



Text Part Number: 78-6482-03 Rev.-B0

# Release Notes for Cisco uBR904 Cable Access Router for Cisco IOS Release 12.0 T

---

**August 23, 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(5)T. These release notes are updated as needed to describe new features, memory requirements, hardware support, software platform deferrals, and changes to the microcode or modem code and related documents.

For a list of software caveats that apply to Release 12.0(5)T, see *Caveats for Cisco IOS Release 12.0 T* that accompanies these release notes. This caveats document is updated for every maintenance release and is located on Cisco Connection Online (CCO) and the Documentation CD-ROM.

Use these release notes with *Cross-Platform Release Notes for Cisco IOS Release 12.0* on CCO and the Documentation CD-ROM.

## Contents

These release notes describe the following topics:

- Introduction, page 2
- System Requirements, page 2
- New and Changed Information, page 5
- Important Notes, page 11
- Caveats, page 18
- Related Documentation, page 18
- Service and Support, page 23
- Cisco Connection Online, page 24
- Documentation CD-ROM, page 25

---

### 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 premise 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 ships from the Cisco factory with a Cisco Internetwork Operating System (IOS) software image stored in nonvolatile memory (NVRAM) that supports DOCSIS-compliant bridging data operations. The Cisco uBR904 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 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 Version of Your Software Release, page 3
- Upgrading to a New Software Release, page 3
- Feature Set Tables, page 3

## Memory Requirements

**Table 1** Memory Requirements for the Cisco uBR904

Feature Set	Image Name	Required Flash Memory	Required DRAM Memory	Runs From	Feature Status
<b>IP Routing Standard Feature Sets</b>					
Home Office, DOCSIS Baseline Privacy, Easy IP	ubr900-k1y5-mz	4 MB Flash	8 MB DRAM	RAM	Added in Release 12.0(3)T
Telecommuter, DOCSIS Baseline Privacy, L2TP, Easy IP, IPsec 56	ubr900-k1sy556i-mz	4 MB Flash	8 MB DRAM	RAM	Encryption image added in Release 12.0(3)T
Small Office, DOCSIS Baseline Privacy, Firewall, Easy IP	ubr900-k1oy5-mz	4 MB Flash	8 MB DRAM	RAM	Added in Release 12.0(3)T
Small Office+, DOCSIS Baseline Privacy, Firewall, L2TP, Easy IP, IPsec 56	ubr900-k1osy556i-mz	4 MB Flash	8 MB DRAM	RAM	Encryption image added in Release 12.0(3)T

## Headend Interoperability

To support data feature sets that involve encryption/decryption, Cisco IOS images must contain encryption/decryption software at both the CMTS and the Cisco uBR904. Both the CMTS router and the Cisco uBR904 must be enabled and configured per the software feature set. Should you have the Cisco uBR7200 series equipment, also reference applicable release notes for the corresponding images at the headend that support the feature set.

## Hardware Supported

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

## Determining the Version of Your Software Release

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

```
router>show version
Cisco Internetwork Operating System Software
IOS (tm) 904 Software (UBR900-k1y5-mz), Version 12.0(5)T...
```

## 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 T Upgrade Paths and Packaging Simplification (#819: 1/99)* on CCO at:

### Service & Support: Product Bulletins: Software

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

---

**Note** The Cisco IOS Software Release 12.0 T Upgrade Paths and Packaging Simplification can also be found at this URL: [http://www.cisco.com/warp/public/732/120/819\\_pp.htm](http://www.cisco.com/warp/public/732/120/819_pp.htm). You must have an account on CCO to access this URL.

---

## 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.

**Table 2** Feature Sets Supported by Cisco uBR904

Feature Set	Feature Set Matrix Term	Software Image	Platform
DOCSIS Baseline Privacy, Easy IP	Home Office	ubr900-k1y5-mz	Cisco uBR904
DOCSIS Baseline Privacy, L2TP, Easy IP, IPSec 56	Telecommuter/IP Sec 56	ubr900-k1sy556i-mz	Cisco uBR904
DOCSIS Baseline Privacy, Firewall, Easy IP	Small Office/Firewall	ubr900-k1oy5-mz	Cisco uBR904

**Table 2 Feature Sets Supported by Cisco uBR904 (continued)**

Feature Set	Feature Set Matrix Term	Software Image	Platform
DOCSIS Baseline Privacy, Firewall, L2TP, Easy IP, IPSec 56	Small Office+/Firewall/IP Sec 56	ubr900-k1osy556i-mz	Cisco uBR904

The image subset legend for Tables 1, 2 and 3 appears below:

- k1=DOCSIS baseline privacy
- s=Plus set includes L2TP
- o = Firewall
- y5=reduced IP image w/easy IP functionality
- 56i=56-bit IPSec

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 supports. NAT/PAT is bundled with DHCP server into a feature referred to as "Easy IP."

A boot image supporting DOCSIS-compliant bridging or routing operations ships from the Cisco factory.



**Caution** Cisco IOS images with strong encryption (including, but not limited to, 56-bit 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, you must obtain local import and use authorizations for all encryption strengths. Please contact your sales representative or distributor for more information, or send e-mail to [export@cisco.com](mailto:export@cisco.com).

Table 3 lists the features and feature sets supported by Cisco IOS Release 12.0 T for the Cisco uBR904 cable access router 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 Cisco IOS release that introduced the feature. For example, (3) means the feature was introduced in 12.0(3)T. If the cell in this column is empty, the feature was included in the initial base release.

**Table 3 Feature List by Feature Set**

Feature	Feature Sets				
	In	Home Office, DOCSIS Baseline Privacy, Easy IP	Telecommuter, DOCSIS Baseline Privacy, L2TP, Easy IP, IPSec 56	Small Office, DOCSIS Baseline Privacy, Firewall, Easy IP	Small Office+, DOCSIS Baseline Privacy, Firewall, L2TP, Easy IP, IPSec 56
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
Full and DOCSIS-compliant Bridging	(2)XC	Yes	Yes	Yes	Yes
Routing (RIP V2)	(2)XC	Yes	Yes	Yes	Yes

## New and Changed Information

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

### No New Hardware Features In Release 12.0(5)T

There are no new hardware features supported by the Cisco uBR904 in Cisco IOS Release 12.0(5)T.

### New Software Features in Release 12.0(5)T

#### Enhancements to Bridging Operation

Using previous Cisco IOS images, only 3 PC's can be directly connected to 3 of the 4 Ethernet hub ports at the rear of the Cisco uBR904 and operate correctly in bridging mode. The 3-node directly-connected bridge limit existed due to the MAC chip contained in the unit. The MAC chip reserved 1 filter for the Cisco uBR904's MAC address, leaving 3 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, 4 PCs can be directly connected to 4 Ethernet hub ports or 1 of the 4 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 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 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 in Cisco IOS Release 12.0(3)T.

### New Software Features In Release 12.0(3)T

#### Cisco IOS Firewall Feature Set (Firewall)

The Cisco IOS Firewall feature set, available for a wide range of Cisco router platforms, adds greater depth and flexibility to existing Cisco IOS software security capabilities, enriching features such as authentication, encryption, and failover with robust firewall functionality and intrusion detection. A Cisco IOS software-based, integrated firewall solution scales to meet the bandwidth and performance requirements of any network. It also maximizes a Cisco router investment by combining multiprotocol routing functionality with sophisticated security policy enforcement throughout the network.

The Cisco IOS Firewall feature set delivers cost-effective perimeter security packaged with advanced features like stateful, application-based filtering, dynamic per-user authentication and authorization, defense against network attacks, Java blocking, and real-time alerts. Because it is completely interoperable with Cisco IOS software features including NAT, VPN tunneling protocols, Cisco Express Forwarding (CEF), AAA extensions, Cisco encryption technology, and Cisco IOS IPSec, It is a complete, integrated VPN solution.

### 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:

- The **docsDevBase** group extends the MIB-II “system” group with objects needed for cable device system management.
- The **docsDevNmAccess** group provides a minimum level of SNMP access security.
- The **docsDevSoftware** group provides information for network downloadable software upgrades.
- The **docsDevServer** group provides information about the progress of interaction with various provisioning servers.
- The **docsDevEvent** group provides information about the progress of reporting.
- The **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 Cisco uBR904 cable access router, and the RFI MIB reports statistics on the radio frequency transmissions over the cable television line.

## Cisco Standard MIBs

The Cisco Standard MIBs consists of the following components:

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

---

**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 CCO at: **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 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 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 are translated to the correct private network IP address and routed out the Ethernet interface. This eliminates the need to run RIP on the cable interface.

To implement 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 for the Cisco uBR904 cable access router complies with the DOCSIS standards for interoperable cable modems.

### IPSec Network Security (IPSec)

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 uBR904s.

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.

With IPSec, data can be transmitted across a public network without fear of observation, modification, or spoofing. This enables applications such as virtual private networks (VPNs) 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.

## Layer 2 Tunneling Protocol (L2TP)

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

Traditional dial-up networking services only supported registered IP addresses, which limited the types of applications that could be implemented over Virtual Private Networks (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. 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.

## 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. If set to support 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 NIC-assigned IP addresses by defining VLSMs for network addresses, and it allows CIDR addressing schema.

# Limitations and Restrictions

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

## Bridging Mode

The Cisco uBR904 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 to grant access to CPE devices is controlled by the "MAX CPE" field in the DOCSIS configuration file. The Cisco uBR904 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 to operate as a router. In routing mode, no maximum upper limitation exists. For instructions to change from bridging to routing modem, see the "Important Notes" section of this document.



**Caution** After you connect a laptop PC to the Cisco uBR904 console port and save configuration changes (provided your network supports remote configuration) power cycle the Cisco uBR904 if you're not using the laptop at the subscriber site. This is important when the Cisco uBR904 is configured to operate in a DOCSIS-compliant bridging mode. Power cycling the Cisco uBR904 ensures the laptop PC does not remain in the list of CPE devices at the subscriber site for the Cisco uBR904 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 series 7200 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 (L2TP)

The current 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.

## Important Notes

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

### Supplemental and Corrected Text for the Cisco uBR904 Cable Modem Installation and Configuration Guide

Data transmitted to a Cisco uBR904 cable access router from the CMTS shares a 27 or 26 Mbps, 6 MHz data channel in the 88 to 860 MHz range. The Cisco uBR904 shares an upstream data rate of up to 10 Mbps on a 200kHz-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 4 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
	<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	16 QAM— +8 to +55 dBmV

**Table 4 Cisco uBR904 Cable Access Router Data Specifications (continued)**

Description	Downstream Values	Upstream Values
Signal-to-Noise Ratio (SNR)	<p>64 QAM: &gt;23.5 dB @ BER&lt;10<sup>-8</sup></p> <p>256 QAM*: &gt;30 dB @ BER &lt;10<sup>-8</sup> (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><b>Note</b> These performance numbers are in laboratory-controlled conditions, against statistically pure noise sources (AWGN). Since 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: &gt;15 dB @ BER&lt;10<sup>-8</sup> (QPSK will work at 98% successful ping rate for SNR&gt;13 dB. An SNR of 15 dB is needed to get almost optimal packets per minute transition.)</p> <p>16 QAM: &gt;22 dB @ BER &lt;10<sup>-8</sup> (For 16 QAM, an SNR&gt;22 dB makes the grade for 98% ping efficiency. To get a good packet rate, you need SNR&gt;25 dB).</p> <p><b>Note</b> 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 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><b>Note</b> Cisco IOS images must contain encryption software at both the CMTS and the Cisco uBR904. 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'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 to constantly cycle off-line. Such errors include: wrong downstream frequency, wrong 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 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 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.

- The CMTS system administrator, when creating a DOCSIS configuration file for the Cisco uBR904, 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 from its default bridging state, follow the procedure in Table 5.

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 5 Configuring Operating Modes for the Cisco uBR904 Cable Access Router**

Step	Command	Purpose
1	<code>uBR904(config)#int c 0</code>	Enter the interface configuration mode for the router interface.
2	<code>uBR904(config-if)#no cable-modem compliant bridge</code> <code>uBR904(config-if)#no bridge group number and remove bridge-group number.</code> <code>uBR904(config-if)#ip address mask ip address x.x.x.x (0-255)</code> <code>subnet mask x.x.x.x (0-255)</code> <code>uBR904(config-if)#exit</code>	Turn off DOCSIS-compliant bridging.  Enable the IP address and subnet.  Return to the global configuration mode.
3	<code>uBR904(config)#int e 0</code> <code>uBR904(config-if)#no bridge group number and remove bridge-group number.</code> <code>uBR904(config-if)#ip address mask ip address x.x.x.x (0-255)</code> <code>subnet mask x.x.x.x (0-255)</code> <code>uBR904(config-if)#exit</code>	Enter the interface configuration mode for Ethernet 0.  Enable the IP address and subnet  Return to the global configuration mode.
4	<code>uBR904(config)#ip routing</code>	Enable IP routing for the router.
5	<code>uBR904(config)#router rip</code> <code>uBR904(config)#version 2 rip</code> <code>uBR904(config)#network network-number</code> <code>uBR904(config-if)#exit</code>	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.
6	<code>uBR904(config-if)#Ctrl-z</code>  <code>uBR904#copy running-config startup-config</code> Building configuration...	Return to the privileged EXEC mode.  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 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 file name, the IP address of the TFTP server where the software upgrade file exists, and the MAC address of the Cisco uBR904 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. This requires a unique DHCP policy for the Cisco uBR904, a unique DOCSIS configuration file to be sent by the DOCSIS process, and a unique Cisco IOS image file name—such as "ios.cfg" file—located in the same TFTP server directory supported by the DOCSIS process.

When the Cisco uBR904 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, 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 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'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 uBR904s, you can define an Organizationally Unique Identifier (OUI) and use this OUI to make the Cisco uBR904s pay attention to the Vendor ID and VSIF. A global OUI can be used—"0-0-c".

- To install a file called "Cisco ios.cf" on ten Cisco uBR904s, (assuming a mixture of OUIs exist on those ten 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.
- Tell the Cisco uBR904s 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					

- By using a similar chart as that above, convert the "ios.cf" string letter-by-letter to a decimal value. Here is what you end up with:

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

- Populate the VSIF field of the DOCSIS configuration file by using the editor of your choice.

---

**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 file name.

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) Once 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 setup. Enter the following command to ensure you can TFTP the file:  
**chmod 777 gold-ios-config.cm**
- (h) Go into your DHCP server by using a Cisco tool such as CNR and change the value for "packet-file-name" to the new file name you just created: "gold-ios-config.cm."
- (i) Once 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 reregisters with the CMTS. When it gets the new DOCSIS configuration file—"gold-ios-config.cm"—it TFTP's the file "ios.cf" to itself.

The console port of the Cisco uBR904 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:

```
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; and all other commands.

If you enter **show version** on the Cisco uBR904, the Cisco uBR904 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.

## Deprecated MIBs

Older Cisco Management Information Bases (MIBs) will be replaced in a future release. OLD-CISCO-\* MIBs are currently migrated into more scalable MIBs—without affecting existing Cisco IOS products or NMS applications. You can update from deprecated MIBs to the replacement MIBs as shown in Table 6.

**Table 6**      **Deprecated and Replacement MIBs**

Deprecated MIB	Replacement
OLD-CISCO-APPLETALK-MIB	RFC1243-MIB
OLD-CISCO-CHASSIS-MIB	ENTITY-MIB
OLD-CISCO-CPUK-MIB	In Development
OLD-CISCO-DECNET-MIB	
OLD-CISCO-ENV-MIB	CISCO-ENVMON-MIB
OLD-CISCO-FLASH-MIB	CISCO-FLASH-MIB
OLD-CISCO-INTERFACES-MIB	IF-MIB CISCO-QUEUE-MIB
OLD-CISCO-IP-MIB	
OLD-CISCO-MEMORY-MIB	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
OLD-CISCO-TCP-MIB	CISCO-TCP-MIB
OLD-CISCO-TS-MIB	

**Table 6**            **Deprecated and Replacement MIBs (continued)**

Deprecated MIB	Replacement
OLD-CISCO-VINES-MIB	CISCO-VINES-MIB
OLD-CISCO-XNS-MIB	

---

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

---

## 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* that accompanies these release notes.

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: **Service & Support: Online Technical Support: Software Bug Toolkit** or at <http://www.cisco.com/support/bugtools>.

---

## Related Documentation

The following sections describe the documentation available for the Cisco uBR900 series cable access routers and related documents. These documents consist of hardware and software installation guides, Cisco IOS configuration and command references, system error messages, and 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 Documentation, page 19
- Platform-Specific Documents, page 19
- Feature Modules, page 20
- Cisco IOS Software Documentation Set, page 20

## Release-Specific Documentation

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:

**Service & Support: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 12.0: Release Notes: Cross-Platform Release Notes for Cisco IOS Release 12.0**

On the Documentation CD-ROM:

**Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 12.0: Release Notes: Cross-Platform Release Notes for Cisco IOS Release 12.0**

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

**Service & Support: Technical Documents**

- *Caveats for Cisco IOS Release 12.0 T*

As a supplement to the caveats listed in the “Caveats” section in these release notes, see *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:

**Service & Support: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 12.0: Caveats: Caveats for Cisco IOS Release 12.0 T**

On the Documentation CD-ROM:

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

---

**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: **Service & Support: Online Technical Support: Software Bug Toolkit** or at <http://www.cisco.com/support/bugtools>.

---

## Platform-Specific Documents

The following documents are available for the Cisco uBR904.

- *Cisco uBR904 Cable Access Router Installation and Config. Guide*
- *Update to the uBR904 Cable Access Router Installation and Config. Guide*
- *Bridging and Routing Features for the Cisco uBR904 Cable Access Router*
- *Regulatory Compliance and Safety Info. for the Cisco uBR904*
- *Troubleshooting Tips for the Cisco uBR904 Cable Access Router*
- *Cisco uBR904 Cable Access Router Subscriber Setup Quick Reference Card*

These documents are also available on CCO and the Documentation CD-ROM.

On CCO:

**Service & Support: Documentation Home Page: Cisco Product Documentation: Broadband/Cable Solutions: Cisco uBR900 Series Cable Access Routers**

On the Documentation CD-ROM:

**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:

**Service & Support: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 12.0: New Feature Documentation: New Features in Release 12.0 T:**

On the Documentation CD-ROM:

**Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 12.0: New Feature Documentation: New Features in Release 12.0 T**

## 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, which are shipped with your order in electronic form on the Documentation CD-ROM—unless you specifically ordered the printed versions.

### Documentation Modules

Each module in the Cisco IOS documentation set consists of 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. Each configuration guide can be used in conjunction 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:

**Service & Support: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 12.0: Configuration Guides and Command References: Cisco IOS Interface Configuration Guide or Cisco IOS Interface Command Reference**

On the Documentation CD-ROM:

**Cisco IOS Software Configuration: Cisco IOS Release 12.0: Configuration Guides and Command References: Cisco IOS Interface Configuration Guide or Cisco IOS Interface Command Reference**

## Release 12.0 Documentation Set

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

---

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

---

On CCO:

**Service & Support: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 12.0: Configuration Guides and Command References**

On the Documentation CD-ROM:

**Cisco IOS Software Configuration: Cisco IOS Release 12.0: Configuration Guides and Command References**

**Table 7 Cisco IOS Software Release 12.0 Documentation Set**

Books	Chapter Topics
<ul style="list-style-type: none"> <li>• <i>Configuration Fundamentals Configuration Guide</i></li> <li>• <i>Configuration Fundamentals Command Reference</i></li> </ul>	Configuration Fundamentals Overview Cisco IOS User Interfaces File Management System Management
<ul style="list-style-type: none"> <li>• <i>Bridging and IBM Networking Configuration Guide</i></li> <li>• <i>Bridging and IBM Networking Command Reference</i></li> </ul>	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"> <li>• <i>Dial Solutions Configuration Guide</i></li> <li>• <i>Dial Solutions Command Reference</i></li> </ul>	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"> <li>• <i>Cisco IOS Interface Configuration Guide</i></li> <li>• <i>Cisco IOS Interface Command Reference</i></li> </ul>	Interface Configuration Overview LAN Interfaces Logical Interfaces Serial Interfaces
<ul style="list-style-type: none"> <li>• <i>Network Protocols Configuration Guide, Part 1</i></li> <li>• <i>Network Protocols Command Reference, Part 1</i></li> </ul>	IP Overview IP Addressing and Services IP Routing Protocols
<ul style="list-style-type: none"> <li>• <i>Network Protocols Configuration Guide, Part 2</i></li> <li>• <i>Network Protocols Command Reference, Part 2</i></li> </ul>	AppleTalk Novell IPX
<ul style="list-style-type: none"> <li>• <i>Network Protocols Configuration Guide, Part 3</i></li> <li>• <i>Network Protocols Command Reference, Part 3</i></li> </ul>	Network Protocols Overview Apollo Domain Banyan VINES DECnet ISO CLNS XNS
<ul style="list-style-type: none"> <li>• <i>Security Configuration Guide</i></li> <li>• <i>Security Command Reference</i></li> </ul>	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"> <li>• <i>Cisco IOS Switching Services Configuration Guide</i></li> <li>• <i>Cisco IOS Switching Services Command Reference</i></li> </ul>	Switching Services Switching Paths for IP Networks Virtual LAN (VLAN) Switching and Routing
<ul style="list-style-type: none"> <li>• <i>Wide-Area Networking Configuration Guide</i></li> <li>• <i>Wide-Area Networking Command Reference</i></li> </ul>	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"> <li>• <i>Voice, Video, and Home Applications Configuration Guide</i></li> <li>• <i>Voice, Video, and Home Applications Command Reference</i></li> </ul>	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"> <li>• <i>Quality of Service Solutions Configuration Guide</i></li> <li>• <i>Quality of Service Solutions Command Reference</i></li> </ul>	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"> <li>• <i>Cisco IOS Software Command Summary</i></li> <li>• <i>Dial Solutions Quick Configuration Guide</i></li> <li>• <i>System Error Messages</i></li> <li>• <i>Debug Command Reference</i></li> </ul>	

## 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” in *Cisco Information Packet* 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 Cisco's 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](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 and deploying 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 access 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](http://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](mailto:cco-help@cisco.com). For additional information, contact [cco-team@cisco.com](mailto: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](mailto: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](mailto:cs-rep@cisco.com).

---

## Documentation CD-ROM

Cisco documentation and additional literature are available in a CD-ROM package, which ships with your product. The Documentation CD-ROM, a member of the Cisco Connection Family, is updated monthly. Therefore, it might be more current than printed documentation. To order additional 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 18.

Access Registrar, AccessPath, Any to Any, AtmDirector, 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, ControlStream, Fast Step, FireRunner, GigaStack, IGX, Internet Quotient, Kernel Proxy, MGX, Natural Network Viewer, NetSonar, Network Registrar, *Packet*, PIX, Point and Click Internetworking, Policy Builder, Precept, RouteStream, Secure Script, ServiceWay, SlideCast, SMARTnet, StreamView, *The Cell*, TrafficDirector, TransPath, ViewRunner, VirtualStream, VisionWay, VlanDirector, 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, Registrar, StrataView Plus, Stratm, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries. All other trademarks mentioned in this document 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. (9908R)

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