



Configuring Subscriber-End Broadband Access Router Features

This chapter contains procedures for manually configuring basic functionality on the Cisco uBR900 series cable access routers. For detailed descriptions of the commands used, refer to the *Cisco IOS Multiservice Applications Command Reference* publication.

This chapter includes the following sections:

- Subscriber-End Overview
- Cisco IOS Software Feature Sets
- Subscriber-End Broadband Access Router Data Operations
- Voice over IP Operations
- Subscriber-End Broadband Access Router Security Features
- Subscriber-End Broadband Access Router Configuration Options
- Subscriber-End Broadband Access Router Configuration Restrictions
- Subscriber-End Broadband Access Router Initial Power-Up Sequence
- Subscriber-End Broadband Access Router Basic Troubleshooting
- Subscriber-End Broadband Access Router Configuration Prerequisites
- Subscriber-End Broadband Access Router Configuration Tasks
- Configuring a Host Name and Password
- Configuring Ethernet and Cable Access Router Interfaces
- Configuring Routing
- Configuring Bridging
- Reestablishing DOCSIS-Compliant Bridging
- Customizing the Cable Access Router Interface
- Using Multiple PCs with the Cable Access Router
- Subscriber-End Broadband Access Router Configuration Examples

Subscriber-end Overview

Cisco uBR900 series cable access routers are fully-functional Cisco IOS routers and standards-based bidirectional cable modems that give a residential or small office/home office (SOHO) subscriber high-speed Internet or intranet access and packet telephone services via a shared two-way cable system and IP backbone network. Cisco uBR900 series cable access routers are based on the current Data-over-Cable Service Interface Specifications (DOCSIS) standards, and interoperate with any bidirectional, DOCSIS-qualified headend cable modem termination system (CMTS).

Cisco uBR900 series routers connect computers, telephone equipment, and other customer premises (CPE) devices at a subscriber site to the service provider hybrid fiber-coaxial (HFC) and IP backbone network. Functioning as cable modems, the Cisco uBR900 series routers transport data and voice traffic on the same cable system that delivers broadcast TV signals.

Cisco uBR900 series cable access routers typically ship from the Cisco factory with a Cisco IOS software image stored in NVRAM. The standard Cisco IOS software image supports DOCSIS-compliant bridging operation for data as the default.

Based on the feature licenses purchased, other Cisco IOS images can be downloaded from Cisco Connection Online (CCO). Each Cisco uBR900 series router in your network can then be configured to support Voice over IP (VoIP) or other special operating modes based on your service offering and the practices in place for your network. A Cisco uBR900 series device can function as an advanced router, providing WAN data connectivity in a variety of configurations.

Cisco IOS Software Feature Sets

This section briefly describes the common feature sets supported by the Cisco uBR900 series cable access routers. Each feature set contains a number of features that provide a specific functionality such as VoIP or virtual private network (VPN) access.

The following feature set categories are currently available:

- Data operations
- Data and voice operations

The data and voice feature sets add VoIP support to the same base features contained in the data only feature sets. Telephones that are connected to the Cisco uBR924 cable access router can make voice calls over the Internet using either the H.323 (gateway/gatekeeper) voice control protocol or Simple Gateway Control Protocol (SGCP). (For more information on these protocols, refer to the “H.323 Protocol Stack” and “SGCP Protocol Stack” sections in this chapter.)

Because voice calls are real-time traffic, the Cisco uBR924 cable access router supports the DOCSIS QoS enhancements to give higher priority to IP packets containing voice traffic.



Note

Voice features are available only on the Cisco uBR924 cable access router.



Note

Feature sets and software images vary depending on the cable access router model you are using and the Cisco IOS software release that is running. For a list of the available software images for your application, and the specific features contained in each image, refer to the release notes for the Cisco uBR900 series cable access router and Cisco IOS software release you are using.

The following feature sets are available in data and voice versions as well as in data only versions:

- Base IP Bridging Feature Set provides full DOCSIS 1.0-compliant cable modem support for users who want a basic high-speed connection to the Internet.
- Home Office (Easy IP) Feature Set provides a high-speed connection to the Internet, along with server functions that simplify the administration of IP addresses, so that the Cisco uBR900 series cable access router can connect a small number of computers to the Internet through the cable interface.
- Small Office Feature Set provides a firewall feature set in addition to the high-speed Internet connection and server functions provided by the Home Office feature set. You can protect your office network from intrusion and interference while still having high-speed access to the Internet.
- Telecommuter Feature Set provides encryption and Layer 2 tunneling support in addition to the high-speed Internet connection and server functions provided by the Home Office feature set. Businesses can establish secure high-speed Internet connections between employees' homes and the office local network.

These feature sets are described in the following sections.

Base IP Bridging Feature Set

Base IP Bridging includes full and DOCSIS-compliant bridging and DOCSIS Baseline Privacy. The Base IP Bridging feature set allows the Cisco uBR900 series cable access router to function as a DOCSIS 1.0 cable modem and to interoperate with any DOCSIS 1.0-qualified CMTS. It provides basic high-speed Internet connectivity for users wanting to connect only one computer to the cable network.

DOCSIS-compliant bridging (also referred to as “plug-and-play” bridging) is the default configuration for Cisco uBR900 series cable access routers. While in plug-and-play bridging mode, the router locates a downstream and upstream channel; finds ToD, TFTP, and DHCP servers; obtains an IP address; downloads a DOCSIS configuration file; and obtains DHCP parameters to work in bridging mode.

**Note**

This feature set does not include Easy IP and Routing.

In DOCSIS-compliant bridging mode, the Cisco uBR900 series cable access router acts as a transparent bridge for up to 254 CPE devices.

**Note**

The ability of the Cisco uBR900 series cable access router to grant access to CPE devices is controlled by the MAX CPE field in the DOCSIS configuration file. The MAX CPE field defaults to one CPE device unless otherwise set to a higher number.

Home Office (Easy IP) Feature Set

The Home Office feature set provides high-speed Internet connectivity for customers having a small home network (typically two to four computers). In addition to full DOCSIS 1.0 support and all of the functionality of the Base IP Bridging Feature Set feature set, the Home Office feature set (also known as Easy IP) supports intelligent DHCP server functions, including DHCP Relay Agent and DHCP Client functionality. It also supports Easy IP (NAT/PAT).

This feature set allows the Cisco uBR900 series cable access router great flexibility in administering IP addresses for the PCs and other CPE devices it is connecting to the cable network. The DHCP functionality allows intelligent use of the IP addresses that allow customer premises computers and other equipment to connect to the Internet. The NAT/PAT functionality allows you to use private IP addresses on the local network, while still maintaining connectivity to the Internet.

Small Office Feature Set

In addition to full DOCSIS 1.0 support and all of the functionality of the Easy IP feature set, the Small Office feature set supports the Cisco IOS firewall feature set which provides a wide range of security features for Cisco uBR900 series cable access routers. Using the firewall feature set, Cisco uBR900 series cable access routers act as buffers between private enterprise networks and the Internet and other connected public networks.

In firewall mode, the Cisco uBR900 series cable access router provides a high-speed Internet connection for an office local network while protecting the computers on the office network from common attacks such as denial of service attacks and destructive Java applets. Real-time alerts of attempted attacks are also given.

The Small Office feature set can be extended with support for IPSec encryption to ensure that the traffic passed over the Internet cannot be intercepted. You can select either standard 56-bit IPSec Network Security encryption or high-security 168-bit Triple Data Encryption Standard (DES) encryption.

Telecommuter Feature Set

In addition to full DOCSIS 1.0 support and all of the functionality of the Easy IP feature set, the Telecommuter feature set supports IPSec encryption and the Layer 2 Tunneling Protocol (L2TP), which can establish secure high-speed Internet connections between employee homes and the office local network.

IPSec is an IP security feature that provides robust authentications and encryption of IP packets for the secure transmission of sensitive information over unprotected networks such as the Internet. You can select either standard 56-bit IPSec Network Security encryption or high-security 168-bit Triple DES encryption.

L2TP is an extension of PPP that allows computers on different physical networks to interoperate as if they were on the same LAN. These features are important components for VPNs.

**Note**

The Telecommuter feature set does not require the firewall feature set because the individual telecommuter has a secure connection to the office network. The office network, however, should implement a firewall for its own connection to the Internet.

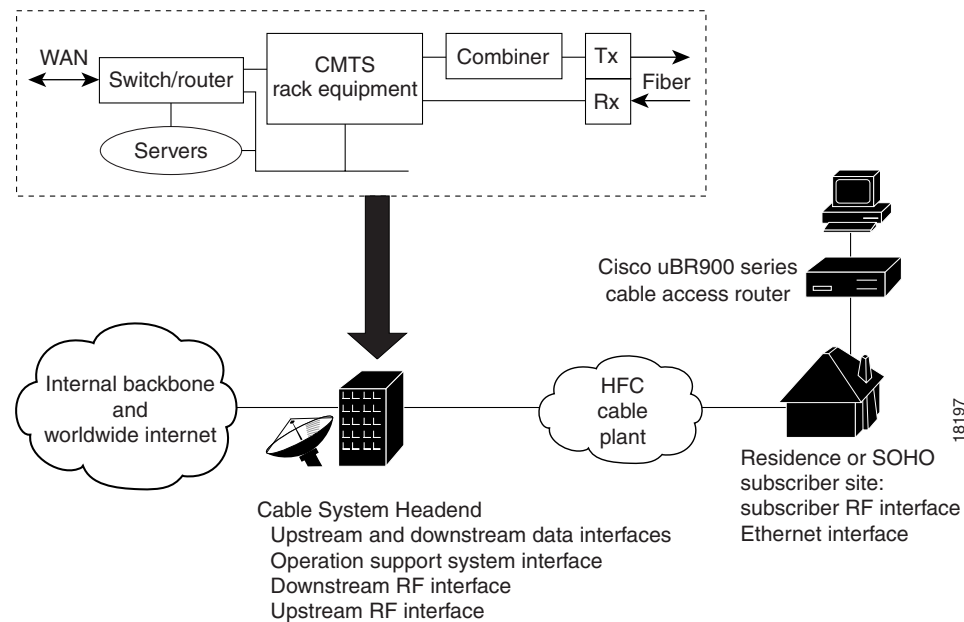
Subscriber-End Broadband Access Router Data Operations

Figure 110 illustrates a typical broadband data cable system. Data transmitted to a Cisco uBR900 series cable access router from the service provider CMTS shares a 27 or 26 Mbps, 6 MHz data channel in the 88 to 860 MHz range. The Cisco uBR900 series 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 server(s), the processing speed and local Ethernet performance of the subscriber computer, and other parameters. Because the network can be configured to support multiple levels of service to meet differing market price/performance requirements, the subscriber service-level agreement also affects throughput. DOCSIS further contains some fundamental performance limitations because standards are designed to give a larger number of customers good performance, rather than permitting a few users to consume the entire capacity.

Figure 110 Typical Cisco Broadband Data Cable System



Operating Modes

The broadband data cable system uses multiple types of access control to ensure efficient use of bandwidth over a wide range of loading conditions. Advanced queuing techniques and service algorithms are used to define the acquisition and release of channels.

Cisco uBR900 series cable access routers support 64 or 256 Quadrature Amplitude Modulation (QAM) downstream, and Quadrature Phase Shift Keying (QPSK) or 16 QAM upstream transmission. The CMTS system administrator can set the preferred modulation scheme based on the quality of the cable plant.

**Note**

In noisy plant environments, 16 QAM upstream and 256 QAM downstream modulation may not be viable. In high-quality HFC networks capable of supporting 16 QAM formats in the upstream direction, we recommend using QPSK for fixed-slot short packets like maintenance or data requests, and 16 QAM for variable-length data packets. This results in the most efficient use of the available upstream timeslots or minislots.

The system uses TCP/IP to transmit data. TCP/IP transmits data in segments encased in IP datagrams, along with checksums to detect data corruption and sequence numbers to ensure an ordered byte stream on the TCP connection between the Cisco cable access router and the CMTS.

Cisco cable access routers also support multicast services—data streams sent to groups of subscribers. These applications utilize the User Datagram Protocol (UDP) instead of TCP. Because UDP does not mandate upstream acknowledgments, these applications can be very efficient in the network. Additionally, restricting upstream throughput will have no effect on downstream UDP streaming throughput.

**Note**

Interactive games are the exception. Although low latency is required in gaming applications, high upstream data throughput is not demanded because the volume of data transmitted upstream is typically small.

Data Specifications

Table 37 provides a summary of the upstream and downstream transmission characteristics of the Cisco uBR900 series cable access routers.

Table 38 Cisco uBR900 Series Cable Access Router Data Specifications





Description	Downstream Values	Upstream Values
Frequency Range	88 to 860 MHz	5 to 42 MHz
Modulation	64 QAM 256 QAM	QPSK 16 QAM
Data Rate	30 Mbps/64 QAM (27 Mbps after FEC overhead) 42.8 Mbps/256 QAM (36 Mbps after FEC overhead)	QPSK—320 kbps to 5 Mbps 16 QAM—640 kbps to 10 Mbps
Bandwidth	6 MHz	200 kHz, 400 kHz, 800 kHz, 1.6 MHz, 3.2 MHz
FEC	RS (122, 128) Trellis	Reed Solomon
One Channel	Receive level of digital signal –15 to +15 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.	QPSK— +8 to +58 dBmV 16 QAM— +8 to +55 dBmV

Table 38 Cisco uBR900 Series 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 from +15 to -8 dBmV, SNR must be greater than 30 dB. For input level from -8 to -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 dB or more 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. A SNR of 15 dB will be needed to get almost optimal packets per minute transition.)</p> <p>16 QAM: >22 dB @ BER <10⁻⁸ (For 16 QAM, a SNR >22 dB makes the grade for 98% ping efficiency. To get good packet rate, you need SNR >25 dB).</p> <p> Note These measurements were made for 0 and -10 dBmV input to the CMTS, 1280 kilosymbols/second, 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, 56-bit, and 168-bit DES encryption, as controlled by the headend and configuration files.</p> <p> Note Cisco IOS images must contain encryption software at both the CMTS and the Cisco uBR900 series. Both routers must be enabled and properly configured to support encryption.</p>	DES encryption

Service Assignments

Each Cisco uBR900 series cable access router on the network is configured to receive data on a particular downstream channel. A downstream channel contains upstream segment(s). Each upstream segment typically serves more than one fiber node.

Partitioning the upstream plant into smaller segments significantly reduces the number of potential ingress sources and failure points. The CMTS divides the cable plant into downstream channels and upstream segments or clusters of nodes.

Downstream and Upstream Data Transfer

When operating normally, the Cisco uBR900 series cable access router receives data addressed to it from the CMTS. The router reads the address in the header of the message, filters the message, and forwards it to the appropriate device at the subscriber site.

**Note**

Bandwidth at the subscriber site is shared by the active data users connected to the network segment.

For upstream data transfer, the Cisco cable access router uses a request/grant mechanism to obtain upstream bandwidth. The CMTS configures, via MAC messages, upstream parameters associated with transmissions from all Cisco cable access routers on the system. Service class registration is granted based on class assignment and load provisioning. Upstream channels are time-slotted and divided into basic scheduling time units.

The CMTS informs the Cisco cable access router of minislots structures on the upstream channel. Some minislots are marked as contention-based—shared by routers to make bandwidth (timeslot) requests with the CMTS. Others are grouped into unicast grants for specific routers to send their data bursts. Yet others are grouped into maintenance slots for keepalive messages from routers to the CMTS.

Bridging Applications

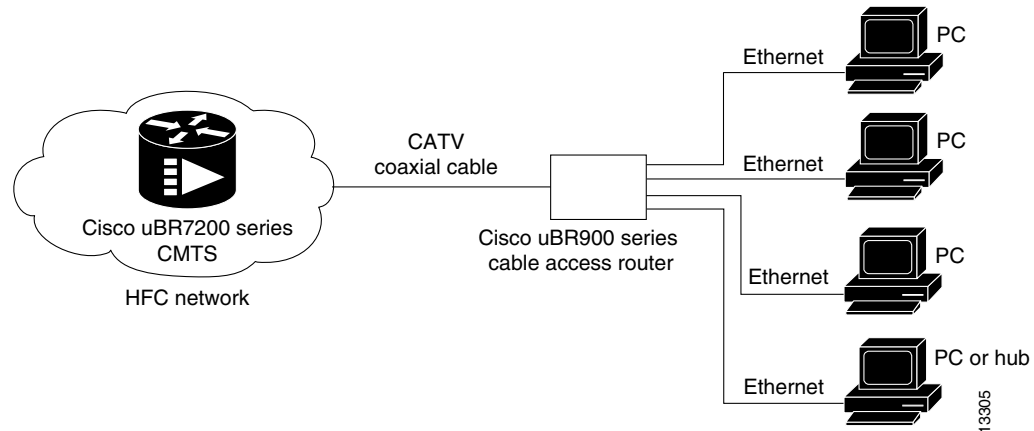
In bridging applications, the Cisco uBR900 series cable access router acts as a transparent bridge for up to 254 devices, depending on the version of Cisco IOS software you are using. Older versions of software allow a maximum of three CPE devices to be bridged. The cable access router is connected to the Internet through the coaxial cable interface. All four 10BaseT Ethernet ports are treated as one Ethernet interface by the Cisco IOS software. The IP addresses for the CPE devices and the coaxial cable interface are typically in the same subnet, although this is not a requirement.

Figure 111 shows the Cisco uBR900 series cable access router in a typical bridging environment. The Cisco uBR900 series complies with the DOCSIS standards for interoperable cable access routers; it supports full transparent bridging and DOCSIS-compliant transparent bridging.

**Note**

If the attached CPE devices and the coaxial cable interface are in different IP subnets, the cable interface must have a secondary address.

Figure 111 Cisco uBR900 Series Cable Access Router in a Bridging Configuration



DOCSIS-compliant transparent bridging is the factory default configuration of the Cisco uBR900 series cable access router. If your cable service provider is using a DHCP server, all you need to do is connect the cables and power on the cable access router; your service provider configuration program will automatically configure both the coaxial cable interface and the bridging functionality. You need not set up IP addresses for the attached PCs or enter any CLI configuration commands. This type of operation is called “plug-and-play” bridging.

In DOCSIS-compliant bridging mode, the cable access router is able to locate a downstream and upstream channel; find the ToD, TFTP, and DHCP server(s); obtain an IP address; download a DOCSIS configuration file; and obtain DHCP parameters to work in a bridging mode.

You can configure a customized bridging application on the Cisco uBR900 series using a downloadable configuration file or the CLI. For details, see the sections “Configuring Bridging” and “Customizing the Cable Access Router Interface” later in this chapter.

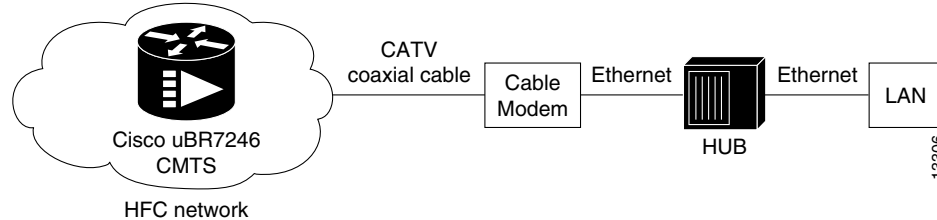
Routing Applications

The Cisco uBR900 series cable access router can be configured to act as a router to preserve IP address space and limit broadcasts that can impact the performance of the network. A typical use would be if you are connecting the cable access router to an internal Ethernet hub that is connected to an existing PC network. The Cisco uBR900 series supports Routing Information Protocol Version 2 (RIP V2) for this application.

When configured in routing mode, the Cisco uBR900 series is automatically configured to use the headend IP address as its IP default gateway. This allows the cable access router to send packets not intended for the Ethernet interface to the headend when IP host-routing is configured.

RIP V2 routing is useful for small internetworks in that it enables optimization of Network Interface Center (NIC)-assigned IP addresses by defining variable-length subnet masks (VLSMs) for network addresses, and it allows classless interdomain routing (CIDR) addressing schema.

Figure 112 Cisco uBR900 Series Cable Access Router in a Routing Configuration with a Hub



L2TP Protocol

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

Traditional dialup 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-initiated tunnel such as L2F.

The current implementation of L2TP in Cisco IOS software is dependent on a PPP connection supported on one of the directly attached interfaces. A dialup PPP connection is required in order to initiate an L2TP tunnel connection. This is a requirement of the L2TP Access Concentrator (LAC). Currently the Cisco uBR900 series 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.

Easy IP

DHCP Server

Cisco uBR900 series cable access routers support 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

Network address translation (NAT) reduces the need for globally unique IP addresses. NAT allows an organization with addresses that are not globally unique to connect to the Internet by translating those addresses into globally routable address space.

Port address translation (PAT) is a similar mechanism that enables all internal hosts to share a single registered IP address (many-to-one translation). When combined, NAT/PAT has the following capabilities:

- 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 uBR900 series 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 PAT)
- Enables packets to be routed correctly to and from the outside world by using the Cisco uBR900 series cable access router
- Allows personal computers on the Ethernet interface to have IP addresses to be mapped to the cable interface 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 NAT on the Cisco uBR900 series, the Ethernet interface is configured with an “inside” address and the cable interface is configured with an “outside” address. The Cisco uBR900 series also supports configuration of static connections, dynamic connections, and address pools.

Voice over IP Operations



Note

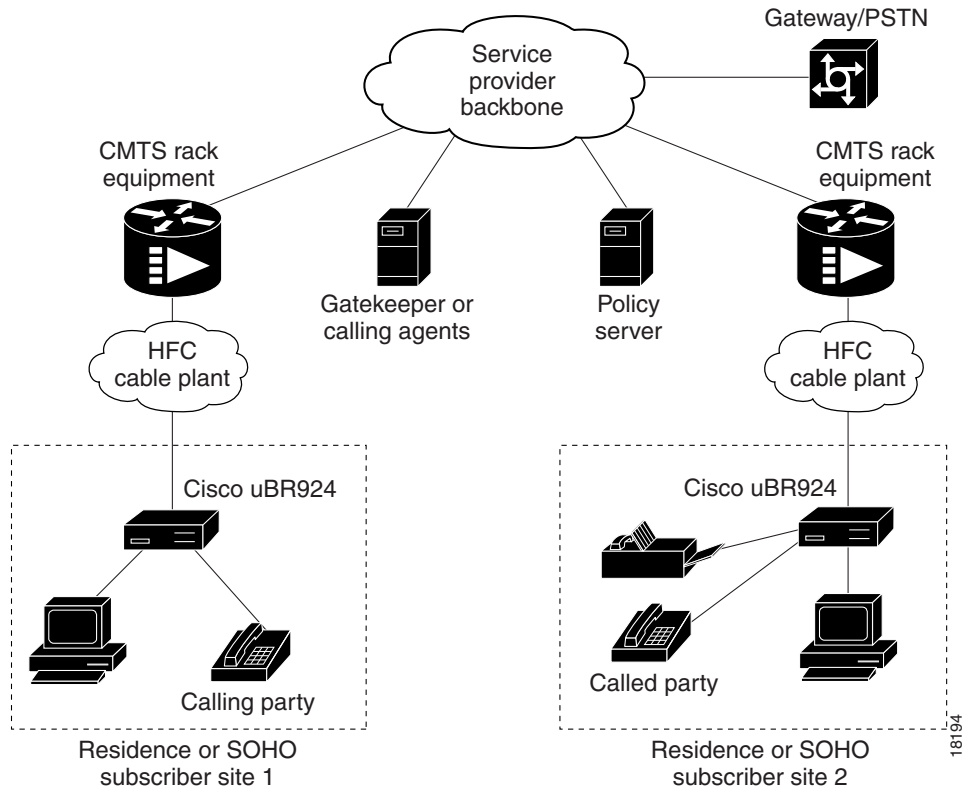
Voice features are available only on the Cisco uBR924 cable access router.

The Cisco uBR924 cable access router uses packets to transmit and receive digitized voice over an IP network. Voice signals are packetized and transported in compliance with H.323 or SGCP. H.323 is an International Telecommunications Union (ITU) standard that specifies call signalling and control protocols for a shared IP data network. SGCP is an alternative to the H.323 protocol that provides signalling and feature negotiation using a remote call agent (CA).

SGCP eliminates the need for a dial plan mapper. It also eliminates the need for static configuration on the router to map IP addresses to telephone numbers because this function is provided by the remote CA.

Figure 113 illustrates a broadband cable system that supports VoIP transmission. QoS and prioritization schemes are used to enable real-time (voice) and nonreal-time traffic to coexist on the same channel. The CMTS routes IP telephony calls intermixed with other data traffic.

Figure 113 Simplified VoIP over Cable Network



You can deploy IP telephony as a local-loop bypass service where voice packets are transferred from the CMTS to one of the following, depending on the signalling protocol used:

- A telephony gatekeeper when using H.323; the Cisco uBR924 acts as an H.323 gateway.
- A call agent when using SGCP.

The gatekeeper or call agents manage voice calls; the gateway interconnects the IP network to the Public Switched Telephone Network (PSTN). The gatekeeper must be running Cisco IOS Release 12.1 or later in order to support registration of the full E.164 address for each Cisco uBR924 port.

Voice calls are digitized, encoded, compressed, and packetized in the originating gateway, then decompressed, decoded, and reassembled in the destination gateway. A server maintains subscriber profiles and policy information.

You can place and receive calls without using the local exchange carrier. Two simultaneous voice and fax calls are supported to and from each subscriber site. Multiple telephones and fax devices can be connected to each of the two VoIP telephone lines at a subscriber site, providing the 5 REN limit is adhered to for each telephone line.

Note the following requirements and characteristics of VoIP applications using the Cisco uBR924 cable access router:

- The telephones at each subscriber site must support touch-tone dialing; rotary dialing is not supported.
- Special telephone features such as call waiting, call forwarding, and conferencing are not supported.
- A two-line telephone can be connected to the V1+V2 port on the Cisco uBR924.

- Fax devices—standard Group III and computer-based Group III machines up to 14,400 baud—are supported in Cisco IOS images that support VoIP.
- In general, fax/modem cards are not supported over VoIP links.

Contact your network management, provisioning, or operations team to determine what your network supports.

Voice Compression and Decompression

The Cisco uBR924 cable access router supports the following compression and decompression algorithms (codecs):

- G.711 A-law 64000 bps
- G.711 U-law 64000 bps
- G.723.1 5300 bps
- G.723.1 6300 bps
- G.726 16000 bps
- G.726 24000 bps
- G.726 32000 bps
- G.728 16000 bps
- G.729 Annex A 8000 bps
- G.729 8000 bps (default codec for telephone calls)

**Note**

Because voice transmission is delay-sensitive, a well-engineered network is critical. Fine-tuning your network to adequately support VoIP typically involves a series of protocols and features geared to support QoS.

To achieve acceptable voice quality and reduce network bandwidth usage, several voice processing techniques and services are employed, including echo cancellation, voice compression, voice activity detection (VAD) or silence compression, and dual tone multifrequency (DTMF) tone detection and generation.

The Cisco uBR924 cable access router supports multiple QoS service IDs (SIDs), enabling multiple classes of service on the cable interface. This enables VoIP and data traffic to be treated separately, with all data assigned to a default class of service, while VoIP traffic is assigned to a different class of service. Thus, voice traffic from the Cisco uBR924 telephone ports can take precedence over the data traffic coming from the Ethernet interfaces.

**Note**

Separate class of service (CoS) streams are only available when the Cisco uBR924 is connected to a CMTS that supports multiple classes of service per router. In addition, the router configuration file must specify the use of multiple classes of service.

If the Cisco uBR924 interoperates with a DOCSIS 1.0 CMTS that does not support multiple CoS per router, voice traffic will be transmitted on a best-effort basis along with data traffic. This may cause poorer voice quality and lower data throughput when calls are being made from the router telephone ports.

The Cisco uBR924 cable access router supports the following service classes:

- The first CoS in the router configuration file is configured as the “Tiered Best Effort Type Class” used by the router as the primary QoS for all regular data traffic. The class has no minimum upstream rate specified for the channel.

This service class results in the assignment of a primary SID for the router. The router uses this SID for all MAC message exchanges with the CMTS, and as a data SID. Any SNMP management traffic from the network to the Cisco uBR924 will also use this SID.

Although this class is strictly best effort, data traffic within this class can be prioritized into eight different priority levels. The CMTS system administrator, however, must define the supported upstream traffic priority levels and include the traffic priority fields in the configuration file downloaded to the Cisco uBR924.

- When creating a configuration for the Cisco uBR924, the CMTS system administrator typically configures extra classes of service. These secondary classes of service are expected to be higher QoS classes and are used by higher priority traffic such as voice. These classes have a minimum upstream rate specified for the channel.

The multiple SID-per-router feature enables the Cisco uBR924 to use multiple SID queues for differentiated services. The Cisco uBR924 diverts voice call traffic to the higher QoS secondary SID, while forwarding best-effort data from the Ethernet interface and MAC messages on the primary SID.

H.323 Protocol Stack

H.323 is an ITU standard that specifies call signalling and control protocols for a shared IP data network. The Cisco uBR924 cable access router acts as an H.323 gateway. In architectures using the VoIP H.323 protocol stack, the session application manages two call legs for each call: a telephony leg managed by the voice telephony service provider; the VoIP leg managed by the cable system operator—the VoIP service provider. Use of the H.323 protocol typically requires a dial plan and mapper at the headend or other server location to map IP addresses to telephone numbers.

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

To make and receive H.323 calls, the Cisco uBR924 cable access router must know the following:

- The IP address of the gateway for the destination dialed. You can configure these IP addresses statically using the **voip dial peer group** CLI commands, or you can obtain these addresses dynamically from the gatekeeper using Registration, Admission, and Status (RAS).
- The telephone numbers of the attached devices. You can configure the telephone numbers attached to the Cisco uBR924 by configuring the IP addresses statically using the **pots port** CLI commands. When using Cisco Network Registrar (CNR) version 3.0 or later with the relay.tcl and setrouter.tcl scripts, you can obtain these addresses dynamically from CNR. The telephone numbers of attached devices are then sent in DHCP response messages. When the Cisco uBR924 processes the DHCP response, it automatically creates the **pots dial peer** for each port, creates the **voip dial peer** for the RAS target, and starts the H.323 RAS gateway support.



Note

To support voice configurations involving Cisco gatekeeper products using RAS, the headend must have IP multicast enabled. The cable interface must be designated as the default for RAS to discover the gatekeeper. The gatekeeper then resolves all dialed destinations sent to the RAS protocol.

SGCP Protocol Stack

The Cisco uBR924 cable access router supports SGCP, an out-of-band signalling protocol that interacts with an external call agent to provide call setup and teardown for VoIP calls made through the Internet or a local intranet. Using the call control agent, SGCP communicates with the voice gateways, allowing you to create a distributed system that enhances performance, reliability, and scalability while still appearing as a single VoIP gateway to external clients. SGCP eliminates the need for a dial plan mapper and static configuration on the router to map IP addresses to telephone numbers because this function is provided by the external call agent.

In architectures using the SGCP protocol stack, the session application implements the gateway functionality defined to support both trunk and residential gateways. The Cisco uBR924 functions in this mode as a residential gateway with two endpoints.

SGCP can preserve signalling System 7 (SS7) style call control information and additional network information such as routing information and authentication, authorization, and accounting (AAA) security information. SGCP allows voice calls to originate and terminate on the Internet; it also allows one end to terminate on the Internet and the other to terminate on a telephone or PBX on the PSTN.


Note

The Cisco uBR924 cable access router supports both H.323 and SGCP call control, but only one method can be active at a time.

Subscriber-End Broadband Access Router Voice Specifications

Table 39 Cisco uBR924 Cable Access Router Voice Specifications

Metric	Value
Loss (between DCS and BTI gateway)	Nominal: 4 dB \pm 0.5 dB (off hook) Nominal: 9 dB \pm 0.5 dB (on hook)
Attenuation distortion: DCS <> BTI (200 Hz to 3.5 kHz) BTI<> DCS (304 Hz to 3004 Hz) DCS -> BTI (204 Hz to 3004 Hz)	Nominal: +1 dB/-3 dB \pm 0.5 dB \pm 0.5 dB0
Idle channel noise	\leq 18 dBmC (noise shall not exceed)
Signal to C-notched noise	\geq 35 dB
Intermodulation distortion: R2 R3	\geq 52 dB \geq 52 dB
Single frequency interference: 0 to 12 kHz 0 to 4 kHz	\leq -28 dBmO \leq -40 dBmO
Frequency shift (offset)	\leq \pm 0.2 Hz (max) \leq \pm 0.1 Hz (99.5%)

Table 39 Cisco uBR924 Cable Access Router Voice Specifications (continued)

Metric	Value
Amplitude tracking (input level, dBmO):	Max Dev. Ave. Dev.
-37 to 0 (on-hook)	<= ±0.5 dB
-37 to +3 (off hook)	<= ±0.5 dB <= ±0.25 dB
-50 to -37 (off-hook)	<= ±1.0dB <= ±0.5 dB
-55 to -50 (off-hook)	<= ±3.0 dB <= ±1.5 dB
Crosstalk	<= -65 dBmO
Amplitude jitter	
20 to 300 Hz	<= 2.5% Peak
4 to 300 Hz	<= 2.9% Peak
Phase jitter	<= 1.5 P-P
20 to 300 Hz	
4 to 300 Hz	<= 1.8 P-P
Envelope delay distortion:	<= 350 usec
1704 Hz to 604 Hz	<= 195 usec
1704 Hz to 2804 Hz	<= 580 usec
1704 Hz to 204 Hz	<= 400 usec
1704 Hz to 3404 Hz	
Hybrid balance:	
Echo Return Loss (ERL)	> 26 dB (standard test line) > 14 dB (station off hook)
SRL	> 21 dB (standard test line) > 11 dB (station off hook)
Clipping:	
Speech segments < 5 ms	< 0.5%
Speech segments > 5ms	0.0%
Impulse noise:	
(>= 6 dB below receive signal)	0 in 93% of all 15 min intervals <= 1 count in all 30 min intervals
Phase hits (>= 10 deg)	0 in 99.75% of all 15 min intervals <= 1 count in all 30 min intervals
Gain hits (>= ± 3 dB)	0 in 99.9% of all 15 min intervals <= 1 count in all 30 min intervals
Dropouts (>= 12)	0 in 99.9% of all 15 min intervals <= 1 count in all 60 min intervals

Backup POTS Connection

The Cisco uBR924 cable access router provides an RJ-11 port (line) that connects to a standard analog telephone wall jack. In the event of a building power failure or a Cisco uBR924 power problem, the cutover port lets you dial out using the backup PSTN line. If the Cisco uBR924 loses power while VoIP calls are in progress, you can reestablish one of the two connections—dialing out over the PSTN.

**Note**

The backup POTS connection enables only one of the VoIP ports on the Cisco uBR924 to function during a power outage. Calls in progress prior to the power outage will be disconnected. If power is reestablished while a cutover call is in progress, the connection will remain in place until the call is terminated. Once the cutover call is terminated, the router automatically reboots.

Subscriber-End Broadband Access Router Security Features

Cisco uBR900 series cable access routers support the security features described in the following sections.

DOCSIS Baseline Privacy

Support for DOCSIS Baseline Privacy in the Cisco uBR900 series is based on the DOCSIS Baseline Privacy Interface Specification (SP-BPI-I01-970922). It provides data privacy across the HFC network by encrypting traffic flows between the cable access router and the 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 uBR900 series 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.

To support encryption/decryption, Cisco IOS images must contain encryption/decryption software at both the CMTS router and the Cisco uBR924 cable access router. Both the CMTS router and the Cisco uBR924 cable access router must be enabled and configured per the software feature set.

IPSec Network Security

IPSec Network Security (IPSec) is an IP security feature that provides robust authentication and encryption of IP packets. IPSec is a framework of open standards developed by the IETF providing security for transmission of sensitive information over unprotected networks such as the Internet. IPSec acts at the network layer (Layer 3), protecting and authenticating IP packets between participating IPSec devices (peers) such as the Cisco uBR900 series cable access router.

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.

Triple Data Encryption Standard

DES is a standard cryptographic algorithm developed by the United States National Bureau of Standards. The Triple DES (3DES) Cisco IOS software release images increase the security from the standard 56-bit IPsec encryption to 168-bit encryption, which is used for highly sensitive and confidential information such as financial transactions and medical records.

Firewall

Cisco uBR900 series cable access routers act as buffers between any connected public and private networks. In firewall mode, Cisco cable access routers use access lists and other methods to ensure the security of the private network.

Cisco IOS firewall-specific security features include the following:

- Context-based Access Control (CBAC). This intelligently filters TCP and UDP packets based on the application-layer protocol. Java applets can be blocked completely, or allowed only from known and trusted sources.
- Detection and prevention of the most common denial of service (DoS) attacks such as ICMP and UDP echo packet flooding, SYN packet flooding, half-open or other unusual TCP connections, and deliberate misfragmentation of IP packets.
- Support for a broad range of commonly used protocols, including H.323 and NetMeeting, FTP, HTTP, MS Netshow, RPC, SMTP, SQL*Net, and TFTP.
- Authentication Proxy for authentication and authorization of web clients on a per-user basis.
- Dynamic Port Mapping. Maps the default port numbers for well-known applications to other port numbers. This can be done on a host-by-host basis or for an entire subnet, providing a large degree of control over which users can access different applications.
- Intrusion Detection System (IDS) that recognizes the signatures of 59 common attack profiles. When an intrusion is detected, IDS can either send an alarm to a syslog server or to a NetRanger Director, drop the packet, or reset the TCP connection.
- User-configurable audit rules.
- Configurable real-time alerts and audit trail logs.

For additional information, see the *Cisco IOS Firewall Feature Set* description in the *Cisco Product Catalog*, or refer to the sections on traffic filtering and firewalls in the *Cisco IOS Security Configuration Guide* and *Cisco IOS Security Command Reference* available on CCO and the Documentation CD-ROM.

NetRanger Support—Cisco IOS Intrusion Detection

NetRanger is an Intrusion Detection System (IDS) composed of the following three parts:

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

Subscriber-End Broadband Access Router Configuration Options

The Cisco uBR900 series cable access router typically ships from the factory ready to work in the Base IP Bridging Feature Set (DOCSIS-compliant bridging) data-only mode. The cable access router is configured automatically at startup by one or more configuration files generated by the cable service provider and downloaded to the router; no configuration or setup is required other than to connect the router to the cable system. The CMTS provides a path from the cable access router to the DHCP server for PC address assignment.

The PCs connected to the Cisco uBR900 series must be configured for IP. Using DHCP, the CMTS assigns an IP subnet address to the cable access router each time it connects to the network. The IP addresses of the cable access router and the individual PCs attached to it enable the CMTS to route data to and from the PCs.

**Note**

When the Cisco uBR900 series cable access router is shipped from the factory, it is configured by default for DOCSIS-compliant bridging.

The configuration file or files downloaded to the Cisco uBR900 series by the CMTS at the headend are dependent on the services purchased by the individual cable service subscriber. The cable access router is provisioned in the following manner:

- When the cable access router is first brought online, the CMTS downloads a binary file to the router that is in DOCSIS-specified format. This file configures the router for the desired level of service and sets other parameters as needed.
- If additional features are required beyond basic DOCSIS-compliant bridging, the DOCSIS configuration file can specify a Cisco IOS image that the CMTS should also download to the router. (To speed up the time required to bring the router online, the cable service provider can preload the Cisco uBR900 series with the appropriate image at the warehouse.)
- To customize the cable access router configuration further, the DOCSIS configuration file can also specify a Cisco IOS configuration file that the CMTS should download to the router. This second configuration file is an ASCII text file that contains the Cisco IOS commands needed to further configure the router as desired.

**Note**

The CMTS typically downloads the DOCSIS configuration file, Cisco IOS image (if needed), and the Cisco IOS configuration file (if needed) only once when the router is initially brought online. However, a new configuration file or image can be downloaded whenever necessary, such as when the cable service provider offers new services or subscribers upgrade their services.

To ensure that you obtain the exact services that you have ordered, the Cisco uBR900 series arrives from the factory with a unique identifier (UID) that consists of a serial number and MAC address. These factory-assigned values are on a label at the bottom of the cable access router; for convenience, these values are also in a barcode label that can be easily scanned for entry into the service provider provisioning and billing system.

Using the MAC address of the cable access router as the key, the CMTS downloads the DOCSIS configuration file and Cisco IOS image that will provide the services that you have purchased. Service technicians at the headend typically create a number of standard configuration files to match the range of services offered by the provider; these configuration files can be created manually or with tools provided for this purpose by Cisco.

The following sections describe the initial power-up and provisioning sequences in more detail, and the requirements that must be met by both the cable access router and the CMTS before provisioning can be successful.

Subscriber-End Broadband Access Router Configuration Restrictions

When using the Cisco uBR900 series cable access router, be aware of the following restrictions and limitations:

- The Cisco uBR900 series is able to implement multiple classes of service (CoS) on the cable interface; however, separate CoS streams are only available when the cable access router is connected to a headend that supports multiple CoS per cable access router. In addition, the configuration file downloaded to the cable access router must specify the use of multiple CoS.
- If the Cisco uBR900 series is connected to a DOCSIS 1.0 headend that does not support multiple CoS per cable access router, voice and data will be mixed, and voice traffic will be transmitted on a best-effort basis. This may cause poorer voice quality and lower data throughput when calls are being made from the cable access router telephone ports. Voice quality is also affected when large files are downloaded or transmitted, and by other substantial network traffic.

**Note**

The Cisco uBR900 series cable access router is typically configured by the headend CMTS. Most cable service providers do not permit local configuration by individual subscribers.

**Note**

Before attempting to reconfigure a Cisco uBR900 series cable access router at a subscriber site, contact your network administrator, provisioning manager, or billing system administrator to ensure that remote configuration is allowed. If remote configuration is disabled, settings you make and save at the local site will not remain in effect after the cable access router is powered down and back up. Instead, settings will return to the previous configuration.

Subscriber-End Broadband Access Router Initial Power-Up Sequence

When connected and first powered up, the Cisco uBR900 series cable access router performs the following boot procedures:

- Boots the ROM from the ROMMON partition of its Flash memory.
- Performs a self-test, initializes processor hardware, and boots the main operating system software—the Cisco IOS release image stored in NVRAM.

Next, the Cisco uBR900 series performs a series of DOCSIS-mandated procedures for automatic installation and configuration. These procedures are summarized in Table 40 and in Figure 114.

Table 40 Cable Access Router Initialization Sequences and Events



Sequence	Event	Description
1.	Scan for a downstream channel and establish synchronization with the CMTS.	<p>The Cisco uBR900 series acquires a downstream channel by matching the clock sync signal that is regularly sent out by the CMTS on the downstream channel. The cable access router saves the last operational frequency in nonvolatile memory and tries to reacquire the saved downstream channel the next time a request is made.</p> <p> Note An ideal downstream signal is one that synchronizes QAM symbol timing, FEC framing, and MPEG packetization, and recognizes downstream sync MAC layer messages.</p>
2.	Obtain upstream channel parameters.	<p>The cable access router waits for an upstream channel descriptor (UCD) message from the CMTS and configures itself for the upstream frequency specified in that message.</p>
3.	Start ranging for power adjustments.	<p>The cable access router waits for the next upstream bandwidth allocation map message (MAP) from the CMTS to find the next shared request timeslot. The router then sends a ranging request message on the next available shared request timeslot, communicating its UID (its unique MAC address) using a temporary SID of 0 (zero) to indicate it has not yet been allocated an upstream channel.</p> <p>In reply to the cable access router ranging request, the CMTS sends a ranging response containing a temporary SID to be used for the initial router configuration and bandwidth allocation. As needed, the router adjusts its transmit power levels using the power increment value given by the CMTS in its ranging response message.</p> <p> Note At this point, the cable access router has established connectivity with the CMTS but is not yet online. The next steps allocate “permanent” upstream and downstream frequencies, and the configuration required for IP network connectivity.</p>

Table 40 Cable Access Router Initialization Sequences and Events (continued)



Sequence	Event	Description
4.	Establish IP connectivity.	<p>After the next MAP message broadcast, the router uses a shared require timeslot to invoke DHCP to establish IP connectivity with the TCP/IP network at the headend.</p> <p>The DHCP server sends a response containing the router IP address and the IP addresses for the default gateway, ToD server, and TFTP server, and the DOCSIS configuration file to be downloaded. Depending on the particular network configuration, other information could be provided, such as the IP addresses for a syslog server or security server.</p> <p> Note The DHCP server is typically a dedicated server at the headend, but it could also be a CMTS such as a Cisco uBR7200 series universal broadband router.</p> <p>The router configures itself for the specified IP address and gets the current date and time from the specified ToD server.</p>
5.	Establish the time of day.	The cable access router accesses the ToD server for the current date and time, which is used to create time stamps for logged events (such as those displayed in the MAC log file).
6.	Establish security.	Full Security, a planned enhancement to Baseline Privacy, is not fully defined nor currently supported by the DOCSIS specification, and is therefore not supported by the Cisco uBR900 series.

Table 40 Cable Access Router Initialization Sequences and Events (continued)

Sequence	Event	Description
7.	Transfer operational parameters.	<p>Using TFTP, the router downloads the specified DOCSIS configuration file and configures itself for the appropriate parameters. The DOCSIS configuration file defines the router operating mode such as the provisioned downstream and upstream service assignments, including assigned frequencies, data rates, modulation schemes, CoS, type of services to support, and other parameters. Cisco provides tools to help automate the creation of configuration files.</p> <p> Note The DOCSIS configuration file must be in the exact format given by the DOCSIS specification. An incorrect DOCSIS configuration file can cause the Cisco uBR900 series to constantly cycle offline. Such errors include wrong downstream frequency, wrong UCD, wrong downstream channel ID, invalid CoS, incorrect BPI privacy configurations or shared secret strings.</p> <p>The cable access router sends another registration request to the CMTS containing the CoS parameters given in the DOCSIS configuration file.</p> <p>The CMTS verifies that the router is using the appropriate CoS profile and converts the temporary SID into a data SID with a service class index that points to the applicable CoS profile.</p>
8.	Perform registration.	The router completes its secondary ranging and is then online, passing data between the HFC network and the PCs and other CPE devices that are connected to the router.
9.	Comply with baseline privacy.	If baseline privacy is configured and enabled on both the router and CMTS, the router and CMTS negotiate the appropriate encryption/decryption parameters and exchange keys for privacy. After encryption is enabled, all information sent within Ethernet packets is encrypted to prevent interception or modification by an unauthorized party.
10.	Enter the operational maintenance state.	As soon as the Cisco uBR900 series cable access router has successfully completed the above sequence, it enters operational maintenance state.

At this point the router is online and operational in the basic DOCSIS bridging (“plug-and-play”) mode. If the DOCSIS configuration file specifies that the router must download a Cisco IOS image and a Cisco IOS configuration file, the router uses TFTP to download the image and configuration file into its local memory. It then installs the new Cisco IOS image and runs the configuration file.

Downloading a DOCSIS configuration file to a Cisco uBR900 series cable access router automatically causes the following actions:

- Ends all Telnet sessions
- Disables the cable access router console port, preventing local access to the CLI
- Performs a write-erase on the cable access router local configuration parameters

Telnet access to the router from the headend is still allowed, but only if the Cisco IOS configuration file includes **enable** and **line vty** passwords; if the configuration file does not include **enable** and **line vty** commands to specify these passwords, Telnet access and console access are both disabled.

The sequence numbers shown in Table 40 are also shown in Figure 114. The Cisco uBR900 series cable access router will complete all the steps shown in the table and flowchart each time it needs to reregister with the CMTS.

Figure 114 Cable Modem Initialization Flowchart

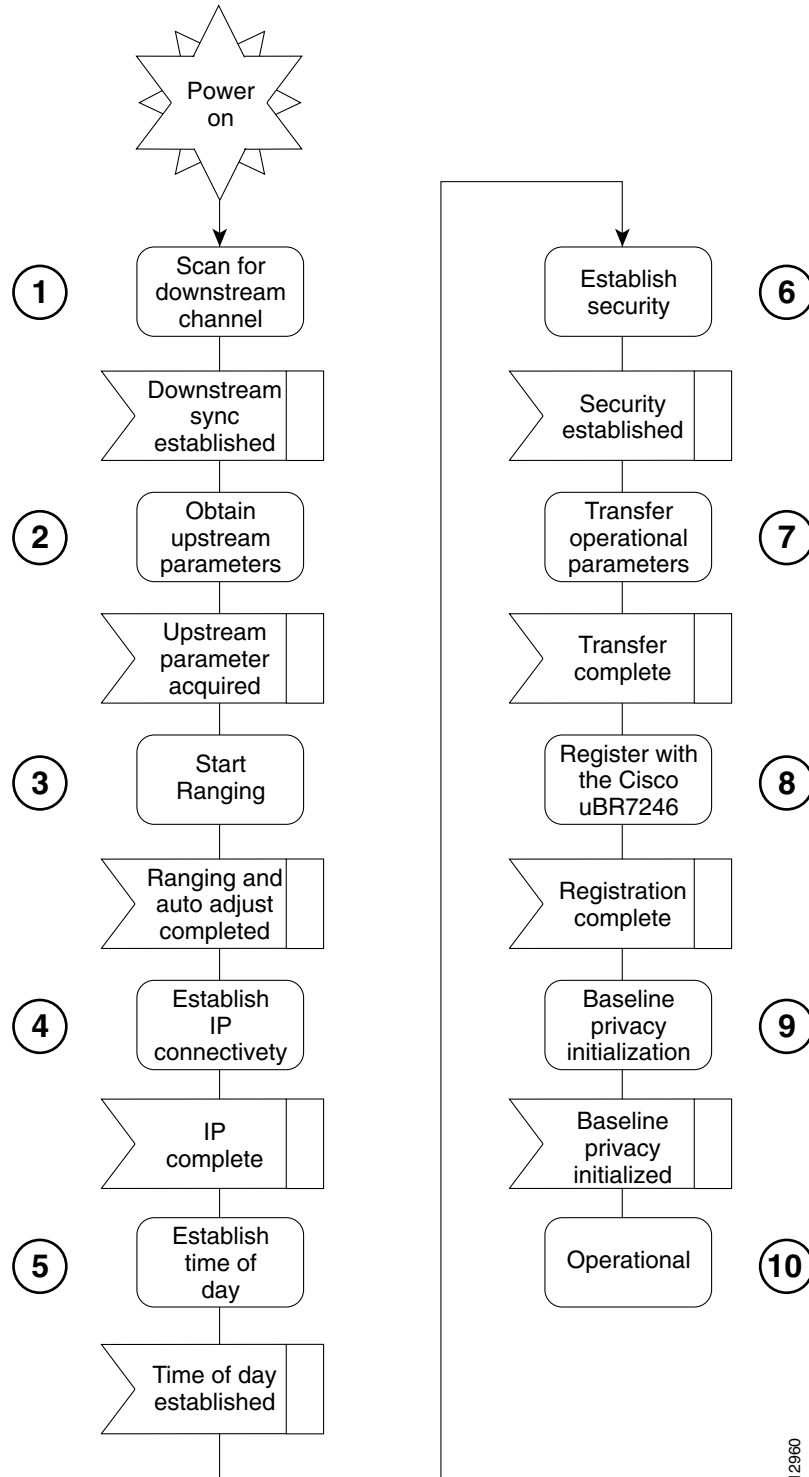
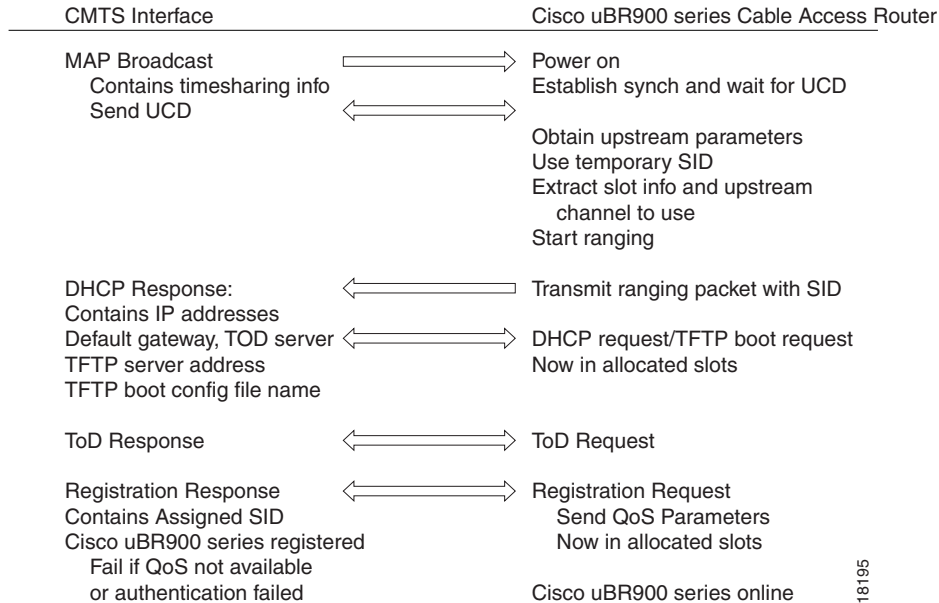


Figure 115 illustrates the traffic flow during the initialization process.

12960

Figure 115 Cisco uBR900 Series Cable Access Router Provisioning Overview

18195

**Note**

For more detail on the provisioning process, see the DOCSIS 1.0 Radio Frequency Interface (RFI) specification (SP-RFII01-990731 or later revision).

After the Cisco uBR900 series cable access router goes online, it begins transferring data between the attached CPE devices and the network (Internet, intranet, VoIP). The cable service provider typically uses DHCP to assign IP addresses to the CPE devices. The number of IP addresses each subscriber can obtain depends on the services purchased from the provider.

Subscriber-End Broadband Access Router Basic Troubleshooting

A MAC-layer circular log file is stored inside the Cisco uBR900 series cable access router. This file contains a history of the log messages such as state event activities and time stamps. This is the most valuable information for troubleshooting the cable interface.

The MAC log file is displayed when you enter the **show controllers cable-modem 0 mac log** command in privileged EXEC mode.

The most useful display fields in this output are the reported state changes. These fields are preceded by the message `CMAC_LOG_STATE_CHANGE`. These fields show how the Cisco uBR900 series progresses through the various processes involved in establishing communication and registration with the CMTS. The normal operational state is `maintenance_state`; the normal state when the interface is shut down is `wait_for_link_up_state`.

**Note**

Because the MAC log file holds only a snapshot of 1023 entries at a time, you should try to display the file within 5 minutes after the reset or problem occurs.

The following is the normal progression of states as the Cisco uBR900 series registers with the CMTS:

```
wait_for_link_up_state
ds_channel_scanning_state
wait_ucd_state
wait_map_state
ranging_1_state
ranging_2_state
dhcp_state
establish_tod_state
security_association_state
configuration_file_state
registration_state
establish_privacy_state
maintenance_state
```

Following is an example of a MAC log file for a cable access router that has successfully registered with the headend CMTS. The output that is displayed is directly related to the messages that are exchanged between the Cisco uBR900 series and the CMTS.

```
uBR924# show controllers cable-modem 0 mac log
508144.340 CMAC_LOG_DRIVER_INIT_IDB_RESET          0x08098FEA
508144.342 CMAC_LOG_LINK_DOWN
508144.344 CMAC_LOG_LINK_UP
508144.348 CMAC_LOG_STATE_CHANGE                  ds_channel_scanning_state
508144.350 CMAC_LOG_WILL_SEARCH_DS_FREQUENCY_BAND 88/453000000/855000000/6000000
508144.354 CMAC_LOG_WILL_SEARCH_DS_FREQUENCY_BAND 89/930000000/105000000/6000000
508144.356 CMAC_LOG_WILL_SEARCH_DS_FREQUENCY_BAND 90/111250000/117250000/6000000
508144.360 CMAC_LOG_WILL_SEARCH_DS_FREQUENCY_BAND 91/231012500/327012500/6000000
508144.362 CMAC_LOG_WILL_SEARCH_DS_FREQUENCY_BAND 92/333015000/333015000/6000000
508144.366 CMAC_LOG_WILL_SEARCH_DS_FREQUENCY_BAND 93/339012500/399012500/6000000
508144.370 CMAC_LOG_WILL_SEARCH_DS_FREQUENCY_BAND 94/405000000/447000000/6000000
508144.372 CMAC_LOG_WILL_SEARCH_DS_FREQUENCY_BAND 95/123015000/129015000/6000000
508144.376 CMAC_LOG_WILL_SEARCH_DS_FREQUENCY_BAND 96/135012500/135012500/6000000
508144.380 CMAC_LOG_WILL_SEARCH_DS_FREQUENCY_BAND 97/141000000/171000000/6000000
508144.382 CMAC_LOG_WILL_SEARCH_DS_FREQUENCY_BAND 98/219000000/225000000/6000000
508144.386 CMAC_LOG_WILL_SEARCH_DS_FREQUENCY_BAND 99/177000000/213000000/6000000
508144.390 CMAC_LOG_WILL_SEARCH_SAVED_DS_FREQUENCY    699000000
508145.540 CMAC_LOG_UCD_MSG_RCVD                    3
508146.120 CMAC_LOG_DS_64QAM_LOCK_ACQUIRED        699000000
508146.122 CMAC_LOG_DS_CHANNEL_SCAN_COMPLETED
508146.124 CMAC_LOG_STATE_CHANGE                  wait_ucd_state
508147.554 CMAC_LOG_UCD_MSG_RCVD                    3
508147.558 CMAC_LOG_UCD_NEW_US_FREQUENCY          20000000
508147.558 CMAC_LOG_SLOT_SIZE_CHANGED             8
508147.622 CMAC_LOG_FOUND_US_CHANNEL              1
508147.624 CMAC_LOG_STATE_CHANGE                  wait_map_state
508148.058 CMAC_LOG_MAP_MSG_RCVD
508148.060 CMAC_LOG_INITIAL_RANGING_MINISLOTS      40
508148.062 CMAC_LOG_STATE_CHANGE                  ranging_1_state
508148.064 CMAC_LOG_RANGING_OFFSET_SET_TO          9610
508148.066 CMAC_LOG_POWER_LEVEL_IS                28.0 dBmV (commanded)
508148.068 CMAC_LOG_STARTING_RANGING
508148.070 CMAC_LOG_RANGING_BACKOFF_SET           0
508148.072 CMAC_LOG_RNG_REQ_QUEUED                0
508148.562 CMAC_LOG_RNG_REQ_TRANSMITTED
508148.566 CMAC_LOG_RNG_RSP_MSG_RCVD
508148.568 CMAC_LOG_RNG_RSP_SID_ASSIGNED          2
508148.570 CMAC_LOG_ADJUST_RANGING_OFFSET          2408
508148.572 CMAC_LOG_ADJUST_OFFSET_SET_TO         12018
508148.574 CMAC_LOG_ADJUST_TX_POWER              20
508148.576 CMAC_LOG_POWER_LEVEL_IS                33.0 dBmV (commanded)
508148.578 CMAC_LOG_STATE_CHANGE                  ranging_2_state
508148.580 CMAC_LOG_RNG_REQ_QUEUED                2
```

```

508155.820 CMAC_LOG_RNG_REQ_TRANSMITTED
508155.824 CMAC_LOG_RNG_RSP_MSG_RCVD
508155.826 CMAC_LOG_ADJUST_RANGING_OFFSET -64
508155.826 CMAC_LOG_RANGING_OFFSET_SET_TO 11954
508155.828 CMAC_LOG_RANGING_CONTINUE
508165.892 CMAC_LOG_RNG_REQ_TRANSMITTED
508165.894 CMAC_LOG_RNG_RSP_MSG_RCVD
508165.896 CMAC_LOG_ADJUST_TX_POWER -9
508165.898 CMAC_LOG_POWER_LEVEL_IS 31.0 dBmV (commanded)
508165.900 CMAC_LOG_RANGING_CONTINUE
508175.962 CMAC_LOG_RNG_REQ_TRANSMITTED
508175.964 CMAC_LOG_RNG_RSP_MSG_RCVD
508175.966 CMAC_LOG_RANGING_SUCCESS
508175.968 CMAC_LOG_STATE_CHANGE dhcp_state
508176.982 CMAC_LOG_DHCP_ASSIGNED_IP_ADDRESS 188.188.1.62
508176.984 CMAC_LOG_DHCP_TFTP_SERVER_ADDRESS 4.0.0.1
508176.986 CMAC_LOG_DHCP_TOD_SERVER_ADDRESS 4.0.0.32
508176.988 CMAC_LOG_DHCP_SET_GATEWAY_ADDRESS
508176.988 CMAC_LOG_DHCP_TZ_OFFSET 360
508176.990 CMAC_LOG_DHCP_CONFIG_FILE_NAME platinum.cm
508176.992 CMAC_LOG_DHCP_ERROR_ACQUIRING_SEC_SVR_ADDR
508176.996 CMAC_LOG_DHCP_COMPLETE
508177.120 CMAC_LOG_STATE_CHANGE establish_tod_state
508177.126 CMAC_LOG_TOD_REQUEST_SENT
508177.154 CMAC_LOG_TOD_REPLY_RECEIVED 3107617539
508177.158 CMAC_LOG_TOD_COMPLETE
508177.160 CMAC_LOG_STATE_CHANGE security_association_state
508177.162 CMAC_LOG_SECURITY_BYPASSED
508177.164 CMAC_LOG_STATE_CHANGE configuration_file_state
508177.166 CMAC_LOG_LOADING_CONFIG_FILE platinum.cm
508178.280 CMAC_LOG_CONFIG_FILE_PROCESS_COMPLETE
508178.300 CMAC_LOG_STATE_CHANGE registration_state
508178.302 CMAC_LOG_REG_REQ_MSG_QUEUED
508178.306 CMAC_LOG_REG_REQ_TRANSMITTED
508178.310 CMAC_LOG_REG_RSP_MSG_RCVD
508178.312 CMAC_LOG_COS_ASSIGNED_SID 5/19
508178.314 CMAC_LOG_COS_ASSIGNED_SID 6/20
508178.316 CMAC_LOG_COS_ASSIGNED_SID 7/21
508178.318 CMAC_LOG_RNG_REQ_QUEUED 19
508178.320 CMAC_LOG_REGISTRATION_OK
508178.322 CMAC_LOG_REG_RSP_ACK_MSG_QUEUED 0
508178.324 CMAC_LOG_STATE_CHANGE establish_privacy_state
508178.326 CMAC_LOG_NO_PRIVACY
508178.328 CMAC_LOG_STATE_CHANGE maintenance_state

```

You can display other aspects of the MAC layer by adding the following keywords to the **show controllers cable-modem 0 mac** command:

```

uBR924# show controllers cable-modem 0 mac ?
  errors      Mac Error Log data
  hardware    All CM Mac Hardware registers
  log         Mac log data
  resets      Resets of the MAC
  state       Current MAC state

```

For examples and descriptions of how to use these keywords, see the **show controllers cable-modem mac** command reference page in the *Cisco IOS Multiservice Applications Command Reference* publication.

The MAC log file gives a detailed history of initialization events that occur in the Cisco uBR900 series cable access router. All pertinent troubleshooting information is stored here.

In the following paragraphs, a sample log file is broken down into the chronological sequence of events listed below. Sample comments are also included in the log file.

- Event 1—Wait for the Link to Come Up
- Event 2—Scan for a Downstream Channel, then Synchronize
- Event 3—Obtain Upstream Parameters
- Event 4—Start Ranging for Power Adjustments
- Event 5—Establish IP Connectivity
- Event 6—Establish the Time of Day
- Event 7—Establish Security
- Event 8—Transfer Operational Parameters
- Event 9—Perform Registration
- Event 10—Comply with Baseline Privacy
- Event 11—Enter the Maintenance State

Event 1—Wait for the Link to Come Up

When the Cisco uBR900 series cable access router is powered up and begins initialization, the MAC layer first informs the cable access router drivers that it needs to reset. The `LINK_DOWN` and `LINK_UP` fields are similar to the shut and no shut conditions on a standard Cisco interface.

```
uBR924# show controllers cable-modem 0 mac log
528302.040 CMAC_LOG_LINK_DOWN
528302.042 CMAC_LOG_RESET_FROM_DRIVER
528302.044 CMAC_LOG_STATE_CHANGE                wait_for_link_up_state
528302.046 CMAC_LOG_DRIVER_INIT_IDB_SHUTDOWN    0x08098D02
528302.048 CMAC_LOG_LINK_DOWN
528308.428 CMAC_LOG_DRIVER_INIT_IDB_RESET      0x08098E5E
528308.432 CMAC_LOG_LINK_DOWN
528308.434 CMAC_LOG_LINK_UP
```

Event 2—Scan for a Downstream Channel, then Synchronize

Different geographical regions and different cable plants use different RF frequency bands. A frequency band is a group of adjacent 6 MHz-wide channels. These bands are numbered from 88 to 99. Each band has starting and ending digital carrier frequencies and a 6 MHz step size. For example, a search of EIA channels 95 to 97 is specified using band 89. The starting frequency of band 89 is 93 MHz; the ending frequency is 105 MHz.

The Cisco uBR900 series' default frequency bands correspond to the North American EIA CATV channel plan for 6 MHz channel slots from 90 to 858 MHz. For example, EIA channel 95 occupies the 90-to-96 MHz slot. The digital carrier frequency is specified as the center frequency of the slot, which is 93 MHz. Channel 95 is usually specified using the analog video carrier frequency of 91.25 MHz, which lies 1.75 MHz below the center of the slot.

Some CATV systems use alternative frequency plans such as the Incrementally Related Carrier (IRC) plan and Harmonically Related Carrier (HRC) plan. Cisco uBR900 series cable access routers support both of these plans. Most of the IRC channel slots overlap the EIA plan.

The Cisco uBR900 series uses a built-in default frequency scanning feature to find and lock onto a downstream channel. After the cable access router successfully finds a downstream frequency channel, it saves the channel to NVRAM. The router recalls this value the next time it needs to synchronize its frequency.

The downstream frequency search table is arranged so that the first frequencies that are scanned are above 450 MHz. Because many CATV systems have been upgraded from 450 MHz to 750 MHz coaxial cable, digital channels have a high chance of being assigned in the new spectrum. The search table omits channels below 90 MHz and above 860 MHz because the DOCSIS specification does not mandate their coverage.

The `CMAC_LOG_WILL_SEARCH_DS_FREQUENCY_BAND` field tells you which frequencies the cable access router will scan. The `CMAC_LOG_WILL_SEARCH_SAVED_DS_FREQUENCY` field tells you the frequency the router locked onto and saved to NVRAM for future recall. The `CMAC_LOG_DS_64QAM_LOCK_ACQUIRED` field communicates the same information. The `CMAC_LOG_DS_CHANNEL_SCAN_COMPLETED` field indicates that the scanning and synchronization was successful.

```
508144.348 CMAC_LOG_STATE_CHANGE ds_channel_scanning_state
508144.350 CMAC_LOG_WILL_SEARCH_DS_FREQUENCY_BAND 88/453000000/855000000/6000000
508144.354 CMAC_LOG_WILL_SEARCH_DS_FREQUENCY_BAND 89/93000000/105000000/6000000
508144.356 CMAC_LOG_WILL_SEARCH_DS_FREQUENCY_BAND 90/111250000/117250000/6000000
508144.360 CMAC_LOG_WILL_SEARCH_DS_FREQUENCY_BAND 91/231012500/327012500/6000000
508144.362 CMAC_LOG_WILL_SEARCH_DS_FREQUENCY_BAND 92/333015000/333015000/6000000
508144.366 CMAC_LOG_WILL_SEARCH_DS_FREQUENCY_BAND 93/339012500/399012500/6000000
508144.370 CMAC_LOG_WILL_SEARCH_DS_FREQUENCY_BAND 94/405000000/447000000/6000000
508144.372 CMAC_LOG_WILL_SEARCH_DS_FREQUENCY_BAND 95/123015000/129015000/6000000
508144.376 CMAC_LOG_WILL_SEARCH_DS_FREQUENCY_BAND 96/135012500/135012500/6000000
508144.380 CMAC_LOG_WILL_SEARCH_DS_FREQUENCY_BAND 97/141000000/171000000/6000000
508144.382 CMAC_LOG_WILL_SEARCH_DS_FREQUENCY_BAND 98/219000000/225000000/6000000
508144.386 CMAC_LOG_WILL_SEARCH_DS_FREQUENCY_BAND 99/177000000/213000000/6000000
508144.390 CMAC_LOG_WILL_SEARCH_SAVED_DS_FREQUENCY 699000000
508145.540 CMAC_LOG_UCD_MSG_RCVD 3
508146.120 CMAC_LOG_DS_64QAM_LOCK_ACQUIRED 699000000
508146.122 CMAC_LOG_DS_CHANNEL_SCAN_COMPLETED
```

Event 3—Obtain Upstream Parameters

The Cisco uBR900 series waits for an upstream channel descriptor (UCD) message from the CMTS. The UCD provides transmission parameters for the upstream channel.

```
508146.124 CMAC_LOG_STATE_CHANGE wait_ucd_state
508147.554 CMAC_LOG_UCD_MSG_RCVD 3
508147.558 CMAC_LOG_UCD_NEW_US_FREQUENCY 20000000
508147.558 CMAC_LOG_SLOT_SIZE_CHANGED 8
508147.622 CMAC_LOG_FOUND_US_CHANNEL 1
508147.624 CMAC_LOG_STATE_CHANGE wait_map_state
508148.058 CMAC_LOG_MAP_MSG_RCVD
508148.060 CMAC_LOG_INITIAL_RANGING_MINISLOTS 40
```

Event 4—Start Ranging for Power Adjustments

The ranging process adjusts the transmit power of the cable access router. Ranging is performed in two stages: ranging state 1 and ranging state 2.

The `CMAC_LOG_POWER_LEVEL_IS` field is the power level that the CMTS told the Cisco uBR900 series to adjust to. The `CMAC_LOG_RANGING_SUCCESS` field indicates that the ranging adjustment was successful.

```

508148.062 CMAC_LOG_STATE_CHANGE          ranging_1_state
508148.064 CMAC_LOG_RANGING_OFFSET_SET_TO  9610
508148.066 CMAC_LOG_POWER_LEVEL_IS       28.0  dBmV (commanded)
508148.068 CMAC_LOG_STARTING_RANGING
508148.070 CMAC_LOG_RANGING_BACKOFF_SET   0
508148.072 CMAC_LOG_RNG_REQ_QUEUED       0
508148.562 CMAC_LOG_RNG_REQ_TRANSMITTED
508148.566 CMAC_LOG_RNG_RSP_MSG_RCVD
508148.568 CMAC_LOG_RNG_RSP_SID_ASSIGNED  2
508148.570 CMAC_LOG_ADJUST_RANGING_OFFSET 2408
508148.572 CMAC_LOG_RANGING_OFFSET_SET_TO 12018
508148.574 CMAC_LOG_ADJUST_TX_POWER      20
508148.576 CMAC_LOG_POWER_LEVEL_IS       33.0  dBmV (commanded)
508148.578 CMAC_LOG_STATE_CHANGE          ranging_2_state
508148.580 CMAC_LOG_RNG_REQ_QUEUED       2
508155.820 CMAC_LOG_RNG_REQ_TRANSMITTED
508155.824 CMAC_LOG_RNG_RSP_MSG_RCVD
508155.826 CMAC_LOG_ADJUST_RANGING_OFFSET -64
508155.826 CMAC_LOG_RANGING_OFFSET_SET_TO 11954
508155.828 CMAC_LOG_RANGING_CONTINUE
508165.892 CMAC_LOG_RNG_REQ_TRANSMITTED
508165.894 CMAC_LOG_RNG_RSP_MSG_RCVD
508165.896 CMAC_LOG_ADJUST_TX_POWER      -9
508165.898 CMAC_LOG_POWER_LEVEL_IS       31.0  dBmV (commanded)
508165.900 CMAC_LOG_RANGING_CONTINUE
508175.962 CMAC_LOG_RNG_REQ_TRANSMITTED
508175.964 CMAC_LOG_RNG_RSP_MSG_RCVD
508175.966 CMAC_LOG_RANGING_SUCCESS

```

Event 5—Establish IP Connectivity

After ranging is complete, the cable interface on the cable access router is UP. Now the cable access router accesses a remote DHCP server to get an IP address. The DHCP server sends a response containing the router IP address plus the TFTP server address, the ToD server address, and the name of a configuration file containing additional configuration parameters. The `CMAC_LOG_DHCP_COMPLETE` field shows that the IP connectivity was successful.

```

508175.968 CMAC_LOG_STATE_CHANGE          dhcp_state
508176.982 CMAC_LOG_DHCP_ASSIGNED_IP_ADDRESS 188.188.1.62
508176.984 CMAC_LOG_DHCP_TFTP_SERVER_ADDRESS 4.0.0.1
508176.986 CMAC_LOG_DHCP_TOD_SERVER_ADDRESS 4.0.0.32
508176.988 CMAC_LOG_DHCP_SET_GATEWAY_ADDRESS
508176.988 CMAC_LOG_DHCP_TZ_OFFSET          360
508176.990 CMAC_LOG_DHCP_CONFIG_FILE_NAME  platinum.cm
508176.992 CMAC_LOG_DHCP_ERROR_ACQUIRING_SEC_SVR_ADDR
508176.996 CMAC_LOG_DHCP_COMPLETE

```

Event 6—Establish the Time of Day

The Cisco uBR900 series accesses the ToD server for the current date and time, which is used to create time stamps for logged events. The `CMAC_LOG_TOD_COMPLETE` field indicates a successful time of day sequence.

```
508177.120 CMAC_LOG_STATE_CHANGE          establish_tod_state
508177.126 CMAC_LOG_TOD_REQUEST_SENT
508177.154 CMAC_LOG_TOD_REPLY_RECEIVED    3107617539
508177.158 CMAC_LOG_TOD_COMPLETE
```

Event 7—Establish Security

This event is currently bypassed by the Cisco uBR900 series because “full security” has not been fully defined by DOCSIS and is therefore not yet supported.

```
508177.160 CMAC_LOG_STATE_CHANGE          security_association_state
508177.162 CMAC_LOG_SECURITY_BYPASSED
```

**Note**

“Full security” was a request made by cable service providers for a very strong authorization and authentication check by the CMTS. The Cisco uBR900 series supports DOCSIS Baseline Privacy (Event 10), which protects your data from being “sniffed” on the cable network.

Event 8—Transfer Operational Parameters

After completing the DHCP and security operations, the Cisco uBR900 series downloads operational parameters by downloading a configuration file located on the TFTP server. The `CMAC_LOG_DHCP_CONFIG_FILE_NAME` field shows the filename containing the transmission parameters.

```
508177.164 CMAC_LOG_STATE_CHANGE          configuration_file_state
508177.166 CMAC_LOG_LOADING_CONFIG_FILE  platinum.cm
508178.280 CMAC_LOG_CONFIG_FILE_PROCESS_COMPLETE
```

Event 9—Perform Registration

After the Cisco uBR900 series is initialized, authenticated, and configured, it requests to be registered with the headend CMTS. The `CMAC_LOG_COS_ASSIGNED_SID` field assigns a CoS number and a SID. Multiple CoS entries in the configuration file imply that multiple SIDs are supported by the cable access router. If several cable access routers use the same configuration file, they will have the same CoS numbers but will be assigned different SIDs.

A successful registration is indicated by the `CMAC_LOG_REGISTRATION_OK` field.

```
508178.300 CMAC_LOG_STATE_CHANGE          registration_state
508178.302 CMAC_LOG_REG_REQ_MSG_QUEUED
508178.306 CMAC_LOG_REG_REQ_TRANSMITTED
508178.310 CMAC_LOG_REG_RSP_MSG_RCVD
508178.312 CMAC_LOG_COS_ASSIGNED_SID    5/19
508178.314 CMAC_LOG_COS_ASSIGNED_SID    6/20
508178.316 CMAC_LOG_COS_ASSIGNED_SID    7/21
508178.318 CMAC_LOG_RNG_REQ_QUEUED      19
508178.320 CMAC_LOG_REGISTRATION_OK
```


Event 10—Comply with Baseline Privacy

During this event, keys for baseline privacy are exchanged between the Cisco uBR900 series and the headend CMTS. A link level encryption is performed so that your data cannot be “sniffed” by anyone else on the cable network.

Following is a trace showing Baseline Privacy enabled. The key management protocol is responsible for exchanging two types of keys: KEKs and TEKs. The KEK, also referred to as the authorization key, is used by the CMTS to encrypt the TEKs it sends to the Cisco uBR900 series. The TEKs are used to encrypt/decrypt the data. There is a TEK for each SID that is configured to use privacy.

```

851.088 CMAC_LOG_STATE_CHANGE                establish_privacy_state
851.094 CMAC_LOG_PRIVACY_FSM_STATE_CHANGE     machine: KEK, event/state:
EVENT_1_PROVISIONED/STATE_A_START, new state: STATE_B_AUTH_WAIT
851.102 CMAC_LOG_BPKM_REQ_TRANSMITTED
851.116 CMAC_LOG_BPKM_RSP_MSG_RCVD
851.120 CMAC_LOG_PRIVACY_FSM_STATE_CHANGE     machine: KEK, event/state:
EVENT_3_AUTH_REPLY/STATE_B_AUTH_WAIT, new state: STATE_C_AUTHORIZED
856.208 CMAC_LOG_PRIVACY_FSM_STATE_CHANGE     machine: TEK, event/state:
EVENT_2_AUTHORIZED/STATE_A_START, new state: STATE_B_OP_WAIT
856.220 CMAC_LOG_BPKM_REQ_TRANSMITTED
856.224 CMAC_LOG_BPKM_RSP_MSG_RCVD
856.230 CMAC_LOG_PRIVACY_FSM_STATE_CHANGE     machine: TEK, event/state:
EVENT_8_KEY_REPLY/STATE_B_OP_WAIT, new state: STATE_D_OPERATIONAL
856.326 CMAC_LOG_PRIVACY_INSTALLED_KEY_FOR_SID 2
856.330 CMAC_LOG_PRIVACY_ESTABLISHED

```

**Note**

In order for Baseline Privacy to work, you must use a code image name on the Cisco uBR900 series that contains the characters **k1**. In addition, Baseline Privacy must be supported on the headend CMTS, and it must be turned on in the configuration file that is downloaded to the cable access router.

Event 11—Enter the Maintenance State

As soon as the Cisco uBR900 series has successfully completed the above events, it enters the operational maintenance state and is authorized to forward traffic into the cable network.

```
508178.322 CMAC_LOG_STATE_CHANGE                maintenance_state
```

Subscriber-End Broadband Access Router Configuration Prerequisites

In order to use the Cisco uBR900 series cable access router for data-over-cable or voice-over-cable (VoIP) applications, the following tasks must be performed:

- All required CMTS routing and network interface equipment must be installed, configured, and operational. This includes all headend routers, servers (DHCP, TFTP, and ToD), network management systems, or other configuration or billing systems in use in your network.
- Based on the quality and capacity of your cable plant, your system administrator or network planner must define your network IP address allocation plan, spectrum management plan outlining the recommended operating parameters to optimize performance, channel plan identifying the channels available to assign to specific Cisco uBR900 series cable access routers, and dial plan based on the supported VoIP protocol.

- The CMTS system administrator or appropriate personnel must specify the policy parameters for the Cisco uBR900 series and all computers and other customer premises devices to be supported at subscriber sites. Refer to the Cisco CNR product documentation.
- The CMTS system administrator or appropriate personnel must define and push DHCP and Cisco uBR900 series configuration files to the appropriate servers such that each cable access router, when initialized, can transmit a DHCP request, receive its IP address, obtain its TFTP and ToD server addresses, and download its configuration file (and updated Cisco IOS image, if required).

**Note**

The MAC address on the cable access router ensures that each router downloads only the file(s) intended for it.

- The Cisco uBR900 series cable access router must be physically installed and cabled as follows:
 - To the headend via CATV coaxial cable. (High-quality, shielded RF coaxial cable with at least 80 percent braid is recommended.)
 - To at least one PC via the straight-through yellow Ethernet cable supplied with the cable access router. Refer to the appropriate cable access router quick start guide for detailed information.

**Note**

When the Cisco uBR900 series is connected to an Ethernet hub, a crossover cable must be used. Category 5 UTP (10BaseT Ethernet) cable with RJ-45 connectors is recommended.

**Note**

For subscriber sites that support multiple telephones or fax devices on a telephone line, all wiring associated with the telephone line extension must be in place. Inside wiring must be in compliance with the country of operation to prevent degradation of service.

- The CMTS system administrator must ensure that appropriate databases are updated to activate and support the new subscriber account in the provisioning, billing, or network management systems in place for your network once each cable access router is registered with the CMTS.
- The PC(s) connected to the Cisco uBR900 series cable access router must be configured for IP.
- Cisco IOS Release 12.1 or later must be running on the Cisco uBR900 series cable access router. When the cable access router is up and running, you can display the Cisco IOS release number by entering the **show version** command in user EXEC mode.

Subscriber-End Broadband Access Router Configuration Tasks

The Cisco uBR900 series cable access router typically is configured automatically on power-up using a configuration file generated by the cable service provider and delivered via the CMTS installed at the cable headend. All of the following configuration tasks are optional.

- Configuring a Host Name and Password
- Configuring Ethernet and Cable Access Router Interfaces
- Configuring Routing
- Configuring Bridging
- Reestablishing DOCSIS-Compliant Bridging

- Customizing the Cable Access Router Interface
- Using Multiple PCs with the Cable Access Router

**Note**

Before attempting to reconfigure a Cisco uBR900 series cable access router at a subscriber site, contact your network administrator, provisioning manager, or billing system administrator to ensure that remote configuration is allowed. If remote configuration is disabled, settings you make and save at the local site will not remain in effect after the cable access router is powered down and back up. Instead, settings will return to the previous configuration.

Configuring a Host Name and Password

One of the first configuration tasks you might want to perform is to configure a host name and set an encrypted password. Configuring a host name allows you to distinguish multiple Cisco uBR900 series cable access routers from each other. Setting an encrypted password allows you to prevent unauthorized configuration changes.

**Note**

Passwords are case sensitive.

To configure a host name and an encrypted password for a Cisco uBR900 series cable access router, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	uBR924(config)# hostname cisco cisco(config)#	Changes the name of the uBR900 series to a meaningful name. Substitute your host name for the cisco keyword.
Step 2	cisco(config)# enable secret guessme	Enters an enable secret password. This password provides access to enable (privileged EXEC) mode. After configuring a password, when you enter enable at the EXEC prompt, you must enter the enable secret password to gain access to configuration mode. Substitute your enable secret password for the guessme keyword.
Step 3	cisco(config)# line console 0 cisco(config-line)# exec-timeout 0 0 cisco(config-line)# exit cisco(config)#	Enters line configuration mode to configure the console port. Prevents the EXEC facility from timing out if you do not type any information on the console screen for an extended period. Exits to global configuration mode.

Verifying the Host Name and Password

To verify that you configured the correct host name and password, perform the following tasks:

- Enter the **show running-config** command in global configuration mode:

```
cisco(config)# show running-config
Using 1888 out of 126968 bytes
!
version XX.X
.
.
!
hostname cisco
!
enable secret 5 $1$60L4$X2JY0woDc0.kqa1lo0/w8/
```

- Check the host name and encrypted password displayed near the top of the command output.
- Exit global configuration mode and attempt to reenter it using the new enable password:

```
cisco# exit

cisco con0 is now available
Press RETURN to get started.
cisco> enable
Password: guessme
cisco#
```

Troubleshooting Tips

To troubleshoot the configuration, perform the following tasks:

- Make sure the **Caps Lock** key is off.
- Make sure you entered the correct passwords. Passwords are case sensitive.

Configuring Ethernet and Cable Access Router Interfaces

To assign an IP address to the Ethernet or cable access router interface so that it can be recognized as a device on the Ethernet LAN, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	uBR924(config)# interface ethernet 0 OR uBR924(config)# interface modem-cable0 uBR924(config-if)#	Enters interface configuration mode for the Ethernet or the cable access router interface.

	Command	Purpose
Step 2	uBR924(config-if)# ip address 172.16.1.1 255.255.255.0	Assigns the appropriate IP address and subnet mask to the interface.
Step 3	uBR924(config-if)# Ctrl-Z uBR924# %SYS-5-CONFIG_I: Configured from console by console	Returns to privileged EXEC mode. This message is normal and does not indicate an error.

Verifying IP Address Configuration

To verify that you have assigned the correct IP address, enter the **show arp** command:

```
uBR924# show arp
Protocol Address      Age (min)  Hardware Addr  Type   Interface
Internet 172.16.1.1        -         0009.0613.6030 ARPA   cable-modem0
Internet 4.0.0.28          -         00e0.1ed7.524d ARPA   Ethernet0
```

Troubleshooting Tips

To troubleshoot the configuration, perform the following tasks:

- Make sure you are using the correct IP address.
- Make sure the cable interface is not shut down. Use the **show running-config** command to check the cable interface status.

Configuring Routing

DOCSIS-compliant transparent bridging is the factory default configuration of the Cisco uBR900 series cable access router. To change the configuration of your cable access router from bridging to routing using the CLI, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	uBR924(config)# interface cable-modem0	Enters interface configuration mode for the cable access router interface.
Step 2	uBR924(config-if)# no cable-modem compliant bridge uBR924(config-if)# no bridge-group 59 uBR924(config-if)# end	Turns off DOCSIS-compliant bridging. Removes the default bridge group assignment from the cable interface. Returns to global configuration mode.
Step 3	uBR924(config)# ip routing uBR924(config)# ip subnet-zero uBR924(config)# ip route <IP address of CMTS> <subnet mask of CMTS>	Enables IP routing for the cable access router. Enables the use of subnet zero for interface addresses and routing updates. Creates a static route to the CMTS to make sure that ToD packets are properly routed out of the cable access router.
Step 4	uBR924(config)# router rip	Enters router configuration mode and enables RIP on the cable access router.

	Command	Purpose
Step 5	uBR924(config-router)# network <i>network-number</i>	Specifies the network connected to the cable access router on which the RIP process will operate. If the cable access router is attached to more than one network, enter each IP address in a separate command.
Step 6	uBR924(config-router)# end uBR924(config)# interface <i>cable-modem0</i>	Exits router configuration mode. Returns to interface configuration mode for the cable access router interface.
Step 7	uBR924(config-if)# ip rip receive v 2	Specifies that only RIP Version 2 packets will be received on the coaxial cable interface.
Step 8	uBR924(config-if)# ip rip send v 2	Specifies that only RIP Version 2 packets will be sent on the coaxial cable interface.
Step 9	uBR924(config-if)# end uBR924(config)# interface <i>ethernet0</i>	Exits interface configuration mode for the cable access router interface and enters interface configuration mode for the Ethernet0 interface.
Step 10	uBR924(config-if)# no bridge-group 59	Removes the default bridge group assignment from the Ethernet0 interface.
Step 11	uBR924(config-if)# ip rip receive v 2	Specifies that only RIP Version 2 packets will be received on this Ethernet interface.
Step 12	uBR924(config-if)# ip rip send v 2	Specifies that only RIP Version 2 packets will be sent on this Ethernet interface.
Step 13	uBR924(config-if)# Ctrl-z uBR924# copy running-config startup-config Building configuration...	Returns to privileged EXEC mode. Saves the configuration to NVRAM so that it will not be lost in the event of a reset, power cycle, or power outage.

Verifying Routing

To verify that bridging is not configured, routing is enabled, and that RIP is configured on the interfaces, enter the **show startup-config** command in privileged EXEC mode:

```
uBR924# show startup-config
Building configuration...

Current configuration:
!
version 12.1
no service pad
no service password-encryption
service udp-small-servers
service tcp-small-servers
!
hostname uBR924
!
!
clock timezone - 4
ip subnet-zero
!
!
!
voice-port 0
!
```

```

voice-port 1
!
!
interface Ethernet0
 ip address 10.1.0.33 255.255.0.0
 no ip directed-broadcast
 ip rip send version 2
 ip rip receive version 2
 no keepalive
!
interface cable-modem0
 ip address 172.16.1.42 255.255.0.0
 no ip directed-broadcast
 ip rip send version 2
 ip rip receive version 2
 no keepalive
cable-modem downstream saved channel 699000000 39
 no cable-modem compliant bridge
!
router rip
 network 4.0.0.0
 network 172.16.0.0
!
ip classless
no ip http server
!
line con 0
 transport input none
line vty 0 4
!
end

```

Configuring Bridging

The Cisco uBR900 series cable access router is configured for DOCSIS-compliant transparent bridging by default. If it becomes necessary to *reconfigure* the unit for bridging after it has been configured for routing, you can erase the routing configuration and return the unit to factory default configuration settings, or you can reconfigure the unit manually using the CLI. To return the cable access router to factory default settings, see the “Reestablishing DOCSIS-Compliant Bridging” section later in this chapter for details. To reconfigure the cable access router manually, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	uBR924(config)# no service pad	Disables packet assembler/disassembler (PAD) commands; prevents the Cisco uBR900 series from accepting incoming or outgoing PAD connections.
Step 2	uBR924(config)# no service password-encryption	Disables password encryption.
Step 3	uBR924(config)# no ip routing	Disables IP routing on the Cisco uBR900 series.
Step 4	uBR924(config)# interface Ethernet0	Enters interface configuration mode for the Ethernet0 interface.
Step 5	uBR924(config-if)# no ip address	Disables the IP address on the Ethernet0 interface.
Step 6	uBR924(config-if)# no ip route-cache	Disables high-speed switching caches for IP routing.

	Command	Purpose
Step 7	uBR924(config-if)# bridge-group <i>bridge-group</i>	Assigns the Ethernet0 interface to a bridge group. The bridge group must be an integer from 1 to 63.
Step 8	uBR924(config-if)# bridge-group <i>bridge-group</i> spanning-disabled	Disables spanning tree on the Ethernet interface.
Step 9	uBR924(config-if)# end uBR924(config)# interface <i>cable-modem0</i>	Exits interface configuration mode for the Ethernet0 interface and enters interface configuration mode for the cable access router interface.
Step 10	uBR924(config-if)# no ip address	Disables the IP address of the coaxial cable interface, if one has been set. The Cisco uBR7200 series cable router assigns an IP address to the cable access router each time it connects to the network.
Step 11	uBR924(config-if)# no ip route-cache	Disables high-speed switching caches for IP routing on the cable interface.
Step 12	uBR924(config-if)# no keepalive	Disables keepalives on the cable interface.
Step 13	uBR924(config-if)# cable-modem compliant bridge	Enables DOCSIS-compliant bridging.
Step 14	uBR924(config-if)# bridge-group <i>bridge-group</i>	Assigns the cable access router interface to a bridge group. The bridge group must be an integer from 1 to 63. (The default is 59.)
Step 15	uBR924(config-if)# bridge-group <i>bridge-group</i> spanning-disabled	Disables spanning tree on the cable interface.
Step 16	uBR924(config-if)# end uBR924(config)# ip classless	Exits interface configuration mode. (Optional) At times, the Cisco uBR900 series might receive packets destined for a subnet of a network that has no network default route. This global configuration mode command allows the Cisco IOS software to forward such packets to the best network route possible.
Step 17	uBR924(config)# line console 0	Enters line configuration mode to configure the console port.
Step 18	uBR924(config-line)# line vty 0 4	Identifies the last line in a contiguous group of virtual terminals you want to configure.
Step 19	uBR924(config-line)# Ctrl-z uBR924# copy running-config startup-config Building configuration...	Returns to privileged EXEC mode. Saves the configuration to NVRAM so that it will not be lost in the event of a reset, power cycle, or power outage.

When the cable interface comes up, the IP address and downstream channel are configured automatically.



Note

To configure multiple PCs, repeat Steps 4 through 7 above for each additional PC. You can connect a maximum of three PCs to the Cisco uBR900 series cable access router in a bridging application.

Verifying Bridging

To verify that routing has been disabled on all interfaces and that bridging has been reenabled, enter the **show startup-config** command in privileged EXEC mode:

```
uBR924# show startup-config
Building configuration...
Current configuration:
!
version 12.1
service config
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname uBR924
!
clock timezone - 4
ip subnet-zero
no ip routing
!
voice-port 0
!
voice-port 1
!
interface Ethernet0
no ip address
no ip directed-broadcast
no ip route-cache
bridge-group 59
bridge-group 59 spanning-disabled
!
interface cable-modem0
no ip address
no ip directed-broadcast
no ip route-cache
no keepalive
cable-modem downstream saved channel 699000000 36
bridge-group 59
bridge-group 59 spanning-disabled
!
ip classless
!
line con 0
line vty 0 4
login
!
end
```

Reestablishing DOCSIS-Compliant Bridging

To erase the current cable access router configuration and return the unit to its factory default DOCSIS-compliant bridging configuration, use the following command in privileged EXEC mode:

Command	Purpose
uBR924# erase startup config	Erases the current configuration (assuming the current running configuration has been saved to NVRAM).

After entering this command, perform a warm reset of the Cisco uBR900 series cable access router by pressing and holding down the Reset button for less than 10 seconds. For information on the location and operation of the Reset button, refer to the “Product Overview” chapter of the *Cisco uBR924 Hardware Installation Guide*.

Verifying DOCSIS-Compliant Bridging

To verify that the cable access router is configured for DOCSIS-compliant bridging, enter the **show startup-config** command in privileged EXEC mode. The configuration should look like this:

```
uBR924# show startup-config
Building configuration...
Current configuration:
!
version 12.1
service config
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname uBR924
!
clock timezone - 4
ip subnet-zero
no ip routing
!
voice-port 0
!
voice-port 1
!
!
interface Ethernet0
no ip address
no ip directed-broadcast
no ip route-cache
bridge-group 59
bridge-group 59 spanning-disabled
interface cable-modem0
no ip address
no ip directed-broadcast
no ip route-cache
no keepalive
cable-modem downstream saved channel 699000000 36
bridge-group 59
bridge-group 59 spanning-disabled
!
ip classless
no ip http server
!
line con 0
transport input none
line vty 0 4
login
!
end
```

Customizing the Cable Access Router Interface

Different geographical regions and different cable plants use different frequency bands. The Cisco uBR900 series cable access router uses a built-in default frequency scanning feature to address this issue. After the cable access router finds a successful downstream frequency channel, it saves the channel and power setting to NVRAM. The cable access router recalls this value the next time it needs to synchronize its frequency or register with the cable service provider CMTS.

However, you can customize the cable access router interface configuration if you need to deviate from the default setting that ships with the unit. For example, you might need to specify a different compliant mode, modify the saved downstream channel setting and upstream power value, or enable a faster downstream search algorithm.



Note

Most cable network scenarios will not require you to use the commands in this section.

To customize the cable access router interface, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	uBR924(config)# interface cable-modem 0	Specifies cable access router interface 0.
Step 2	uBR924(config-if)# cable-modem compliant bridge	Enables DOCSIS-compliant bridging.
Step 3	uBR924(config-if)# cable-modem downstream saved channel ds-frequency us-power	Modifies the saved downstream channel setting and upstream power value. If you do this, you must specify an exact downstream frequency and a power value. ¹
Step 4	uBR924(config-if)# cable-modem fast-search	Enables a faster downstream search algorithm.

1. Use the **no cable-modem downstream saved channel ds-frequency us-power** command to remove a saved frequency and power setting from NVRAM.

Using Multiple PCs with the Cable Access Router

The MAX CPE parameter in the DOCSIS configuration file determines how many PCs or other CPE devices are supported by a particular cable access router. The default value for the MAX CPE parameter is 1, which means only one PC can be connected to the cable access router unless this value is changed.

The DOCSIS 1.0 specification states that a CMTS cannot age out MAC addresses for CPE devices. Thus, if MAX CPE = 1, the first PC that is connected to a cable access router is normally the only one that the CMTS recognizes as valid. If you wish to replace an existing PC or change 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.

If you wish to replace an existing PC or NIC, use one of the following workarounds:

- Use the **clear cable host reset** command on the Cisco uBR7200 series universal broadband router to remove the PC MAC address from the router internal address tables. The PC MAC address will be rediscovered and associated with the correct cable access router during the next DHCP lease cycle.

- Power down the cable access router for approximately one minute and then power it back up so that the PC MAC address will be rediscovered and associated with the cable access router during the normal provisioning process. The PC might also need to be rebooted.
- Increase the value of the MAX CPE parameter in the cable access router DOCSIS configuration file so that it can accommodate the desired number of PCs. Reset the cable access router to force it to load the updated configuration file.

Subscriber-End Broadband Access Router Configuration Examples

To view the configuration of a Cisco uBR900 series cable access router, enter the **show running-config** command at the CLI prompt in global configuration mode.

This section provides examples of the following configurations:

- Basic Internet Access Bridging Configuration Example
- Basic Internet Access Routing Configuration Example
- IP Multicast Routing Configuration Example
- VoIP Bridging Using H.323v2 Configuration Example
- VoIP Routing Using H.323v2 Configuration Example
- NAT/PAT Configuration Example
- VoIP Bridging Using SGCP Configuration Example
- IPSec Configuration Example
- L2TP Configuration Example

Basic Internet Access Bridging Configuration Example

The following Cisco uBR900 series cable access router configuration supports a typical residential Internet-access, data-only subscriber:

```
Current configuration:
!
version 12.1
service config
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname uBR904
!
clock timezone - 4
ip subnet-zero
no ip routing
!
voice-port 0
!
voice-port 1
!
interface Ethernet0
ip address 172.16.1.40 255.255.0.0
```

```

no ip directed-broadcast
no ip route-cache
bridge-group 59
bridge-group 59 spanning-disabled
!
interface cable-modem0
ip address 172.16.1.40 255.255.0.0
no ip directed-broadcast
no ip route-cache
cable-modem downstream saved channel 699000000 36
bridge-group 59
bridge-group 59 spanning-disabled
!
ip classless
no ip http server
!
line con 0
  transport input none
line vty 0 4
!
end

```

Basic Internet Access Routing Configuration Example

The Cisco uBR900 series cable access router can be configured to act as a router to preserve IP address space and limit broadcasts that can impact the performance of the network. A sample configuration file follows.



Note

To configure the Cisco uBR900 series to act as a router, the **no cable-modem compliant bridge** command must be used. In addition, the **bridge group 59** command must be removed from the Ethernet and cable-modem interfaces.

```

Current configuration:
!
version 12.1
service config
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname uBR904
!
clock timezone - 4
ip subnet-zero
!
voice-port 0
!
voice-port 1
!
interface Ethernet0
ip address 10.1.0.33 255.255.0.0
no ip directed-broadcast
!
interface cable-modem0
ip address 172.16.1.42 255.255.0.0
no ip directed-broadcast
cable-modem downstream saved channel 699000000 39
no cable-modem compliant bridge

```

```

!
router rip
  version 2
  network 4.0.0.0
  network 172.16.0.0
!
ip classless
no ip http server
!
line con 0
  transport input none
line vty 0 4
!
end

```

IP Multicast Routing Configuration Example

The following configuration is for a Cisco uBR900 series that uses PIM sparse-dense mode and belongs to a specific multicast group. Other multicast routing protocols such as PIM sparse-mode or PIM dense-mode can be used.

Current configuration:

```

!
! Last configuration change at 23:16:44 - Thu Dec 16 1999
!
version 12.1
service config
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname uBR924
!
clock timezone - 4
ip subnet-zero
!
!
ip multicast-routing
ip dvmrp route-limit 20000
!
!
voice-port 0
!
voice-port 1
!
!
interface Ethernet0
  ip address 24.1.0.1 255.255.0.0
  no ip directed-broadcast
  ip pim sparse-dense-mode
  no ip route-cache
  no ip mroute-cache
!
interface cable-modem0
  ip address 10.1.0.25 255.255.0.0
  no ip directed-broadcast
  ip pim sparse-dense-mode
  no ip route-cache
  no ip mroute-cache

```

```
cable-modem downstream saved channel 477000000 56
no cable-modem compliant bridge
!
!
router rip
  version 2
  network 24.0.0.0

network 10.0.0.0
!
ip classless
no ip http server
!
line con 0
  transport input none
line vty 0 4
!
end
```

VoIP Bridging Using H.323v2 Configuration Example

In this example, the Cisco uBR924 is configured for bridging, with an H.323v2 dial peer to another Cisco uBR924 attached to the same downstream interface on the headend CMTS.

Current configuration:

```
!
! Last configuration change at 21:54:41 - Thu Dec 16 1999
! NVRAM config last updated at 21:56:20 - Thu Dec 16 1999
!
version 12.1
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname 2007
!
clock timezone - 3
ip subnet-zero
no ip routing
!
voice-port 0
  input gain -3
!
voice-port 1
  input gain -3
!
dial-peer voice 1 pots
  destination-pattern 6501
  port 0
!
dial-peer voice 2 pots
  destination-pattern 6502
  port 1
!
dial-peer voice 62 voip
  destination-pattern 620.
  session target ipv4:10.1.71.62
!
interface Ethernet0
  ip address 10.1.71.65 255.255.255.0
  no ip directed-broadcast
```

```

no ip route-cache
bridge-group 59
bridge-group 59 spanning-disabled
!
interface cable-modem0
description DHCP Reserved Address 10.1.71.65
ip address 10.1.71.65 255.255.255.0
no ip directed-broadcast
no ip route-cache
cable-modem downstream saved channel 537000000 27
bridge-group 59
bridge-group 59 spanning-disabled
!
ip classless
no ip http server
!
line con 0
exec-timeout 0 0
transport input none
line vty 0 4
!
end

```

VoIP Routing Using H.323v2 Configuration Example

In this example, the Cisco uBR924 is configured for IP routing, with an H.323v2 dial peer to another Cisco uBR924 attached to the same downstream interface on the headend CMTS.

```

Current configuration:
!
! No configuration change since last restart
!
version 12.1
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname 2007
!
class-map class-default
match any
!
clock timezone - 3
ip subnet-zero
!
voice-port 0
!
voice-port 1
!
dial-peer voice 1 pots
destination-pattern 6101
port 0
!
dial-peer voice 2 pots
destination-pattern 6102
port 1
!
dial-peer voice 101 voip
destination-pattern 620*
codec g711alaw
session target ipv4:10.1.71.62

```



```

!
interface Ethernet0
 ip address 24.1.61.1 255.255.255.0
 no ip directed-broadcast
 no ip mroute-cache
!
interface cable-modem0
 ip address 10.1.71.61 255.255.255.0
 no ip directed-broadcast
 no ip mroute-cache
 cable-modem downstream saved channel 537000000 27
 no cable-modem compliant bridge
!
router rip
 version 2
 network 10.0.0.0
 network 24.0.0.0
 no auto-summary <==== Not necessary
!
no ip classless
ip route 0.0.0.0 0.0.0.0 10.1.71.1
no ip http server
!
line con 0
 exec-timeout 0 0
 transport input none
line vty 0 4
 login
!
end

```

NAT/PAT Configuration Example

```

Current configuration:
!
! No configuration change since last restart
!
version 12.1
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname uBR924
!
!
ip nat inside source list 1 interface cable-modem0 overload
clock timezone - -4
!
!
interface Ethernet0
 ip address 10.1.1.1 255.255.255.0
 ip nat inside
!
interface cable-modem0
 ip address 24.3.90.20 255.255.255.0
 ip nat outside
 no keepalive
 cable-modem downstream saved channel 627000000 54
 no cable-modem compliant bridge
!
ip default-gateway 24.3.90.2

```

```

ip classless
ip route 0.0.0.0 0.0.0.0 24.3.90.2
access-list 1 permit any
!
line con 0
line vty 0 4
  login
!
end

```

VoIP Bridging Using SGCP Configuration Example

In this example, Cisco uBR924 is configured to support VoIP in bridging mode using SGCP. Note the following in the sample configuration file:

- SGCP is enabled.
- The call agent IP address is specified.
- The SGCP application is specified for each port.

To configure this application via DHCP, the following fields must also be set:

- Host name
- Domain name
- Domain Name System (DNS) server
- Merit dump file — S:0:<call agen FQDN>:S:1<call agent FQDN>

```

Current configuration:
!
! Last configuration change at 16:30:00 - Thu Dec 16 1999
!
version 12.1
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname art1
!
clock timezone - 0 6
ip subnet-zero
no ip routing
ip domain-name cisco.com
ip name-server 4.0.0.32
!
sgcp
!
xgcp snmp sgcp
!
!
voice-port 0
!
voice-port 1
!
dial-peer voice 100 pots
  application SGCPAPP
  port 0
!
dial-peer voice 101 pots

```

```

application SGCFAPP
port 1
!
process-max-time 200
!
interface Ethernet0
ip address 188.186.1.14 255.255.0.0
no ip directed-broadcast
no ip route-cache
no ip mroute-cache
bridge-group 59
bridge-group 59 spanning-disabled
!
interface cable-modem0
ip address 188.186.1.14 255.255.0.0
no ip directed-broadcast
no ip route-cache
no ip mroute-cache
cable-modem downstream saved channel 699000000 27
bridge-group 59
bridge-group 59 spanning-disabled
!
ip classless
no ip http server
!
!
line con 0
transport input none
line vty 0 4
login
!
end

```

IPSec Configuration Example



Note

Encryption/decryption is subject to export licensing controls. To support IPSec, the Cisco uBR900 series must be configured in routing mode. The software images running at both the headend and the subscriber end must support the feature set.



Note

Careful address assignment on user equipment and policy routing at the headend is required. The headend may or may not use tunnels to convey traffic back to the corporate gateway.

For detailed information on IP security, L2TP, and firewalls, refer to the *Cisco IOS Security Configuration Guide*.

```

Current configuration:
!
Last configuration change at 23:24:55 - Thu Dec 16 1999
!
version 12.1
no service pad
service timestamps debug uptime
service timestamps log uptime
!

```

```

hostname Router
!
clock timezone - 0 6
ip subnet-zero
no ip domain-lookup
!
crypto isakmp policy 1
  hash md5
  authentication pre-share
  lifetime 5000
crypto isakmp key 1111 address 30.1.1.1
crypto isakmp identity hostname
!
crypto ipsec transform-set test-transform ah-md5-hmac esp-des esp-md5-hmac
!
crypto map test-ipsec local-address cable-modem0
crypto map test-ipsec 10 ipsec-isakmp
set peer 30.1.1.1
set transform-set test-transform
match address 100
!
interface Ethernet0
ip address 24.1.0.1 255.255.0.0
no ip directed-broadcast
!
interface cable-modem0
ip address 10.1.0.25 255.255.0.0
no ip directed-broadcast
no keepalive
cable-modem downstream saved channel 213000000 30
no cable-modem compliant bridge
crypto map test-ipsec
router rip
  version 2
  network 10.0.0.0
  network 24.0.0.0
!
ip classless
no ip http server
!
access-list 100 permit ip host 10.1.0.25 30.1.1.0 0.0.0.255
!
line con 0
  exec-timeout 0 0
  transport input none
line vty 0 4
  login
!
end

```

L2TP Configuration Example



Note

Encryption/decryption is subject to export licensing controls. To support L2TP and firewalls, the Cisco uBR900 series must be configured in routing mode. Software images running at both the headend and the subscriber end must support the feature set.

**Note**

Careful address assignment on user equipment and policy routing at the headend is required. The headend may or may not use tunnels to convey traffic back to the corporate gateway.

For detailed information on IP security, L2TP, and firewalls, refer to the *Cisco IOS Security Configuration Guide*.

```

Current configuration:
!
! Last configuration change at 20:24:59 - Thu Dec 23 1999
! NVRAM config last updated at 20:34:52 - Thu Dec 23 1999
!
version 12.1
no service pad
service timestamps debug uptime
service timestamps log uptime
!
hostname Router
!
class-map class-default
  match any
!
!
clock timezone - 0 1
ip subnet-zero
ip tftp source-interface cable-modem0
no ip domain-lookup
!
vpdn enable
!
vpdn-group 1
  accept dialin l2tp virtual-template 1 remote L2TP_LAC
  no l2tp tunnel authentication
  !
  !
interface Ethernet0
  ip address 80.1.1.1 255.255.255.0
  no ip directed-broadcast
  !
interface Virtual-Template1
  ip unnumbered Ethernet0
  no ip directed-broadcast
  peer default ip address pool dialup
  ppp authentication chap
  !
interface cable-modem0
  ip address 255.255.0.0
  no ip directed-broadcast
  cable-modem downstream saved channel 639000000 38
no cable-modem compliant bridge
!
router rip
  version 2
  network 10.0.0.0
  network 24.0.0.0
  !
ip local pool dialup 24.1.0.100
ip classless
no ip http server
!

```

```
line con 0
  transport input none
line vty 0 4
  login
!
end
```

Free Manuals Download Website

<http://myh66.com>

<http://usermanuals.us>

<http://www.somanuals.com>

<http://www.4manuals.cc>

<http://www.manual-lib.com>

<http://www.404manual.com>

<http://www.luxmanual.com>

<http://aubethermostatmanual.com>

Golf course search by state

<http://golfingnear.com>

Email search by domain

<http://emailbydomain.com>

Auto manuals search

<http://auto.somanuals.com>

TV manuals search

<http://tv.somanuals.com>