5)T.

The ability of the Cisco uBR904 cable access router to grant access to customer premises equipment (CPE) devices is controlled by the "MAX CPE" field in the DOCSIS configuration file. The Cisco uBR904 cable access router defaults to one CPE MAC address unless this option is set to a higher number. The valid range using Cisco IOS Release 12.0(5)T or higher images is 1 to 254 for bridging operation; 1 filter is reserved for the broadcast address.

You can install and configure the Cisco uBR904 cable access router to operate as a router. In routing mode, no maximum upper limitation exists. For instructions to change from bridging to routing mode, see the "Important Notes" section on page 12.



Caution After you connect a laptop PC to the Cisco uBR904 cable access router console port and save configuration changes (provided your network supports remote configuration) power cycle the Cisco uBR904 cable access router if you're not using the laptop at the subscriber site. This is important when the Cisco uBR904 cable access router is configured to operate in a DOCSIS-compliant bridging mode. Power cycling the Cisco uBR904 cable access router ensures the laptop PC does not remain in the list of CPE devices at the subscriber site for the Cisco uBR904 cable access router to support. Only reinitialization of the cable interface clears out the bridge table and resets the counter that specifies the number of CPE devices being bridged.

Note This behavior is in accordance with DOCSIS. For configurations including Cisco 7200 series CMTS equipment, enter the **clear cable modem host mac address** command to clear the laptop PC from the headend security access control tables.

Layer 2 Tunneling Protocol

Implementation of L2TP in Cisco IOS Release 12.0(5)T is dependent on a PPP connection supported on one of the directly attached interfaces. A dial-up PPP connection is required in order to initiate an L2TP Tunnel connection. This is a requirement of the L2TP Access Concentrator (LAC). In Cisco IOS Release 12.0(5)T, the Cisco uBR904 cable access router cannot function as the LAC; it can only function as the L2TP Network Server (LNS), which terminates a tunnel created elsewhere in the network.

Note The L2TP feature is removed in Cisco IOS Release 12.0(7)T.

Important Notes

This section contains important information about using your Cisco IOS Release 12.0 T software.

Last Maintenance Release of Cisco IOS Release 12.0 T

Cisco IOS Release 12.0(6)T has been renamed 12.0(7)T to align this release with the 12.0(7) mainline release. The closed caveats for Release 12.0(7)T are identical to the caveats closed in the 12.0(7) mainline release. There was no change in the feature content of the renamed release—the features in 12.0(6)T are the same as 12.0(7)T. Release 12.0(7)T is the last maintenance release of the 12.0 T release train.

Customers needing closure of caveats for the 12.0 T features should migrate to the 12.1 mainline release, which has the complete feature content of Release 12.0 T and will eventually reach General Deployment (GD). Release 12.0 T is a superset of the 12.0 mainline release, so all caveats closed in the 12.0 mainline are also closed in 12.0 T.

Supplemental and Corrected Text for the Online Feature Module

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 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 uBR904 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 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 very first time it is added to the cable system.”

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 3 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 | QPSK |
| | 256 QAM | 16 QAM |
| Data Rate | 30 Mbps/64 QAM (27 Mbit/sec after FEC overhead) | QPSK—320 Kbit/sec to 5 Mbit/sec |
| | 42.8 Mbps/256 QAM (36 Mbit/sec after FEC overhead) | 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 |
| | Note Most field measurements are of nearby or adjacent analog signal, which is normally +6 to +10 dB (system specific) above the digital signal level | 16 QAM— +8 to +55 dBmV |

Table 3 Cisco uBR904 Cable Access Router Data Specifications (continued)

| Description | Downstream Values | Upstream Values |
|-----------------------------|--|---|
| Signal-to-Noise Ratio (SNR) | <p>64 QAM: >23.5 dB @ BER<10⁻⁸</p> <p>256 QAM*: >30 dB @ BER <10⁻⁸ (For input level between +15 and -8 dBmV, SNR must be greater than 30 dB. For input level between -8 and -15 dBmV, SNR must be greater than 33 dB.)</p> <p>Note These performance numbers are in laboratory-controlled conditions, against statistically pure noise sources (AWGN). Because such conditions do not exist in practice, a 6 or more dB SNR margin is required for reliable operation. Check with your local system guidelines.</p> | <p>QPSK: >15 dB @ BER<10⁻⁸ (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.)</p> <p>16 QAM: >22 dB @ BER <10⁻⁸ (For 16 QAM, an SNR>22 dB makes the grade for 98% ping efficiency. To get a good packet rate, you need SNR>25 dB).</p> <p>Note These measurements were done for 0 and -10 dBmV input to the CMTS, 1280 ksymb/sec and 64 bytes packet size with a Cisco uBR904 cable access router and laboratory-controlled conditions.</p> |
| Security | <p>DES decryption: DOCSIS Baseline Privacy (BPI), 40 bit- and 56 bit-encryption, as controlled by the headend and configuration files.</p> <p>Note Cisco IOS images must contain encryption software at both the CMTS router and the Cisco uBR904 cable access router. Enable and configure both routers to support encryption.</p> | DES encryption. |

DOCSIS configuration files are created at the headend typically 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 off-line. 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 QoS for all regular data traffic. The class has no minimum upstream rate specified for the channel.

This service class assigns a primary 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 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, however, must define the supported upstream traffic priority levels and include the traffic priority fields in the DOCSIS configuration file downloaded to the Cisco uBR904 cable access 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.

To change the operating mode of the Cisco uBR904 cable access router from its default bridging state, follow the procedure in Table 4.

To configure routing, follow these instructions when in global configuration mode. After you have completed the procedure, enter the **show startup-config** command to verify that routing is enabled.

Table 4 Configuring Operating Modes for the Cisco uBR904 Cable Access Router

| Step | Command | Purpose |
|------|---|---|
| 1 | uBR904(config)# int c 0 | Enter the interface configuration mode for the router interface. |
| 2 | uBR904(config-if)# no cable-modem compliant bridge uBR904(config-if)# no bridge group number and remove bridge-group number. uBR904(config-if)# ip address mask ip address x.x.x.x (0-255) subnet mask x.x.x.x (0-255) uBR904(config-if)# exit | Turn off DOCSIS-compliant bridging. Enable the IP address and subnet. Return to the global configuration mode. |
| 3 | uBR904(config)# int e 0 uBR904(config-if)# no bridge group number and remove bridge-group number. uBR904(config-if)# ip address mask ip address x.x.x.x (0-255) subnet mask x.x.x.x (0-255) uBR904(config-if)# exit | Enter the interface configuration mode for Ethernet 0. Enable the IP address and subnet. Return to the global configuration mode. |
| 4 | uBR904(config)# ip routing | Enable IP routing for the router. |
| 5 | uBR904(config)# router rip uBR904(config)# version 2 rip uBR904(config)# network network-number uBR904(config-if)# exit | Enter the router configuration mode and enable RIP version 2 routing. Specify the network that is connected to the router where RIP will operate. If the router is attached to more than one network, enter each IP address in a separate command. Return to the global configuration mode. |

Table 4 Configuring Operating Modes for the Cisco uBR904 Cable Access Router (continued)

| Step | Command | Purpose |
|------|--|---|
| 6 | uBR904 (config-if) # Ctrl-z | Return to the privileged EXEC mode. |
| | uBR904# copy running-config startup-config Building configuration... | Save the configuration to nonvolatile RAM, so that it will not be lost in the event of a reset, power cycle, or power outage. |

To download an updated Cisco IOS image to a Cisco uBR904 cable access router installed in the field, follow the procedure in “Downloading Specific Cisco IOS Images.”

Downloading Specific Cisco IOS Images

Normally, the CMTS system administrator uses the provisioning and billing system to set the software upgrade filename, the IP address of the TFTP server where the software upgrade file exists, and the MAC address of the Cisco uBR904 cable access router to upgrade in the field. Refer to the procedure that follows.

Option 128 in the DOCSIS configuration file supports a vendor-defined attribute (type = 43) that lets the system administrator define the name of a Cisco IOS image 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 image filename—such as “ios.cfg” file—located in the same TFTP server directory supported by the DOCSIS process.

When the Cisco uBR904 cable access router initializes, Cisco IOS software processes the DOCSIS configuration file. 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 cable access router, the router downloads the new Cisco IOS image from the TFTP server and automatically reboots.

To download an updated Cisco IOS image via a DOCSIS configuration file:

Step 1 Create a file to send to the remote Cisco uBR904 cable access router by using a configuration file editor of your choice. In that file, specify commands such as:

- **hostname SUCCEED**
- **service linenumber**
- **enable password cisco**
- **interface ethernet 0**
- **load 30**
- **no shut**
- **line vty 0 4**
- **password cisco**
- **end**

Step 2 Save the file by using a short name such as “ios.cf.”

Step 3 Ensure that file permissions allow the file to be sent by TFTP.

Note An easy way to do this on UNIX is to make sure the “ios.cfg” file is in /tftpboot; then enter the following command: **chmod 777 ios.cfg**

Step 4 Start an Internet browser, such as NetScape 4.08, and create a generic DOCSIS configuration file by using the Cisco configuration file editor of your choice. Cisco provides a number of tools to help automate this process.

Step 5 Follow the instructions provided in the specific Cisco tool. Select the starting point for your configuration file, for example, bronze.cm, silver.cm, gold.cm, platinum.cm. This populates the configuration file with default provisioning values.

Correctly populate the following two fields:

- Vendor ID (hexadecimal)—The vendor ID field is typically the first three octets of the Cisco uBR904 cable access router’s MAC address as found on the label of the unit.
- Vendor Specific Information Field (dotted-decimal)—This is referred to as the VSIF field.

Note DOCSIS configuration files work on the “TLV” basis—meaning Type, Length, Value. Use the Cisco configuration file editor tool of your choice to help automate the specification. Most Cisco tools include online help.

To download a specific Cisco IOS image to a group of Cisco uBR904 cable access routers, you can define an Organizationally Unique Identifier (OUI) and use this OUI to make the Cisco uBR904 cable access routers pay attention to the Vendor ID and VSIF. A global OUI can be used—“0-0-c.”

- (a) To install a file called “Cisco ios.cf” on 10 Cisco uBR904 cable access routers (assuming a mixture of OUIs exist on those 10 units such as “00-50-7b,” “00-10-7d”, and so on), use the configuration file editor of your choice and specify “0-0-c” in the Vendor ID field.
- (b) Tell the Cisco uBR904 cable access routers that they must get the file called “ios.cf” through TFTP. You do this with the VSIF field. Calculate the “dotted-decimal” equivalent of the ASCII characters: i o s . c f

Use a Sun workstation or any UNIX box and enter:

unix-workstation%man ascii

This prints out the man page. You can find the ASCII-to-decimal conversion chart 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 |

- (c) By using a chart similar to that above, convert the “ios.cf” string letter-by-letter to a decimal value:

| | | | | | |
|-----|-----|-----|----|----|-----|
| i | o | s | . | c | f |
| 105 | 111 | 115 | 46 | 99 | 102 |

- (d) Use the editor of your choice to populate the VSIF field of the DOCSIS configuration file.

Note You cannot directly enter the decimal of “105.111.115.46.99.102” because this is only the “value” part of the TLV. What you actually enter is the sub-type of “128” then, count the length of the word you have chosen for the Cisco IOS image filename.

The “ios.cf” name is used in this example. Thus, the length is 6. Therefore, this is what you enter in the VSIF field: 128.6.105.111.115.46.99.102.

- (e) Save your changes by using the configuration file editor of your choice. Change the “File Name” field selected in Step 5: for example, bronze.cm, silver.cm, gold.cm, platinum.cm, to a different value such as:
/tftpboot/gold-ios-config.cm

Note Do not save this file using the same name as the default that served as your starting point, because this will override the default selected.

- (f) After you have saved the file as “gold-ios-config.cm”, then, FTP back to cs and log in. Make sure you use the binary mode of FTP and choose the file you just created.
- (g) Put the file in the /tftpboot (or equivalent) directory of the TFTP server you are using for your Cisco uBR904 cable access router setup. Enter the following command to ensure you can TFTP the file:
chmod 777 gold-ios-config.cm

- (h) Use a Cisco tool such as CNR to go into your DHCP server and change the value for “packet-file-name” to the new filename you just created: “gold-ios-config.cm.”
- (i) After you have reloaded the CNR DHCP server or the tool you are using, enter the following command from the CMTS:

clear cable modem x.x.x.x reset

The Cisco uBR904 cable access router reregisters with the CMTS. When it gets the new DOCSIS configuration file—“gold-ios-config.cm”—it sends the file “ios.cf” to itself via TFTP.

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



Caution You must Telnet to the unit from the CMTS. If you do not put an enable password and line vty passwords in the ios.cf file you created, then you will not be able to access the unit.

If you entered passwords for enable and vty, you should see something similar to the example shown below when you telnet to the Cisco uBR904 cable access router:

```
UBR7246# telnet 10.1.1.255
Trying 10.1.1.255 ... Open

SUCCEED line 1

User Access Verification

Password:
SUCCEED>en
Password:
SUCCEED#
```

You should see the value of the **hostname** command you put in the ios.cf file “now installed on the Cisco uBR904 cable access router”; and in all other commands.

If you enter **show version** on the Cisco uBR904 cable access router, the Cisco uBR904 cable access router indicates a “HOST CONFIGURATION FILE” has been loaded by using TFTP in the middle of the output. Look at the last line of the example below:

```
System restarted by power-on at 20:23:35 - Tue Jun 15 1999
System image file is "flash:ubr900-y4-mz.113-9.NA", booted via flash
Host configuration file is "ios.cf", booted via tftp from 207.249.162.170
```

You have successfully loaded the Cisco IOS image and DOCSIS configuration file.

Supported MIBs

The Cisco uBR904 cable access router supports the following categories of MIBs:

- SNMP standard MIBs—These are the MIBs required by any agent supporting SNMPv1 or SNMPv2 network management.
- Cisco’s platform and network-layer enterprise 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.

Important Notes

- **Cable-specific MIBs**—These MIBs provide information about the cable interface and related information on the Cisco uBR904 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 uBR904 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.

The *Cable-Specific MIBs* and *Deprecated MIBs* are described in the following sections. For information on the SNMP standard MIBs and Cisco's platform and network-layer enterprise MIBs, see Cisco's MIB web site at <http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>.

Cable-Specific MIBs

Table 5 shows the cable-specific MIBs that are supported on the Cisco uBR904 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. Because of interdependencies, the MIBs must be loaded in the order given in the table.

Note The names given in Table 5 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 *V1SMI* as part of their filenames.

Table 5 Supported MIBs for the Cisco uBR904 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, 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. (This MIB is being updated on a release basis to add RFC2670 support as needed.) | 12.0(4)XI |
| DOCS-BPI-MIB.my | This module—available in an snmpv2 version only—describes the attributes for the DOCSIS-specified Baseline Privacy Interface (BPI) on cable modems and the CMTS. | 12.0(5)T |

Table 5 Supported MIBs for the Cisco uBR904 Cable Access Router (continued)

| MIB Filename | Description | Release |
|--|--|---|
| 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 |
| CABLE-DEVICE-MIB.my CABLE-DEVICE-MIB-V1SMI.my | This module contains generic cable-related objects for DOCSIS-compliant cable modems. | 12.0(4)XI |
| CISCO-CABLE-MODEM-MIB.my | This module—available in an snmpv2 version only—contains the Cisco enterprise objects for DOCSIS-compliant cable modems. | 12.0(4)XI |
| DOCS-CABLE-DEVICE-MIB | This module—available in an snmpv2 version only—is the DOCSIS-specified MIB for DOCSIS-compliant cable modems. | 12.0(4)XI |

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

Table 6 Replacements for Deprecated MIBs

| 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 |

Table 6 Replacements for Deprecated MIBs (continued)

| Deprecated MIB | Replacement MIBs | |
|---------------------|-----------------------|-----------------|
| | SNMPv1 MIB | SNMPv2 MIB |
| OLD-CISCO-TCP-MIB | CISCO-TCP-MIB-V1SMI | CISCO-TCP-MIB |
| OLD-CISCO-TS-MIB | | |
| OLD-CISCO-VINES-MIB | CISCO-VINES-MIB-V1SMI | CISCO-VINES-MIB |
| OLD-CISCO-XNS-MIB | | |

Note Some of the MIBs listed in Table 6 represent feature sets that are not supported on the Cisco uBR904 cable access router.

Caveats

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

For information on caveats in Cisco IOS Release 12.0 T, see *Caveats for Cisco IOS Release 12.0 T*.

All caveats in Release 12.0 are also in Release 12.0 T.

For information on caveats in Cisco IOS Release 12.0, see *Caveats for Cisco IOS Release 12.0*, which lists severity 1 and 2 caveats, 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. You can reach Bug Navigator II on CCO at **Software Center: Cisco IOS Software: Cisco IOS Bug Toolkit: Cisco Bug Navigator II**, or at <http://www.cisco.com/support/bugtools>.

Open Caveats—Cisco IOS Release 12.0(7)T

This section describes possibly unexpected behavior by Cisco IOS Release 12.0(7)T and describes only severity 1 and 2 caveats:

- CSCdp03177

The Cisco uBR904 cable access router does not come up after all four downstreams are combined after upconverter. All of the upstreams of the four cards are combined. When the Cisco uBR904 cable access router is instructed to go to a different downstream, it fails on time of day (TOD) and configuration file. The Cisco uBR904 cable access router gets the correct IP address corresponding to the downstream, but fails to update the default-gateway from the DHCP reply. The Cisco uBR904 repeatedly fails on TOD and configuration file until the gateway address is corrected manually.

Related Documentation

The following sections describe the documentation available for the Cisco uBR904 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.

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

Use these release notes with these documents:

- Release-Specific Documents, page 23
- Platform-Specific Documents, page 24
- Feature Modules, page 24
- Cisco IOS Software Documentation Set, page 24

Release-Specific Documents

The following documents are specific to Release 12.0 and are located on CCO and the Documentation CD-ROM:

- *Cross-Platform Release Notes for Cisco IOS Release 12.0*

On CCO at:

Technical Documents: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 12.0

On the Documentation CD-ROM at:

Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 12.0: 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 12.0 T*

As a supplement to the caveats listed in these release notes, see *Caveats for Cisco IOS Release 12.0* and *Caveats for Cisco IOS Release 12.0 T*, which contains caveats applicable to all platforms for all maintenance releases of Release 12.0 T.

On CCO at:

Technical Documents: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 12.0: Caveats

On the Documentation CD-ROM at:

Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS 12.0: Caveats

Note If you have an account with CCO, you can use Bug Navigator II to find caveats of any severity for any release. You can reach Bug Navigator II on CCO at **Software Center: Cisco IOS Software: Cisco IOS Bug Toolkit: Cisco Bug Navigator II** or at <http://www.cisco.com/support/bugtools>.

Platform-Specific Documents

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*
- *Bridging and Routing Features for the Cisco uBR904 Cable Access Router*
- *Regulatory Compliance and Safety Information for the Cisco uBR904*
- *Troubleshooting Tips for the Cisco uBR904 Cable Access Router*
- *Cisco uBR904 Cable Access Router Subscriber Setup Quick Reference Card*

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 12.0 T, 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 12.0: New Feature Documentation

On the Documentation CD-ROM at:

Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 12.0: 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.

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, 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 12.0: Configuration Guides and Command References

On the Documentation CD-ROM at:

Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 12.0: Configuration Guides and Command References

Release 12.0 Documentation Set

Table 7 describes the contents of the Cisco IOS Release 12.0 software documentation set, which is available in electronic form and in printed form upon request.

You can find the most current Cisco IOS documentation on CCO and the Documentation CD-ROM.

On CCO at:

Technical Documents: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 12.0

On the Documentation CD-ROM at:

Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 12.0

Table 7 Cisco IOS Software Release 12.0 Documentation Set

| Books | Chapter Topics |
|--|---|
| <ul style="list-style-type: none"> • <i>Configuration Fundamentals Configuration Guide</i> • <i>Configuration Fundamentals Command Reference</i> | Configuration Fundamentals Overview Cisco IOS User Interfaces File Management System Management |
| <ul style="list-style-type: none"> • <i>Bridging and IBM Networking Configuration Guide</i> • <i>Bridging and IBM Networking Command Reference</i> | Transparent Bridging Source-Route Bridging Token Ring Inter-Switch Link Remote Source-Route Bridging DLSw+ STUN and BSTUN LLC2 and SDLC IBM Network Media Translation DSPU and SNA Service Point SNA Frame Relay Access Support APPN Cisco Database Connection NCIA Client/Server Topologies Cisco Mainframe Channel Connection Airline Product Set |

Table 7 Cisco IOS Software Release 12.0 Documentation Set (continued)

| Books | Chapter Topics |
|--|--|
| <ul style="list-style-type: none"> • <i>Dial Solutions Configuration Guide</i> • <i>Dial Solutions Command Reference</i> | X.25 over ISDN Appletalk Remote Access Asynchronous Callback, DDR, PPP, SLIP Bandwidth Allocation Control Protocol ISDN Basic Rate Service ISDN Caller ID Callback PPP Callback for DDR Channelized E1 & T1 Dial Backup for Dialer Profiles Dial Backup Using Dialer Watch Dial Backup for Serial Lines Peer-to-Peer DDR with Dialer Profiles DialOut Dial-In Terminal Services Dial-on-Demand Routing (DDR) Dial Backup Dial-Out Modem Pooling Large-Scale Dial Solutions Cost-Control Solutions Virtual Private Dialup Networks Dial Business Solutions and Examples |
| <ul style="list-style-type: none"> • <i>Cisco IOS Interface Configuration Guide</i> • <i>Cisco IOS Interface Command Reference</i> | Interface Configuration Overview LAN Interfaces Logical Interfaces Serial Interfaces |
| <ul style="list-style-type: none"> • <i>Network Protocols Configuration Guide, Part 1</i> • <i>Network Protocols Command Reference, Part 1</i> | IP Overview IP Addressing and Services IP Routing Protocols |
| <ul style="list-style-type: none"> • <i>Network Protocols Configuration Guide, Part 2</i> • <i>Network Protocols Command Reference, Part 2</i> | AppleTalk Novell IPX |
| <ul style="list-style-type: none"> • <i>Network Protocols Configuration Guide, Part 3</i> • <i>Network Protocols Command Reference, Part 3</i> | Network Protocols Overview Apollo Domain Banyan VINES DECnet ISO CLNS XNS |
| <ul style="list-style-type: none"> • <i>Security Configuration Guide</i> • <i>Security Command Reference</i> | AAA Security Services Security Server Protocols Traffic Filtering and Firewalls IP Security and Encryption Passwords and Privileges Neighbor Router Authentication IP Security Options |
| <ul style="list-style-type: none"> • <i>Cisco IOS Switching Services Configuration Guide</i> • <i>Cisco IOS Switching Services Command Reference</i> | Switching Services Switching Paths for IP Networks Virtual LAN (VLAN) Switching and Routing |
| <ul style="list-style-type: none"> • <i>Wide-Area Networking Configuration Guide</i> • <i>Wide-Area Networking Command Reference</i> | Wide-Area Network Overview ATM Frame Relay SMDS X.25 and LAPB |

Table 7 Cisco IOS Software Release 12.0 Documentation Set (continued)

| Books | Chapter Topics |
|--|--|
| <ul style="list-style-type: none"> • <i>Voice, Video, and Home Applications Configuration Guide</i> • <i>Voice, Video, and Home Applications Command Reference</i> | Voice over IP Voice over Frame Relay Voice over ATM Voice over HDLC Frame Relay-ATM Internetworking Synchronized Clocks Video Support Universal Broadband Features |
| <ul style="list-style-type: none"> • <i>Quality of Service Solutions Configuration Guide</i> • <i>Quality of Service Solutions Command Reference</i> | Policy-Based Routing QoS Policy Propagation via BGP Committed Access Rate Weighted Fair Queueing Custom Queueing Priority Queueing Weighted Random Early Detection Scheduling Signaling RSVP Packet Drop Frame Relay Traffic Shaping Link Fragmentation RTP Header Compression |
| <ul style="list-style-type: none"> • <i>Cisco IOS Software Command Summary</i> • <i>Dial Solutions Quick Configuration Guide</i> • <i>System Error Messages</i> • <i>Debug Command Reference</i> | |

Note *Cisco Management Information Base (MIB) User Quick Reference* is no longer published. For the latest list of MIBs supported by Cisco, see *Cisco Network Management Toolkit* on Cisco Connection Online. From CCO, click on the following path: **Service & Support: Software Center: Network Mgmt Products: Cisco Network Management Toolkit: Cisco MIB**.

Service and Support

For service and support for a product purchased from a reseller, contact the reseller, who offers a wide variety of Cisco service and support programs described in “Service and Support” of *Cisco Information Packet* that shipped with your product.

Note If you purchased your product from a reseller, you can access CCO as a guest. CCO is Cisco Systems’ primary real-time support channel. Your reseller offers programs that include direct access to CCO services.

For service and support for a product purchased directly from Cisco, use CCO.

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/serv_tips.shtml

This URL is subject to change without notice. If it changes, point your Web browser to CCO and click on this path: **Products & Technologies: Products: 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.
- Software Products—Contains Cisco IOS Software Bulletins, Cisco TCP/IP Suite 100, General Cisco IOS, Internet/Intranet Applications and Software, Network Management, Network Protection Software Tips, and WAN Switching Products and Software.
- Special Collections—Lists other helpful documents, including Case Studies, References & Request for Comments (RFCs), and Security Advisories.

Cisco Connection Online

Cisco Connection Online (CCO) is Cisco Systems' primary, real-time support channel. Maintenance customers and partners can self-register on CCO to obtain additional information and services.

Available 24 hours a day, 7 days a week, CCO provides a wealth of standard and value-added services to Cisco's customers and business partners. CCO services include product information, product documentation, software updates, release notes, technical tips, the Bug Navigator, configuration notes, brochures, descriptions of service offerings, and download access to public and authorized files.

CCO serves a wide variety of users through two interfaces that are updated and enhanced simultaneously: a character-based version and a multimedia version that resides on the World Wide Web (WWW). The character-based CCO supports Zmodem, Kermit, Xmodem, FTP, and Internet e-mail, and it is excellent for quick access to information over lower bandwidths. The WWW version of CCO provides richly formatted documents with photographs, figures, graphics, and video, as well as hyperlinks to related information.

You can reach CCO in the following ways:

- WWW: <http://www.cisco.com>
- WWW: <http://www-europe.cisco.com>
- WWW: <http://www-china.cisco.com>
- Telnet: cco.cisco.com
- Modem: From North America, 408 526-8070; from Europe, 33 1 64 46 40 82. Use the following terminal settings: VT100 emulation; databits: 8; parity: none; stop bits: 1; and connection rates up to 28.8 kbps.

For a copy of CCO's Frequently Asked Questions (FAQ), contact cco-help@cisco.com. For additional information, contact cco-team@cisco.com.

Note If you are a network administrator and need personal technical assistance with a Cisco product that is under warranty or covered by a maintenance contract, contact Cisco's Technical Assistance Center (TAC) at 800 553-2447, 408 526-7209, or tac@cisco.com. To obtain general information about Cisco Systems, Cisco products, or upgrades, contact 800 553-6387, 408 526-7208, or cs-rep@cisco.com.

Documentation CD-ROM

Cisco documentation and additional literature are available in a CD-ROM package. The Documentation CD-ROM, a member of the Cisco Connection Family, is updated monthly. Therefore, it might be more current than printed documentation. To order copies of the Documentation CD-ROM, contact your local sales representative or call customer service. The CD-ROM package is available as a single package or as an annual subscription. You can also access Cisco documentation on the World Wide Web at <http://www.cisco.com>, <http://www-china.cisco.com>, or <http://www-europe.cisco.com>.

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

This document is to be used in conjunction with the documents listed in the "Related Documentation" section on page 22.

Access Registrar, AccessPath, Any to Any, AtmDirector, Browse with Me, CCDA, CCDE, CCDP, CCIE, CCNA, CCNP, CCSI, CD-PAC, the Cisco logo, Cisco Certified Internetwork Expert logo, *CiscoLink*, the Cisco Management Connection logo, the Cisco *NetWorks* logo, the Cisco Powered Network logo, Cisco Systems Capital, the Cisco Systems Capital logo, Cisco Systems Networking Academy, the Cisco Systems Networking Academy logo, the Cisco Technologies logo, ConnectWay, Fast Step, FireRunner, Follow Me Browsing, FormShare, GigaStack, IGX, Intelligence in the Optical Core, Internet Quotient, IP/VC, Kernel Proxy, MGX, MultiPath Data, MultiPath Voice, Natural Network Viewer, NetSonar, Network Registrar, the Networkers logo, *Packet*, PIX, Point and Click Internetworking, Policy Builder, Precept, ScriptShare, Secure Script, ServiceWay, Shop with Me, SlideCast, SMARTnet, *The Cell*, TrafficDirector, TransPath, ViewRunner, Virtual Loop Carrier System, Virtual Service Node, Virtual Voice Line, VisionWay, VlanDirector, Voice LAN, Wavelength Router, Wavelength Router Protocol, WaRP, WebViewer, Workgroup Director, and Workgroup Stack are trademarks; Changing the Way We Work, Live, Play, and Learn, Empowering the Internet Generation, The Internet Economy, and The New Internet Economy are service marks; and ASIST, BPX, Catalyst, Cisco, Cisco IOS, the Cisco IOS logo, Cisco Systems, the Cisco Systems logo, the Cisco Systems Cisco Press logo, Enterprise/Solver, EtherChannel, EtherSwitch, FastHub, FastLink, FastPAD, FastSwitch, GeoTel, IOS, IP/TV, IPX, LightStream, LightSwitch, MICA, NetRanger, Post-Routing, Pre-Routing, Registrar, StrataView Plus, Stratm, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. or its affiliates in the U.S. and certain other countries. All other trademarks mentioned in this document 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. (9911R)

Copyright © 1999, Cisco Systems, Inc.
All rights reserved.