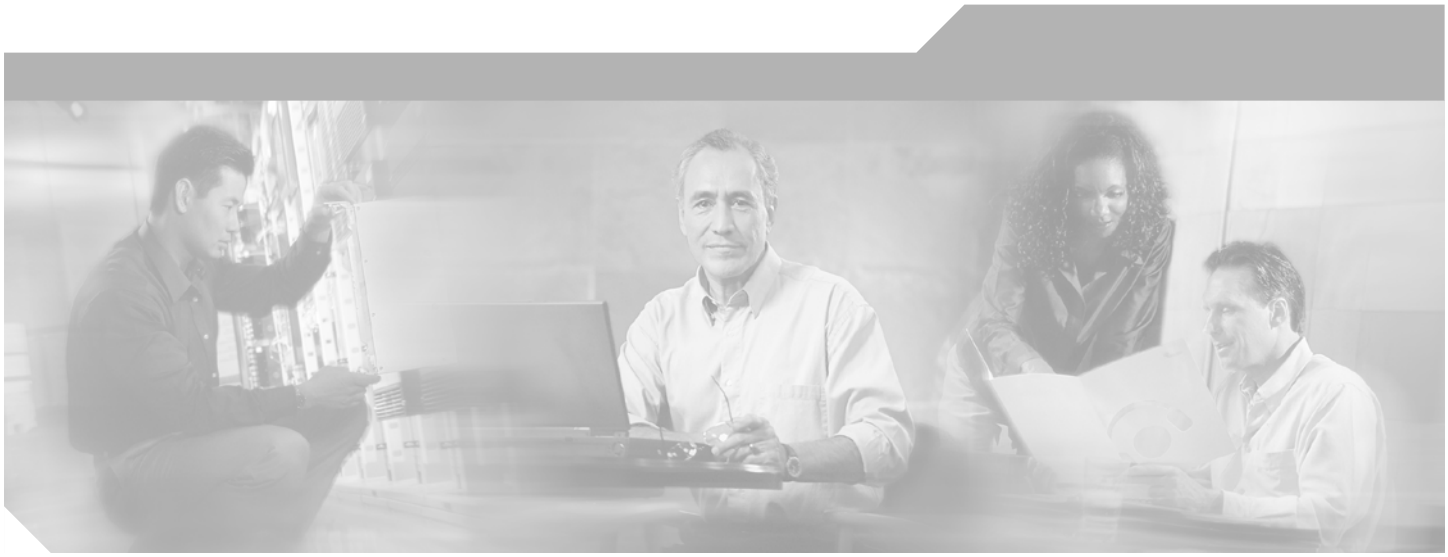


Cisco uBR924 Cable Access Router Software Configuration Guide

12.2(8)
August 2002

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Text Part Number: OL-0337-05

Cisco uBR924 Cable Access Router
Software Configuration Guide
OL-0337-05

CONTENTS

Preface

This document is the *Cisco uBR924 Cable Access Router Software Configuration Guide* and describes the configuration of the Cisco uBR924 cable access router. This section describes the following topics:

Audience

This configuration guide is designed for system administrators who have some experience downloading software from the World Wide Web and configuring cable modem/router systems. This guide is also directed to the network administrators who are responsible for administering the customer's local area network.

All users should have some experience with configuring Cisco routers and using the Cisco IOS command-line interface (CLI). A basic familiarity with DOCSIS 1.0, DOCSIS 1.0+ quality of service (QoS) principles, H.323, and SGCP/MGCP is helpful.

Cable system installers and technicians should be familiar with their cable plant's base operating parameters and subscriber service offerings. Cable system support engineers and administrators should be acquainted with cable data networks and WAN communications protocols. Network administrators should be familiar with the principles of IP routing and subnetting; some of the advanced configurations also require a thorough understanding of access lists and how to use them.

Note This document contains instructions to install or configure the Cisco uBR924 cable access router using procedures that only qualified personnel should perform. This document is not intended for subscribers. Refer to the "Subscriber Publications" section of this preface for a list of documents available for subscribers.

Purpose

This configuration guide explains the initial and basic software configuration procedures for the Cisco uBR924 cable access router. This guide contains procedures for configuring the Cisco uBR924 router for both data only operation, as well as for voice and data operation. This guide also describes how to set up basic security, the headend interface (CMTS-to-CM), and how to use ROM monitor.

Organization

This guide is organized into the chapters and appendixes shown in Table 1, which also shows the changes from the previous version of this guide:

Table 1 Organization

Chapter	Title	Description	Changes from the Previous Release
Chapter 1	Overview	Provides an overview of the Cisco uBR924 cable access router and its possible configurations.	Includes features added in Cisco IOS Release 12.1(5)T.
Chapter 2	DOCSIS-Bridging Configuration	Describes how to configure the router for its default of DOCSIS-compliant bridging operation.	None.
Chapter 3	Advanced Data-Only Configurations	Describes how to configure the router for various data-only configurations such as routing operation and IPSec encryption.	None.
Chapter 4	Voice over IP Configurations	Describes how to configure the router for Voice over IP (VoIP) traffic using either the H.323v2 or SGCP/MGCP call control protocols.	None.
Appendix A	Using Cisco IOS Software	Describes the basics of using the Cisco IOS command line interface (CLI).	None.
Appendix B	Using the Cable Monitor Tool	Describes how to display diagnostic information about the Cisco uBR924 cable access router using any web browser.	None.
Appendix C	Using the ROM Monitor	Describes how to use the Cisco IOS ROM monitor.	Minor changes on entering ROMMON mode and returning to normal mode.
Appendix D	New and Changed Commands Reference	Lists the commands that are new to the Cisco IOS 12.1 T software releases.	Includes commands added in Cisco IOS Release 12.1(5)T.

Note For a complete list of changes in each Cisco IOS release, see the Release Notes that accompany that release.

Document Conventions

This publication uses the following conventions:

Convention	Meaning	Comments
Boldface	Commands and keywords you enter literally as shown	**offset-list**
Italics	Variables for which you supply values	**command** *type interface* You replace the variable with the type of interface. In contexts that do not allow italics, such as online help, arguments are enclosed in angle brackets (< >).
Square brackets ([ ])	Optional elements	**command** [abc] abc is optional (not required), but you can choose it.
Vertical bars (|)	Separated alternative elements	**command** [abc | def] You can choose either abc or def, or neither, but not both.
Braces ({ })	Required choices	**command** { abc | def } You **must** use either abc **or** def, but not both.
Braces and vertical bars within square brackets ([{ | }])	A required choice within an optional element	**command** [abc { def | ghi }] You have three options: • Nothing • abc def • abc ghi
Caret character (^)	Control key	The key combinations ^D and Ctrl-D are equivalent: Both mean hold down the Control key while you press the D key. Keys are indicated in capital letters, but are not case sensitive.
A string	A non-quoted set of characters	For example, when setting an SNMP community string to *public*, do not use quotation marks around the string; otherwise, the string will include the quotation marks.
`System prompts`	Denotes interactive sessions, indicates that the user enters commands at the prompt	The system prompt indicates the current command mode. For example, the prompt `Router (config) #` indicates global configuration mode.
`Screen` font	Terminal sessions and information the system displays	
Angle brackets (< >)	Non-printing characters such as passwords	
Exclamation points (!) at the beginning of a line	A comment line	Comments are sometimes displayed by the Cisco IOS software.

Caution Means *reader be careful*. You are capable of doing something that might result in equipment damage or loss of data.

Note Means *reader take note*. Notes contain helpful suggestions or references to materials not contained in this guide.

Timesaver Means *the described action saves time*. You can save time by performing the action described in the paragraph.

Warning **This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. (To see translations of the warnings that appear in this publication, refer to the appendix, "Translated Safety Warnings," in the installation guide that accompanied this device.)**

Waarschuwing **Dit waarschuwingssymbool betekent gevaar. U verkeert in een situatie die lichamelijk letsel kan veroorzaken. Voordat u aan enige apparatuur gaat werken, dient u zich bewust te zijn van de bij elektrische schakelingen betrokken risico's en dient u op de hoogte te zijn van standaard maatregelen om ongelukken te voorkomen. (Voor vertalingen van de waarschuwingen die in deze publicatie verschijnen, kunt u het aanhangsel "Translated Safety Warnings" (Vertalingen van veiligheidsvoorschriften) in de installatiegids die bij dit toestel is ingesloten, raadplegen.**

Varoitus **Tämä varoitusmerkki merkitsee vaaraa. Olet tilanteessa, joka voi johtaa ruumiinvammaan. Ennen kuin työskentelet minkään laitteiston parissa, ota selvää sähkökytkentöihin liittyvistä vaaroista ja tavanomaisista onnettomuuksien ehkäisykeinoista. (Tässä julkaisussa esiintyvien varoitusten käännökset löydät tämän laitteen mukana olevan asennusoppaan liitteestä "Translated Safety Warnings" (käännetyt turvallisuutta koskevat varoitukset).)**

Attention **Ce symbole d'avertissement indique un danger. Vous vous trouvez dans une situation pouvant entraîner des blessures. Avant d'accéder à cet équipement, soyez conscient des dangers posés par les circuits électriques et familiarisez-vous avec les procédures courantes de prévention des accidents. Pour obtenir les traductions des mises en garde figurant dans cette publication, veuillez consulter l'annexe intitulée « Translated Safety Warnings » (Traduction des avis de sécurité) dans le guide d'installation qui accompagne cet appareil.**

Warnung **Dieses Warnsymbol bedeutet Gefahr. Sie befinden sich in einer Situation, die zu einer Körperverletzung führen könnte. Bevor Sie mit der Arbeit an irgendeinem Gerät beginnen, seien Sie sich der mit elektrischen Stromkreisen verbundenen Gefahren und der Standardpraktiken zur Vermeidung von Unfällen bewußt. (Übersetzungen der in dieser Veröffentlichung enthaltenen Warnhinweise finden Sie im Anhang mit dem Titel "Translated Safety Warnings" (Übersetzung der Warnhinweise) in der diesem Gerät beiliegenden Installationsanleitung.)**

Avvertenza **Questo simbolo di avvertenza indica un pericolo. Si è in una situazione che può causare infortuni. Prima di lavorare su qualsiasi apparecchiatura, occorre conoscere i pericoli relativi ai circuiti elettrici ed essere al corrente delle pratiche standard per la prevenzione di incidenti. La traduzione delle avvertenze riportate in questa pubblicazione si trova nell'appendice, "Translated Safety Warnings" (Traduzione delle avvertenze di sicurezza), del manuale d'installazione che accompagna questo dispositivo.**

Advarsel **Dette varselsymbolet betyr fare. Du befinner deg i en situasjon som kan føre til personskade. Før du utfører arbeid på utstyr, må du være oppmerksom på de faremomentene som elektriske kretser innebærer, samt gjøre deg kjent med vanlig praksis når det gjelder å unngå ulykker. (Hvis du vil se oversettelser av de advarslene som finnes i denne publikasjonen, kan du se i vedlegget "Translated Safety Warnings" [Oversatte sikkerhetsadvarsler] i installasjonsveiledningen som ble levert med denne enheten.)**

Aviso **Este símbolo de aviso indica perigo. Encontra-se numa situação que lhe poderá causar danos fisicos. Antes de começar a trabalhar com qualquer equipamento, familiarize-se com os perigos relacionados com circuitos eléctricos, e com quaisquer práticas comuns que possam prevenir possíveis acidentes. (Para ver as traduções dos avisos que constam desta publicação, consulte o apêndice "Translated Safety Warnings" - "Traduções dos Avisos de Segurança", no guia de instalação que acompanha este dispositivo).**

Advertencia **Este símbolo de aviso significa peligro. Existe riesgo para su integridad física. Antes de manipular cualquier equipo, considerar los riesgos que entraña la corriente eléctrica y familiarizarse con los procedimientos estándar de prevención de accidentes. (Para ver traducciones de las advertencias que aparecen en esta publicación, consultar el apéndice titulado "Translated Safety Warnings," en la guía de instalación que se acompaña con este dispositivo.)**

Varning! **Denna varningssymbol signalerar fara. Du befinner dig i en situation som kan leda till personskada. Innan du utför arbete på någon utrustning måste du vara medveten om farorna med elkretsar och känna till vanligt förfarande för att förebygga skador. (Se förklaringar av de varningar som förekommer i denna publikation i appendix "Translated Safety Warnings" [Översatta säkerhetsvarningar] i den installationshandbok som medföljer denna anordning.)**

Acronyms and Terms

To fully understand the content of this guide, you should be familiar with the acronyms and terms listed in this section. These terms are specific to the operation of a data cable network; more general networking acronyms and terms can be found in *Internetworking Terms and Acronyms*, available on CCO and the Documentation CD-ROM.

- 3DES—Triple Data Encryption Standard.
- ASIC—Application Specific Integrated Circuit.
- BPI—Baseline Privacy Interface.
- BPI+ —Extension to the initial BPI standard with improved authentication and encryption.
- CM—Cable modem.
- CMTS—Cable Modem Termination System (headend).
- CoS—Class of service.
- CPE—Customer Premises Equipment.

- DES—Data Encryption Standard.
- DOCSIS 1.0—Data Over Cable Service Interface Specification.
- DOCSIS 1.0+—Extension of the DOCSIS 1.0 standard with features that support quality of service (QoS) options to offer better than best effort, low latency, and low jitter services.
- Downstream—Transmission of traffic from the CMTS (headend) to the CM (cable modem).
- IPSec—IP network security.
- Kbps—Kilobits per second.
- MAC—Media Access Control.
- Mbps—Megabits per second.
- MODEM—modulator/demodulator.
- MSO—Multiple Systems Operator.
- NIU/STB—Network Interface Unit/Set-Top Box.
- PPS—Packets per second.
- QAM—Quadrature Amplitude Modulation.
- QoS—Quality of service.
- QPSK—Quadrature Phase Shift Keying.
- RF—Radio frequency.
- SID—Service Identifier (DOCSIS MAC-level service flow identifier)
- SM—Subscriber Modem or Spectrum Manager.
- uBR—Universal broadband router.
- Upstream—Transmission of traffic from CM (cable modem) to the CMTS (headend).
- VoIP—Voice over IP.

Related Documentation

Refer to the following Cisco documents for related information. The documents can be found online at Cisco Connection Online (CCO) or on the Documentation CD-ROM. You can also order printed copies of most current documents.

Note The list that follows is not all-inclusive. New documents and revisions occur frequently.

Cisco uBR924 Cable Access Router

- *Cisco uBR924 Cable Access Router Software Configuration Guide* (this manual)
- *Cisco uBR924 Cable Access Router Hardware Installation Guide*
- *Cisco uBR924 Cable Access Router Quick Start Guide*
- *DOCSIS CPE Configurator Help*
- Release Notes for each release of Cisco IOS software for the Cisco uBR924 cable access router

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

CMTS Hardware Installation Publications

- *Cisco uBR7200 Series Universal Broadband Router Hardware Installation Guide*
- *Cisco uBR7200 Series Universal Broadband Router Software Configuration Guide*
- *Cisco uBR7200 Series Universal Broadband Router Cable Modem Card Installation and Configuration*
- *Cisco uBR7200 Series Universal Broadband Router Port Adapter Installation and Configuration*
- *Cisco uBR7200 Series Universal Broadband Router 550-Watt DC-Input Power Supply Replacement Instructions*
- *Cisco uBR7200 Series Universal Broadband Router Subchassis and Midplane Replacement Instructions*
- *Cisco uBR7200 Series Rack-Mount and Cable-Management Kit Installation Instructions*
- *Cisco uBR7200 Series Universal Broadband Router Fan Tray Replacement Instructions*
- *Cisco uBR7200 Series Universal Broadband Router Feature Enhancements*

Cisco IOS Publications

- *Cisco IOS Release 12.1 New Feature Documentation* for feature module descriptions on Cisco IOS Release 12.1-based releases
- *Cisco IOS Release 12.1 Configuration Guides and Command References* for task and command descriptions on Cisco IOS Release 12.1-based releases

Note Use the Cisco IOS *Command Reference Master Index(es)* to obtain document pointers for specific software release feature sets and commands.

Configuration Editor and Network Management Publications

- *Cisco Cable Configuration Guide* for information on the Cisco Network Registrar (CNR) product
- *CiscoView: Internetworking Device Monitoring and Management*
- *CiscoView Incremental Installation Quick Reference Guide*
- CiscoWorks documentation for networks that use the Simple Network Management Protocol (SNMP) to monitor Cisco uBR924 router

Subscriber Publications

- *Quick Start, Cisco uBR924 Cable Access Router Subscriber Setup*

Note Service provider and subscriber publications for other models of Cisco uBR900 Series cable access routers are also available on CCO.

Obtaining Documentation

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at http://www.cisco.com, http://www-china.cisco.com, or http://www-europe.cisco.com.

Documentation CD-ROM

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

Ordering Documentation

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

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

Obtaining Technical Assistance

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

Cisco Connection Online

Cisco continues to revolutionize how business is done on the Internet. Cisco Connection Online is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information and resources at anytime, from anywhere in the world. This highly integrated Internet application is a powerful, easy-to-use tool for doing business with Cisco.

CCO's broad range of features and services helps customers and partners to streamline business processes and improve productivity. Through CCO, you will find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online support services, download and test software packages, and order Cisco learning materials and merchandise. Valuable online skill assessment, training, and certification programs are also available.

Customers and partners can self-register on CCO to obtain additional personalized information and services. Registered users may order products, check on the status of an order and view benefits specific to their relationships with Cisco.

You can access CCO in the following ways:

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

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

Technical Assistance Center

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

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

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

Language	E-mail Address
English	tac@cisco.com
Hanzi (Chinese)	chinese-tac@cisco.com
Kanji (Japanese)	japan-tac@cisco.com
Hangul (Korean)	korea-tac@cisco.com
Spanish	tac@cisco.com
Thai	thai-tac@cisco.com

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

Documentation Feedback

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

You can e-mail your comments to bug-doc@cisco.com.

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

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

We appreciate and value your comments.

Overview

This chapter provides a basic understanding of the Cisco uBR924 cable access router's software feature sets, as well as the processes used for provisioning the router within a cable network and configuring it for different services. This chapter contains the following sections:

Note This manual describes the Cisco uBR924 cable access router and feature sets as they exist in Cisco IOS Release 12.1(5)T.

Cisco IOS Software Release Feature Sets

The Cisco uBR924 cable access router supports a number of feature sets. Each feature set contains features that provide a specific functionality, such as firewall or advanced encryption. All feature sets, however, support base IP bridging as required by the Data Over Cable Service Interface Specification (DOCSIS). This allows the Cisco uBR924 cable access router to transmit data traffic over the HFC cable network.

In addition to data traffic, the images for the Cisco uBR924 cable access router enable the voice ports, allowing the router to transmit Voice over IP (VoIP) and fax traffic over the cable network and Internet. Voice and data traffic can be transmitted simultaneously, but real-time traffic such as voice calls requires different handling than data traffic—data traffic can be sent on a "best-effort" basis because it can accept some loss or delay in the transmission of packets, but such losses and delays are unacceptable for voice calls.

For this reason, the Cisco uBR924 cable access router supports the DOCSIS Quality of Service (QoS) enhancements that give higher priority to IP packets containing voice traffic. This ensures that real-time traffic is delivered more reliably than "best-effort" data traffic.

The telephones and fax machines connected to the Cisco uBR924 router can route their calls over the Internet using either the H.323v2 (Gateway/Gatekeeper) or Simple Gateway Control Protocol (SGCP) voice control protocols. Depending on the protocol used and the level of support provided by the service provider, these calls can be made either to other VoIP devices or to phones connected on the regular telco network.

The following Cisco IOS Release 12.1 images support both data and voice traffic, in addition to the other feature sets that are listed:

- **Base IP DOCSIS-Compliant Bridging**—Provides full DOCSIS 1.0-compliant cable modem support for customers who want a basic high-speed connection to the Internet. This is the default software image for the Cisco uBR924 cable access router in Cisco IOS Release 12.0; in Cisco IOS Release 12.1 and later, this image is superseded by the Home Office (Easy IP) image.
- **Home Office (Easy IP)**—Provides a high-speed DOCSIS connection to the Internet, along with server functions that simplify the administration of IP addresses. In addition to simplifying network management, this allows the Cisco uBR924 router to connect multiple computers to the Internet through the cable interface. This is the default software image for the Cisco uBR924 cable access router in Cisco IOS Release 12.1.
- **Value Telecommuter** —Adds IPsec encryption and layer 2 tunneling support to the functions provided by the Home Office (Easy IP) image. This allows businesses to establish secure high-speed Internet connections between employees' homes and the office local area network (LAN). This gives the employees' computers the same connectivity they would have if they were directly connected to the office network.
- **Performance Telecommuter** —Adds advanced IPsec encryption to the functions provided by the Value Telecommuter image, enabling high-speed and high-security Internet connections between employees' homes and the office LAN.
- **Value Small and Branch Office**—Adds IPsec encryption and the Cisco Secure Integrated Software (firewall) feature set to the functions provided by the Home Office image. This allows customers to establish secure connections across the Internet; this feature set also protects the office network from intrusion and interference while preserving the permanent high-speed access to the Internet.
- **Performance Small and Branch Office**—Adds advanced IPsec encryption to the functions provided by the Value Small and Branch Office image. This allows customers to establish high-security connections across the Internet; this feature set also protects the office network from intrusion and interference while preserving the permanent high-speed access to the Internet.

Note Starting with Cisco IOS Release 12.1(1), the Cisco uBR924 cable access router supports fewer software images than previous releases (which supported 14 separate images). The new simplified set of software images are a superset of the images supported in the previous releases, allowing for an easy upgrade path from Release 12.0 to Release 12.1.

The following sections describe the feature sets in each of these categories. Descriptions of the features themselves are in the section "Feature Descriptions" section on page 1-5.

Note Not all Cisco IOS software releases and images support all features. In particular, early deployment (ED) releases might contain a limited number of images that support a subset of feature sets and images. ED releases might also support images and feature sets that are not listed here—see the Release notes for each Release for complete details on images and feature support.

Base IP DOCSIS-Compliant Bridging

The Base IP Bridging feature set includes DOCSIS-compliant bridging and DOCSIS Baseline Privacy Interface (BPI) encryption. This is the default feature set for the Cisco uBR924 cable access router in Cisco IOS Release 12.0 and allows the router to function as a DOCSIS 1.0 cable modem that can interoperate with any DOCSIS-qualified Cable Modem Termination System (CMTS). It provides basic high-speed Internet connectivity for customers who want to connect a small number of computers to the cable network.

DOCSIS-compliant bridging (also referred to as "plug-and-play" bridging) is the default configuration for the Cisco uBR924 router. In this mode, the router automatically does the following at power-on and system reset:

- Acquires temporary downstream and upstream channels
- Finds the appropriate Time of Day (ToD), Trivial File Transfer Protocol (TFTP), and Dynamic Host Configuration Protocol Server (DHCP) servers
- Gets the current time of day from the ToD server
- Obtains an IP address from the DHCP server
- Downloads a DOCSIS configuration file from the TFTP server
- Configures itself for its permanent downstream and upstream channels
- Obtains other DHCP parameters to work in bridging mode
- Optionally downloads a Cisco IOS image and Cisco IOS configuration file if specified in the DOCSIS configuration file
- Establishes a BPI session (if enabled on both the router and CMTS)

Note The Base IP Bridging feature set is the default image for the Cisco uBR924 cable access router in Cisco IOS Release 12.0. It is not available as a separate image in Cisco IOS Release 12.1 because is incorporated in all other available images.

In DOCSIS-compliant bridging mode, the Cisco uBR924 cable access router acts as a transparent bridge for one or more customer premises equipment (CPE) devices. The maximum number of CPE devices depends on the Cisco IOS Release being used:

- 3 CPE devices using Cisco IOS Release 12.0(4) XI1
- 254 CPE devices using Cisco IOS Release 12.0(5)T or later images

Note The maximum number of CPE devices also depends on the value of the "MAX CPE" field in the DOCSIS configuration file. The MAX CPE field defaults to one CPE device unless set otherwise. In this situation, the Cisco uBR924 router can connect only one computer to the cable network, regardless of the Cisco IOS Release being used.

Home Office (Easy IP)

The Home Office feature set provides high-speed Internet connectivity for customers who have a small home network. In addition to full DOCSIS 1.0 support (see Base IP DOCSIS-Compliant Bridging), the Home Office feature set provides the Easy IP set of features that simplifies the administration of IP addresses in a cable network.

This feature set supports intelligent Dynamic Host Configuration Protocol Server (DHCP) functions, such as DHCP Relay Agent and DHCP Client functionality. It also supports Network Address Translation and Port Address Translation (NAT/PAT).

The DHCP features provide intelligence and flexibility in the handling and distribution of IP addresses for the PCs and other CPE devices being connected to the cable network. The NAT/PAT features allow the customer to use private IP addresses on the local network, while still maintaining connectivity to the Internet.

Value Telecommuter

In addition to full DOCSIS 1.0 support and the Home Office (Easy IP) feature set, the Value Telecommuter feature set supports 56-bit IPsec encryption and the Layer 2 Tunneling Protocol (L2TP). These additional features allow employees to establish secure high-speed Internet connections between the employees' homes and the business' local area network (LAN).

IPsec encryption provides robust authentication and encryption of IP packets so that sensitive information can be securely transmitted over unprotected networks such as the Internet. The standard 56-bit Data Encryption Standard (DES) encryption provides sufficient security for most applications.

Note IPsec encryption is in addition to BPI encryption. BPI encryption is done only on the traffic between the Cisco uBR924 router and the CMTS, not on traffic sent over the Internet. IPsec encryption, however, is end-to-end encryption, protecting traffic sent across the Internet from one host to another.

L2TP is an extension of the Point-to-Point Protocol (PPP) that allows computers on different physical networks to interoperate as if they were on the same local network. L2TP and IPsec encryption are often used to create virtual private networks (VPNs).

Note The Cisco uBR924 cable access router does not support the L2TP feature in Cisco IOS Release 12.1(3)T and later releases.

Performance Telecommuter

The Performance Telecommuter feature set includes all of the features found in the Value Telecommuter image, but adds 168-bit IPsec Triple Data Encryption Standard (3DES) encryption. The advanced IPsec encryption provides a higher-level of security to protect very sensitive information, such as medical and banking records.

Value Small and Branch Office

The Value Small and Branch Office feature set adds the Cisco Secure Integrated Software firewall feature to the DOCSIS 1.0 support, Home Office (Easy IP), and 56-bit IPsec encryption feature sets, providing a wide range of security features for the Cisco uBR924 router. The Cisco uBR924 router uses the firewall capability to protect the computers in the local office network from threats such as denial of service attacks and destructive Java applets. The router can also provide real-time alerts of such attacks.

IPsec encryption provides robust authentication and encryption of IP packets so that sensitive information can be securely transmitted over unprotected networks such as the Internet. The standard 56-bit Data Encryption Standard (DES) encryption provides sufficient security for most applications.

Note The Cisco uBR924 cable access router does not support the L2TP feature in Cisco IOS Release 12.1(3)T and later releases.

Performance Small and Branch Office

The Performance Small and Branch Office feature set includes all of the features found in the Value Small and Branch Office image, but adds 168-bit IPsec Triple Data Encryption Standard (3DES) encryption. The advanced IPsec encryption provides a higher-level of security to protect very sensitive information, such as medical and banking records.

Feature Descriptions

This section describes the particular features that are contained in the feature sets supported by the Cisco uBR924 cable access router. See the Release Notes for any particular release for information on which features are contained in a particular Cisco IOS image.

Cable Monitor Web Diagnostics Tool

The Cable Monitor is a web-based diagnostic tool to display the current status and configuration of the Cisco uBR924 router. The Cable Monitor can also be used when the cable network is down, providing an easy way for subscribers to provide necessary information to service technicians and troubleshooters.

The Cable Monitor is introduced in Cisco IOS Release 12.1(1)T and is described in detail in Appendix B, "Using the Cable Monitor Tool."

Cisco Cable Clock Card Support

The Cisco uBR924 router automatically supports the use of the Cisco Cable Clock Card on the Cisco uBR7246 VXR universal broadband router. The National Clock Card enables the Cisco uBR7246 VXR router to use a primary and secondary external clock derived from a Stratum 1 source. This provides a high quality clocking signal that minimizes jitter and other timing problems that can interfere with real-time traffic such as VoIP calls.

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

Cisco IOS Firewall

The Cisco IOS Firewall feature set provides firewall-specific security features to the Cisco uBR924 router. When this feature is enabled, the Cisco uBR924 router acts as a buffer between the Internet and other public networks and the private network that is connected to the Cisco uBR924 router. Security is provided by access lists, as well as by examining incoming traffic for suspicious activity.

The security features include the following:

- Authentication proxy services to intelligently apply specific security policies on a per-user basis without impacting performance.
- Checking packet headers and dropping suspicious packets to detect and prevent denial of service attacks, such as ICMP and UDP echo packet flooding, SYN packet flooding, half-open or other unusual TCP connections, and deliberate mis-fragmentation of IP packets.
- Context-Based Access Control (CBAC) which gives internal-to-the-firewall users secure, per-application-based traffic control across the Internet/Intranet. This includes protection against Simple Mail Transfer Protocol (SMTP) attacks, one of the most common attacks against computers connected to the Internet.

- Dynamic port mapping to allow network applications with well-known port assignments to use customized 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 perform a number of actions: send an alarm to a syslog server or to NetRanger Director, drop the packet, or reset the TCP connection.
- Java blocking to protect against destructive Java applets. Applets can be allowed from only known and trusted sources or blocked completely.
- Real time and configurable alerts and audit trail capabilities to record and timestamp source and destination hosts.
- Support for a broad range of commonly used protocols, including H.323 and NetMeeting, FTP, HTTP, MS Netshow, RPC, SMTP, SQL*Net, and TFTP.
- User-configurable audit rules, real-time alerts, and audit-trail logs.

This feature is introduced in Cisco IOS Release 12.0(5)T and is enhanced with additional capabilities in 12.0(7)T.

Note For general information about these features, see the description of the *Cisco IOS Firewall Feature Set* in the Cisco *Product Catalog*. For detailed information, see the *Cisco IOS Firewall Feature Set* documentation set, as well as the sections on Traffic Filtering and Firewalls in the *Security Configuration Guide* and *Security Command Reference* (available on the Documentation CD-ROM and CCO).

DOCSIS-Compliant Bridging

DOCSIS-compliant bridging allows the Cisco uBR924 cable access router to operate as a DOCSIS 1.0 cable modem, so that it can interoperate with any DOCSIS-qualified CMTS. This is the default mode of operation for the Cisco uBR924 router.

This feature is introduced in Cisco IOS Software Release 12.0(4)XI1.

DOCSIS Baseline Privacy Interface

The DOCSIS Baseline Privacy Interface (BPI) feature is based on the DOCSIS BPI Specification (SP-BPI-I02-990319 or later revision). It provides data privacy across the Hybrid Fiber-Coaxial (HFC) network by encrypting traffic flows between the Cisco uBR924 router and the cable operator's CMTS.

This feature is introduced in Cisco IOS Software Release 12.0(5)T.

Dynamic Host Configuration Protocol Server

The DHCP server on the Cisco uBR924 router includes both Intelligent DHCP Relay and DHCP Client functionality. A DHCP Relay Agent is any host that forwards DHCP packets between clients and servers—this 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.

This feature is introduced in Cisco IOS Release 12.0(4)XI.

Dynamic Host Configuration Protocol Proxy Support

The DHCP Proxy Support feature is useful in two situations:

- When the Cisco uBR924 cable access router is configured for routing mode, an IP address must be assigned to its Ethernet interface. The DHCP Proxy Support feature allows an external DHCP server to assign an IP address to the Ethernet interface, as opposed to having to assign it manually with the appropriate CLI commands.
- When network address translation (NAT) is used, an inside global address pool must be created on the Ethernet interface. The DHCP Proxy Support feature allows a DHCP server to assign an IP address that automatically creates the NAT address pool, as opposed to manually specifying a static IP address with the appropriate CLI commands.

When configured for DHCP Proxy Support, during startup the Cisco uBR924 cable access router sends a proxy DHCP request to the DHCP server using the Ethernet interface's MAC address. The DHCP server replies with a second IP address that the router assigns to either the Ethernet interface or to the NAT pool, depending on which option was specified.

This feature is introduced in Cisco IOS Release 12.1(1)T and is described in detail in Appendix D, "New and Changed Commands Reference."

Enhanced IP Bridging

The Cisco uBR924 cable access router can transparently bridge traffic between its cable interface and its four RJ-45 hub ports with 10BaseT Ethernet connectivity. Up to four computers can be directly connected to these hub ports. Additional computers can be connected to the Cisco uBR924 router by connecting an Ethernet hub to one of the router's four ports; the hub, in turn, can be connected to additional computers or devices at the site.

A maximum of 3 devices can be bridged using Cisco IOS Release 12.0(4)XI images. A maximum of 254 devices can be bridged using Cisco IOS Release 12.0(5)T or higher images. (No limit exists when the Cisco uBR924 cable access router is operating in routing mode.)

This feature is introduced in Cisco IOS Release 12.0(5)T.

Note The maximum number of CPE devices also depends on the value of the "MAX CPE" field in the DOCSIS configuration file. The MAX CPE field defaults to one CPE device unless set otherwise. In this situation, the Cisco uBR924 router can connect only one computer to the cable network, regardless of the Cisco IOS Release being used.

Ecosystem Gatekeeper Interoperability Enhancements

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

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

The Cisco uBR924 cable access router automatically supports this feature when acting as an H.323v2 voice gateway. This feature has been implemented in two phases:

- Phase 1—Adds support for the alternate gatekeeper field (altGKInfo) to the gatekeeper rejection (GRJ) and registration rejection (RRJ) messages. This allows a gateway to move between gatekeepers during the gatekeeper request (GRQ) and registration request (RRQ) phases.
- Phase 2—Adds support for the alternate gatekeeper field (altGKInfo) to the admission rejection (ARJ) message. This allows a gateway to move between gatekeepers during the admission request (ARQ) phase.

Phase 1 of this feature is introduced in Cisco IOS Release 12.1(1)T. Phase 2 is introduced in Cisco IOS Release 12.1(2)T.

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

Fax over IP

Fax over IP is a form of VoIP support that supports the unique characteristics of fax transmissions. When using a voice-enabled image, the two voice ports on the Cisco uBR924 router can be connected to either fax machines or voice telephones, allowing fax traffic to be sent as VoIP traffic.

This feature is introduced in Cisco IOS Software Release 12.0(5)T.

H.323v2 (Gateway/Gatekeeper)

The Cisco uBR924 cable access router can support VoIP traffic as an H.323v2 gateway. The H.323v2 protocol maps an IP address to an E.164 telephone number, allowing VoIP calls to terminate either on other VoIP devices or on devices in the regular telco network. The H.323v2 protocol uses a dial plan and mapper on a server located at the CMTS or elsewhere to perform this mapping, which can be done either statically or dynamically, depending on the version of Cisco IOS software being used.

- In Cisco IOS Release 12.0(4)XI1 or higher images, the service provider can configure the IP addresses statically using the **voip dial peer group** command. The service provider can also configure the telephone numbers attached to the Cisco uBR924 cable access router by configuring the IP addresses statically using the CLI **pots port** command.
- In Cisco IOS Release 12.0(5)T or higher images, the service provider can obtain IP addresses dynamically from a Cisco gatekeeper using Registration, Admission, and Status (RAS). The service provider can also dynamically obtain telephone IP addresses using Cisco Network Registrar (CNR).
- Cisco IOS Release 12.1(1)T adds a number of H.323v2 features:
  - Fast Connect—This H.323v2 feature allows connections for the most common types of calls to be created without establishing a separate H.245 control channel.
  - H.245 Tunneling—Supports two H.245 features during a call without having to establish an H.245 channel:

    DTMF digit relay—Dual-tone multifrequency (DTMF) tones are often used during a voice call to convey information, such as entering an account number voicemail commands. Certain forms of compression (such as G.729) might interfere with these tones, so they must be transmitted "out of band," separated from the encoded voice stream.

    Hookflash relay—Many types of PBX and telephone switches give a special meaning to a hookflash (quickly depressing and releasing the hook on your telephone). Because this creates a voltage change that cannot be transmitted across an IP network, the H.323 protocol can send an H.245 User Input Indication message to convey the hookflash to the remote end.

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

- Cisco IOS Release 12.1(2)T adds H.323 support for virtual interfaces, allowing the use of the Ethernet interface's IP address for outgoing H.323 traffic, which includes H.225, H.245, and RAS messages. This enables the use of VoIP traffic over VPN solutions. See the **h323-gateway voip bind srcaddr** command for more information. In addition, the value of the H.225 TCP connection timeout timer is configurable.

Support for H.323 is introduced in Cisco IOS Release 12.0(4)XI1 and enhanced with support for H.323v2 in Cisco IOS Release 12.0(5)T. Additional H.323v2 features are added in Cisco IOS Release 12.1(1)T and Cisco IOS Release 12.1(2)T.

IP Address Negotiation

Cisco IOS Release 12.1(4)T for Cisco uBR900 series cable access routers adds support for the **ip address docsis** command on the cable interface. Previous releases used the **ip address dhcp** and **ip address negotiated** command for this purpose, but these commands cannot be used on cable interfaces.

IPsec Network Security

IPsec network security provides robust authentications and encryption of IP packets. IPsec is a framework of open standards developed by the Internet Engineering Task Force (IETF) for the secure 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 uBR924 cable access router.

Unlike BPI encryption, which protects traffic only on the cable interface between the cable modem and CMTS, IPsec encryption provides end-to-end protection across open networks such as the Internet. Two levels of encryption—56-bit and 168-bit—are available, depending on the software image being used.

This feature is introduced in Cisco IOS Release 12.0(5)T.

Note Cisco IOS images with strong encryption (including, but not limited to, 168-bit [3DES] data encryption feature sets) are subject to United States government export controls and have limited distribution. Strong encryption images to be installed outside the United States may require an export license. Customer orders may be denied or subject to delay due to United States government regulations. When applicable, the purchaser or user must obtain local import and use authorizations for all encryption strengths. Contact your sales representative or distributor for more information, or send an e-mail to export@cisco.com.

Layer 2 Tunneling Protocol

Layer 2 Tunneling Protocol (L2TP) is an IETF standard that combines the best features of two existing tunneling protocols: Cisco's Layer 2 Forwarding (L2F) and Microsoft's Point-to-Point Tunneling Protocol (PPTP). L2TP extends the Point-to-Point Protocol (PPP) to provide a secure connection across an open network and is an important component for virtual private networks (VPNs).

This feature is introduced in Cisco IOS Release 12.0(5)T and is supported through Cisco IOS Release 12.1(2)T. L2TP is not supported in Cisco IOS Release 12.1(3)T or later images.

Note Cisco IOS Release 12.1(5)T, 12.2(2), or greater is required to support GRE IP tunnels.

Media Gateway Control Protocol V12.1.3T

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

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

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

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

NetRanger Support—Cisco IOS Intrusion Detection

The Cisco uBR924 router supports NetRanger, which is an Intrusion Detection System (IDS) composed of three parts:

- A management console (director) that displays alarms and manages the sensors.
- One or more sensors that monitor traffic, comparing it to a list of known signatures to detect misuse of the network. When a signature is matched, the sensor can take certain actions, such as resetting a session, dropping traffic, or sending alarms to the director.
- Automated report generation of standardized and customizable reports.

This feature is introduced in Cisco IOS Release 12.0(7)T.

Network Address Translation and Port Address Translation

Network address translation (NAT) and port address translation (PAT) frees a private network from the requirement of having a worldwide unique IP address for every computer connected to the Internet. Instead, the Cisco uBR924 router translates the IP addresses used on the private network into a global IP address that can be used on the Internet. One IP address can be used for multiple computers because the Cisco uBR924 router uses a unique port address to identify individual computers on the private network.

This feature is introduced in Cisco IOS Release 12.0(4)XI1.

Network Address Translation Support for NetMeeting Directory (Internet Locator Service)

Microsoft NetMeeting is a Windows-based application that allows users to interact and collaborate using their PCs over the Internet or an intranet. Previously, users had to know the IP addresses of other users' PCs to make a connection. The NetMeeting Directory (ILS) feature enables the users to connect by using the names that are in the directory built into the NetMeeting application. Users no longer need to know the destination IP addresses to make a connection.

This feature is introduced in Cisco IOS Release 12.1(5)T.

Quality of Service

Quality of service (QoS) is a set of features that identify different types of traffic on a network so that certain types of traffic can be given higher priority than other types of traffic that have only a "best effort" attempt at delivery. This feature is especially important for real-time traffic, such as voice traffic, where delays would have a serious impact on the traffic's usefulness.

Depending on the software image used, the Cisco uBR924 cable access router supports the following QoS features:

- Resource Reservation Protocol (RSVP)—Layer 3 QoS signaling protocol that provides for the reservation of resources across an IP network. Applications running on IP end systems can use RSVP to indicate to other nodes the nature (such as bandwidth, jitter, and maximum burst) of the packet streams they want to receive. RSVP is defined in RFC 2205.
- Distributed Open Signaling Architecture/Session Initialization Protocol (DOSA/SIP)—Call flow protocol that uses the AT&T VoIP over cable architecture.
- DOSA/QoS—Quality of service mechanism used on the AT&T VoIP over cable architecture.
- Committed Access Rate (CAR)—Specifies the minimum bandwidth that is guaranteed for a particular type of traffic.
- Multi-Service Identifier (SID)—Allows a service provider to offer different classes of service to its customers, so that different types of traffic can be given different priorities of service.
- Traffic Shaping—Process of delaying packets that would otherwise be dropped because they exceed the rate limit on a particular cable modem's upstream. The Cisco uBR924 router buffers the upstream packet until bandwidth is available. This is particularly important with TCP/IP traffic because when a TCP packet is dropped, the destination device automatically drops all other packets it currently contains in its receive buffer and then requests the retransmission of those packets. This retransmission of packets increases the congestion that already exists in this situation, drastically reducing overall throughput.

These features are introduced in Cisco IOS Release 12.0(7)T and enhanced in subsequent releases.

Quality of Service—DOCSIS 1.0+ Extensions

In addition to the other QoS features, DOCSIS 1.1 supports a number of features that are required for the delivery of high quality voice traffic. To use these features before the DOCSIS 1.1 specification is finalized, Cisco has created the DOCSIS 1.0+ extensions that contain the most important of these features.

- Concatenation—DOCSIS concatenation combines multiple upstream packets into one packet to reduce packet overhead and overall latency, as well as increase transmission efficiency. Using concatenation, a DOCSIS cable modem makes only one bandwidth request for multiple packets, as opposed to making a different bandwidth request for each individual packet; this technique is especially effective for bursty real-time traffic, such as voice calls.
- Dynamic Multi-SID Assignment—To give priority to voice traffic, the Cisco uBR924 router assigns a different SID to each voice port. Without the DOCSIS 1.0+ extensions, the router creates these SIDs during the provisioning process, and the SIDs remain in effect until the router is rebooted with a different configuration. As part of this process, a minimum guaranteed bandwidth is permanently allocated to the voice ports; this bandwidth is reserved to the voice ports even if no calls are being made.

To avoid potentially wasting bandwidth in this manner, the DOCSIS 1.0+ extensions support the dynamic creation of multiple SIDs. New MAC messages dynamically add, delete, and modify SIDs when needed. When a phone connected to the router is taken off-hook, the Cisco uBR924 router creates a SID that has the QoS parameters needed for that particular voice call. When the call terminates, the router deletes the SID, releasing its bandwidth for use elsewhere.

The DOCSIS 1.0+ features are introduced in Cisco IOS Software Release 12.0(7)XR and 12.1(1)T.

Note Both the Cisco uBR924 cable access router and the CMTS router must support the dynamic multi-SID and concatenation features for them to be used on the cable network. If you are using the Cisco uBR7200 series universal broadband router as the CMTS, Cisco IOS Release 12.0(7)XR, Release 12.1(1)T, or later is required on both the Cisco uBR924 and Cisco uBR7200 series routers to use these features.

Routing Information Protocol Version 2

When configured for routing mode, the Cisco uBR924 cable access router defaults to using the Routing Information Protocol Version 2 (RIPv2). In routing mode the Cisco uBR924 router automatically configures itself to use the headend's IP address as its IP default gateway. This allows the Cisco uBR924 router to send packets not intended for the Ethernet interface to the headend.

RIPv2 routing is useful for small internetworks because it optimizes 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.

This feature is introduced in Cisco IOS Release 12.0(4)XI1.

Note The Cisco uBR924 cable access router supports only static routes and the RIPv2 routing protocol.

Secure Shell Version 1

The Cisco uBR924 router supports the Secure Shell (SSH) Version 1 protocol, which allows network administrators to make a secure Telnet connection with the router. SSH provides for authentication and encryption at the application layer, providing a secure connection even when BPI or IPsec authentication and encryption are not used at the network layer.

By default, the SSH feature uses 56-bit DES encryption. Higher security 168-bit 3DES encryption is available when using Cisco IOS images that support 3DES IPsec encryption. (The SSH server and client must support the same level of encryption.)

SSH server support is introduced in Cisco IOS Release 12.1(1)T. SSH client support is introduced in Cisco IOS Release 12.1(3)T.

Note For configuration and other information, see the *Secure Shell Version 1 Client* feature module, available on CCO and the Documentation CD-ROM.

Simple Gateway Control Protocol

The Simple Gateway Control Protocol (SGCP) provides for control call setup and teardown for VoIP calls made through the Internet or a local Intranet. SGCP uses call control agents to communicate with the voice gateways, allowing customers to create a distributed system that enhances performance, reliability, and scalability while still appearing as a single VoIP gateway to external clients.

SGCP can preserve Signaling System 7 (SS7) style call control information, as well as additional network information, such as routing information and authentication, authorization, and accounting (AAA) security information. SGCP allows voice calls to be originate and terminate on the Internet, as well as allowing one end to terminate on the Internet and the other to terminate on a telephone or PBX on the Public Switched Telephone Network (PSTN).

The Cisco uBR924 cable access router functions as an SGCP residential gateway (RGW), not as the trunking gateway (TGW), which controls the telephone call.

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

This feature is introduced in Cisco IOS Release 12.0(5)T and enhanced in Release 12.0(7)T. In Cisco IOS Release 12.1(3)T, this feature is merged with the Media Gateway Control Protocol V12.1.3T feature, providing simultaneous support for both SGCP and MGCP.

Triple Data Encryption Standard

The Data Encryption Standard (DES) is a standard cryptographic algorithm developed by the United States National Bureau of Standards. The Triple DES (3DES) standard increases the security from the standard 56-bit IPsec encryption to 168-bit encryption, providing a level of security that is suitable for highly sensitive and confidential information such as financial transactions and medical records.

This feature is introduced in Cisco IOS Release 12.0(5)T.

Note Cisco IOS images with strong encryption (including, but not limited to, 168-bit [3DES] data encryption feature sets) are subject to United States government export controls and have limited distribution. Strong encryption images to be installed outside the United States may require an export license. Customer orders may be denied or subject to delay due to United States government regulations. When applicable, the purchaser or user must obtain local import and use authorizations for all encryption strengths. Contact your sales representative or distributor for more information, or send an e-mail to export@cisco.com.

Note Cisco IOS Release 12.1(5)T, 12.2(2), or greater is required to support GRE IP tunnels.

VPN IPsec Enhancement—Dynamic Crypto Map

The **crypto dynamic-map** command is part of the Cisco Secure PIX firewall and IPsec network security feature. The **crypto dynamic-map** command creates dynamic crypto maps, which are policy templates used when processing negotiation requests for new security associations from a remote IPsec peer. This allows you to negotiate a session even if you do not know all of the remote peer's crypto map parameters (such as the peer's IP address); in particular, this allows you to accept requests for new security associations from previously unknown peers, while still requiring the peer to complete the proper ISAKMP (IKE) authentication.

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

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

The **crypto dynamic-map** global configuration command supports a number of options, but the only required option is the transform-set. The other parameters are optional, depending on the needs of your network.

This feature is introduced in Cisco IOS Release 12.0(7)T.

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

Initial Provisioning

The Cisco uBR924 cable access router typically ships from the Cisco factory ready to work in the Base IP DOCSIS-Compliant Bridging data-only mode. However, before router can transmit either data or voice traffic, the CMTS at the headend must properly provision the router as follows:

- The appropriate service must be purchased from the service provider. If certain features, such as voice support or advanced encryption, are desired, a license for the appropriate Cisco IOS software image must also be purchased.
- The service provider must create a DOCSIS configuration file for the Cisco uBR924 router. This file must be stored on a TFTP server—each router could have its own unique DOCSIS configuration file, or the same file could be used for multiple routers, depending on the needs of the subscribers.
- When the router is first brought online, the CMTS at the headend downloads the DOCSIS configuration file to the router. This file is a binary file that configures the router for the appropriate level of services and that sets other parameters as needed.
- At this point the router is completely configured for the basic DOCSIS bridging mode, but when additional features are required, the DOCSIS configuration file specifies that the CMTS should download a second Cisco IOS image to the router. For example, to enable Triple DES encryption on the Cisco uBR924 router, a Cisco IOS image with 3DES IPsec support must be downloaded to the router. (The service provider can also preload the router with this image at the warehouse to speed up the router's initialization and boot time.)
- Finally, any additional configuration on the router must be done. This can be done in the following ways:
  - When using Cisco IOS Release 12.1(1)T or greater, CLI commands can be embedded in the DOCSIS configuration file, using the Vendor Specific Information Field (subtype 131).
  - The router can download a Cisco IOS configuration file from a host workstation specified by the DOCSIS configuration file. The Cisco IOS configuration file is an ASCII text file that contains the Cisco IOS commands needed to configure the router.
  - A system administrator can manually configure the router by giving Cisco IOS commands at the router's CLI interface. This can be done either locally by connecting to the router's RJ-45 console port or remotely by establishing a Telnet connection with the router.

Note The CMTS typically downloads the DOCSIS configuration file, Cisco IOS image (if needed), and 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 offers new services or when subscribers upgrade their services.

To ensure that subscribers obtain the exact services they have ordered, the Cisco uBR924 cable access router arrives from the Cisco factory with a unique identifier (UID) that consists of a serial number and media access control (MAC) address. These factory-assigned values are on a label at the bottom of the router; for convenience, these values are also in a barcode label that can be scanned in for easy entry into the service provider's provisioning and billing system.

Using the MAC address of the router as the key, the CMTS downloads the DOCSIS configuration file and Cisco IOS image that will provide the services this particular subscriber has 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 that Cisco Systems provides for this purpose.

Note For a more detailed description of the provisioning process, see the *Cisco uBR924 Cable Access Router Hardware Installation Guide*, available on CCO and the Documentation CD-ROM.

Supporting Multiple Classes of Service

In data-only mode, the Cisco uBR924 cable access router typically uses only one class of service (CoS) profile that provides for best-effort delivery of data traffic. In data and voice mode, however, multiple CoS profiles are required so that the real-time voice traffic can be given a higher priority than normal data traffic. This allows voice traffic to be delivered in a timely manner by delaying transmission of data traffic in a way that does not degrade the overall quality of service (QoS).

DOCSIS 1.0 Static Profiles

In a DOCSIS 1.0 network, the multiple CoS profiles must be created at the time the Cisco uBR924 router is registered, using the CoS parameters in the DOCSIS configuration file. To support voice services in a DOCSIS 1.0 environment, the service provider typically specifies a primary CoS profile for best-effort data and second CoS profiles for voice and fax traffic.

The router requests the multiple profiles in a registration request message sent to the CMTS. In response, the CMTS assigns a Service Identifier (SID) for each CoS profile. The first SID assigned is the primary SID that is used for best effort data traffic as well as for the handling of MAC and maintenance messages. The other SIDs are secondary SIDs used for voice and fax traffic. These SID assignments remain in effect until the modem resets and reregisters itself using a different configuration.

DOCSIS 1.0+ and 1.1 Dynamic Profiles

When the Cisco uBR924 cable access router is running DOCSIS 1.0+ software, the router does not need to request additional SIDs at registration time. Instead, the router specifies the number of phone lines connected to the router, using the Vendor Specific Information Field (VSIF) in the DOCSIS configuration file.

When one of the phones connected to the Cisco uBR924 router is taken off-hook, the router sends an Unsolicited Grant (UG) request to the CMTS, which responds by assigning a SID for that voice call. This dynamically-created SID is assigned a secondary CoS profile that matches the type of call being made (voice or fax). When the voice or fax call terminates, its SID is deleted so the bandwidth can be used by another user.

Creating Multiple Profiles

In both DOCSIS 1.0 and 1.1 environments, the provider must create and maintain multiple CoS profiles for voice and fax users. Typically, different CoS profiles are used for voice and fax traffic because these services use different codec algorithms that have different timing requirements.

The provider could assign the same CoS profiles for all voice and fax users, or the provider could create a number of different CoS profiles that provide different levels of service, depending on the number of voice lines and other services purchased. This latter approach requires a method of associating a particular profile with specific users.

For this purpose, Cisco offers a set of software products for DOCSIS provisioning of different CoS profiles:

- User Registrar for subscriber self-provisioning and administration
- Modem Registrar for cable modem management
- Cisco Network Registrar for DNS and DHCP services
- Access Registrar for RADIUS services in one-way modems and roaming

This set of software products can be used by the service provider deploying a subscriber provisioning system. The following sections describe each product in brief; for complete details, see the *Cisco Subscriber Registration Center* documentation set, available in the *Network Management* section of CCO and the customer documentation CD-ROM. Also see the *Cisco Network Registrar for the Cisco uBR7200 Series* documentation.

User Registrar

User Registrar (UR) provides a set of web pages and extensions that enable subscriber self-registration. User Registrar addresses the needs of three separate classes of users in the provisioning system implemented by the customer (typically a service provider). This software tool addresses the needs of the:

- *Subscriber* who may be signing up for network services for the first time, or augmenting services. The set of options for the subscriber is determined by the customer and will change between customers, even in the same industry.
- *Administrator* who will be called on to generate reports for individual users, generate system wide reports and resolve provisioning system problems that a subscriber may have.
- *Configurer* who is responsible for making modifications to the templates and workflows that define a customer's solution. This role may also involve building interfaces to the customer's existing business systems.

User Registrar includes the following features:

- Web-based user interface, including HTML templates workflow scripts that provide a sample out-of-the-box user provisioning system with a set of "extension points" for the most anticipated customizations.
- Multi-level subscriber service privileges

- Subscriber authentication and service validation
- Workflow scripts and templates can be customized as needed to suit a customer's needs
- Cable modem reset via SNMP
- A preliminary set of NAS extensions to communicate with supported backend customer systems. This includes interfaces to a central LDAP directory and Network Registrar (via NRCMD).

Modem Registrar

Modem Registrar (MR) provides dynamic generation of DOCSIS configuration files based on network and service policies. It builds DOCSIS configuration files for clients based on parameters stored in an LDAP directory. The customized DOCSIS configuration file is sent to the Cisco uBR924 cable access router using TFTP as part of the normal modem registration process.

Modem Registrar includes the following features:

- Policy based dynamic creation of DOCSIS configuration files
- Web-based user interface to define the policies for creating configuration files
- A fully functional TFTP server

Cisco Network Registrar

Cisco Network Registrar (CNR) supplies IP addresses and configuration parameters for DOCSIS cable modems and PCs based on user-defined network and service policies. CNR also allocates host names for these devices in DNS and the related information is stored in an LDAP directory.

CNR assigns available IP addresses from address pools based on the identity or type of the requesting device and the policies in effect. For example, CNR can distinguish between registered devices, unregistered devices, and registered devices that have been assigned to a particular class of service.

Key features of Cisco Network Registrar include:

- DHCP server, with multiple address pools and multiple policies that can define different DHCP options based on the address pool being used
- DNS server and dynamic DNS updates
- Verification of address usage prior to allocation
- Address pools on multiple subnets, secondary subnets on the same wire, and BOOTP
- DHCP operation over routers using BOOTP relay
- CLI and web-based GUI access

Access Registrar

Access Registrar (AR) provides authorization and authentication services for DOCSIS-compliant modems that operate in a one-way cable plant requiring telco-return for upstream data. AR services can also provide dial-in data services for users who are roaming outside their cable service area. AR returns configuration parameters from RADIUS servers to NAS clients based on per-subscriber policies, which are obtained from an LDAP directory.

Note AR does not apply to Cisco uBR924 cable access routers, which are two-way devices that do not require telco-return services.

CHAPTER 2

DOCSIS-Bridging Configuration

This chapter describes the default configuration of the Cisco uBR924 cable access router. With this configuration, the Cisco uBR924 router functions in its "plug and play" DOCSIS-bridging mode, performing as a DOCSIS-compliant two-way cable modem. Every DOCSIS-compliant cable modem provides the following minimum set of features:

- Automatically provisions and configures itself using the DOCSIS configuration file that is downloaded from a server at the headend.
- Acts as a transparent bridge to send IP data traffic between its Ethernet and cable interfaces, providing connectivity from the customer's system to the Internet backbone.
- Provides Internet connectivity to PCs or other CPE devices connected to the Cisco uBR924 router.

Note In Cisco IOS Release 12.1, Voice over IP (VoIP) traffic is automatically supported when using the DOCSIS-bridging mode. However, in Cisco IOS Release 12.0, the default "plug and play" image does not enable the Cisco uBR924 router's voice ports. To enable the voice ports, you must use a Cisco IOS image with voice support and download an appropriate Cisco IOS configuration file. See Chapter 4, "Voice over IP Configurations," for more information.

The following sections describe the configuration for "plug and play" DOCSIS bridging:

The DHCP server configuration and DOCSIS configuration file are required for every DOCSIS-compliant cable modem. The Cisco IOS image and configuration files are optional, depending on the needs of the subscribers. The remaining configurations are optional, depending on the needs of the subscribers.

The information described in this chapter applies to every Cisco uBR924 cable access router that is used in a DOCSIS-compliant network. Additional configuration steps might be needed, however, to support additional features, such as VoIP and IPSec encryption—this additional configuration is described in the other chapters in this guide.

Caution Before attempting to reconfigure the Cisco uBR924 cable access router at a subscriber site, contact your provisioning or billing system administrator to ensure 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 Cisco uBR924 router is powered off and on. Instead, the router's settings will return to the previous configuration.

DHCP Server Configuration

The DOCSIS specification (SP-RFI-IO5-991105 or later revision) requires that a DOCSIS-compliant cable modem connect to a DHCP server at power-on or reset to establish temporary IP connectivity with the cable network. This enables the cable modem to download the additional configuration information needed to establish a permanent connection with the headend and cable network.

The DHCP server can be a CMTS with DHCP server capabilities (such as a Cisco uBR7200 series universal broadband router), or it can be a dedicated server located at the headend. The server can be configured manually for each cable modem or it can be part of an automated provisioning system such as Cisco Network Registrar (CNR).

Note The DOCSIS specification requires that every DOCSIS cable modem obtain its IP address from an authorized DHCP server during the reset or power-on provisioning process. Any IP address specified in an IOS configuration file is overwritten by the one assigned by the DHCP server. The only way to assign a static IP address to a cable modem is to configure the DHCP server so that it assigns the desired IP address on the basis of the cable modem's MAC address. However, service providers should warn subscribers that changes in the cable network's topology—due to traffic levels, growth, or changes to the cable plant and other hardware—might still require changing the subnets and IP addresses assigned to a particular cable modem.

The DHCP server provides the information shown in Table 2-1 to each cable modem.

Table 2-1 DHCP Server Parameters

Parameter	Description
IP address for the cable modem's cable interface	This IP address typically is assigned dynamically but the service provider can also statically assign IP addresses on the basis of each modem's MAC address. **Note** When the router is in DOCSIS-bridging mode, it automatically assigns this IP address to both the cable and Ethernet interfaces. When the router is in routing mode, it assigns this IP address only to the cable interface; the IP address for the Ethernet interface must be configured separately.
IP subnet mask for the cable modem's cable interface	This subnet mask typically is used for all cable modems using the same downstream, but this depends on the setup of the CMTS network as well as subscribers' needs.
IP address for the TFTP server	This TFTP server provides the DOCSIS configuration file to the cable modem and is typically a dedicated server located at the headend.

Table 2-1 DHCP Server Parameters (continued)

Parameter	Description
IP address for the DHCP relay agent	A DHCP relay agent is required if the DHCP server is located on a different network than the IP address assigned to the cable modem's cable interface. The DHCP relay agent is also used if the DHCP server is providing IP addresses to the CPE devices connected to the cable modem and the CPE devices are on a different subnet than the cable modem.
Complete filename for the DOCSIS configuration file	This is the filename for the DOCSIS configuration file that the cable modem should download from the TFTP server.
IP address for one or more time of day (ToD) servers	The cable modem uses the ToD server to get the current date and time so that it can accurately timestamp its SNMP messages and error log entries.
One or more IP addresses for the routers that will forward IP traffic from the cable modem	Typically, the CMTS acts as the default gateway for the cable modem. **Note** Typically, the DHCP server sets the default gateway for DOCSIS cable modems. When this is done on Cisco routers, the default gateway does not appear in the Cisco IOS configuration file, to indicate that the gateway is being set dynamically by the DHCP server and should not be saved after a reset of the router. To display the default gateway, use the **show ip default-gateway** command.
One or more IP addresses for System Log (SYSLOG) servers	The cable modem can send its error log messages to the SYSLOG servers, which are optional and typically located at the headend.

After making a successful DHCP request, the cable modem contacts the ToD server to get the current date and time. It also begins the TFTP download of the DOCSIS configuration file, which is described in the next section, "DOCSIS Configuration File" section on page 2-3.

Note At this point in the registration process, the DHCP server provides an IP address only for the cable modem, not for the CPE devices it is connecting to the network. The same DHCP server can provide the IP addresses for the CPE devices after the cable modem goes online, or the cable modem itself can be configured as a DHCP server (see "Routing with DHCP Server" section on page 3-4).

DOCSIS Configuration File

The DOCSIS specification requires that a DOCSIS-compliant cable modem download a DOCSIS configuration file during its power-on or reset sequence. This file must be in the format described in the SP-RFI-IO5-991105 specification (or later revision) and must contain the information shown in Table 2-2.

Note The parameters shown in Table 2-2 are organized according to the categories used in the Cisco DOCSIS Cable Modem Configuration tool, which is available on CCO at http://www.cisco.com/support/toolkit/CableModem. (You must have an account on CCO to access this tool.)

Table 2-2 DOCSIS Configuration File Parameters

Parameter[1]	Description
Radio Frequency Parameters	
Downstream Frequency	Specifies the center frequency (in multiples of 62500 Hz) for the downstream channel to be used by the router. (This parameter does not need to be specified in the configuration file because the router will scan the downstream for available frequencies, but typically it is specified to ensure that the router conforms to the provider's channel plan.)
Upstream Channel ID	Specifies channel ID for the upstream channel to be used by the router. (This parameter does not need to be specified in the configuration file because it can be set dynamically by the CMTS during provisioning.)
Network Access Configuration	Determines whether CPE devices attached to the cable modem are allowed access to the cable network. The default is to allow access for CPE devices (which is required for normal operations).
Class of Service	
Class of Service ID	Specifies the ID for this class of service (1–16).
Maximum Downstream Rate	Specifies the maximum downstream data rate (in bits/sec) allowed for traffic associated with this class of service. (This is a limit, not a guarantee of service.)
Maximum Upstream Rate	Specifies the maximum upstream data rate (in bits/sec) allowed for traffic associated with this class of service. (This is a limit, not a guarantee of service.)
Upstream Channel Priority	Specifies the priority for upstream traffic (0–7, where 7 is highest priority).
Minimum Upstream Rate	Specifies the minimum upstream data rate (in bits/sec) that is guaranteed for traffic associated with this class of service.
Maximum Upstream Channel Burst	Specifies the maximum size of burst traffic to be allowed on this upstream channel. The size is specified in bytes, 0–65535, where 0 is no limit. If this field is set to a non-zero value, it should be set to at least 1800 so that it is greater than the maximum Ethernet frame size of 1518 plus the associated packet overhead).
Class of Service Privacy Enable	Specifies whether BPI encryption should be enabled on traffic associated with this class of service (1 enables BPI encryption, 0 disables BPI encryption).
Vendor Specific Options	
Vendor ID	The three-byte Organization Unique Identifier for the vendor, which is also usually the first three bytes of the cable modem's MAC address. This value is usually expressed as a hexadecimal number. This field should be "**00000C**" for Cisco Systems routers.
Vendor-Specific Options	Contains any arbitrary values that are defined by the manufacturer of the cable modem. The Cisco uBR924 cable access router uses this field to identify the Cisco IOS configuration file that should be downloaded (if any). Arbitrary Cisco IOS commands can also be specified in this field.
SNMP Management	
SNMP Write-Access Control and SNMP MIB Objects	Allows the service provider to set arbitrary SNMP attributes on the cable modem. For the Cisco uBR924 router, these two fields are typically used to enable SNMP management of the router because SNMP management is disabled by default. **Note** If using the Cisco DOCSIS Cable Modem Configurator tool, you can enable SNMP management by filling in the IP address for the SNMP manager. The Configurator tool then prepares the proper MIB objects to enable SNMP access.

Table 2-2 DOCSIS Configuration File Parameters (continued)

Parameter[1]	Description
Baseline Privacy Interface Configuration	
Authorize Wait Timeout	Specifies the retransmission interval, in seconds, of Authorization Request messages from the Authorize Wait state. Valid values are 2–30 seconds.
Reauthorize Wait Timeout	Specifies the retransmission interval, in seconds, of Reauthorization Request messages from the Authorize Wait state. Valid values are 2–30 seconds.
Authorization Grace Timeout	Specifies the grace period for re-authorization, in seconds. Valid values are 1–1800 seconds.
Operational Wait Timeout	Specifies the retransmission interval, in seconds, of Key Requests from the Operational Wait state. Valid values are 1–10 seconds.
Rekey Wait Timeout	Specifies the retransmission interval, in seconds, of Key Requests from the Rekey Wait state. Valid values are 1–10 seconds.
TEK Grace Time	Specifies the grace period for re-keying, in seconds. Valid values are 1–1800 seconds.
Authorize Reject Wait Timeout	Specifies how long, in seconds, a cable modem waits in the Authorize Reject Wait state after receiving an Authorization Reject. Valid values are 60–1800 seconds.
Customer Premises Equipment	
Maximum Number of CPEs	Determines the maximum number of CPE devices that can use the cable modem to connect to the cable network. The default value is 1. In bridging mode, the Cisco uBR924 router supports a maximum number of either 3 or 254 CPE devices, depending on the Cisco IOS software release being used.
CPE Ethernet MAC Address	Configures the cable modem with the MAC addresses for one or more CPE devices that are allowed to connect to the cable network. Entering values in this field is optional because the cable modem can learn the MAC addresses of CPE devices dynamically, up to the maximum allowable number. However, DOCSIS cable modems give priority to the CPE devices whose MAC addresses are in the configuration file.
Software Upgrade	
TFTP Software Server IP Address	Specifies the IP address for the TFTP server that will provide software images. This server does not necessarily have to be the same TFTP server that provided the DOCSIS configuration file.
Software Image Filename	Specifies the fully qualified path name for the software image that the cable modem should be running. If necessary, the cable modem uses TFTP to download this image from the software server.

Table 2-2 DOCSIS Configuration File Parameters (continued)

Parameter[1]	Description
Miscellaneous	
Concatenation Support	Specifies whether the cable modem supports DOCSIS 1.1 concatenation of upstream packet requests.
Use RFC2104 HMAC-MD5	Specifies the algorithm used to compute the CMTS Message Integrity Check (MIC). If yes, the HMAC-MD5 algorithm specified in RFC 2104 is used; otherwise, the algorithm specified by RFC 1321 is used. (The algorithm used must match the one used on the CMTS.) **Note** Because the RFC 1321 algorithm can be reversed, Cisco strongly recommends the use of only the more secure HMAC-MD5 algorithm.
CMTS Authentication	Specifies an authentication string to be used between the provisioning server (which creates the configuration files) and the CMTS. It allows the CMTS to authenticate the CM provisioning with a central authentication service, such as a RADIUS server. This field is typically used only for one-way cable modems that use telco-return.

1. The DOCSIS configuration file also contains fields for one-way cable modems that use telco-return, but these fields do not apply to the Cisco uBR924 router, which is a two-way cable modem.

Cisco IOS Software Image

The DOCSIS configuration file contains the filename for the software image that the Cisco uBR924 router must be running. If this filename does not match the software image that is currently installed on the router, the router must use the TFTP protocol to download the new image from the server specified in the DOCSIS configuration file.

After the new software image has been downloaded, the Cisco uBR924 router resets itself and repeats the entire power-on and provisioning process. This includes downloading the DOCSIS configuration file again. However, because the software image is stored in non-volatile Flash memory, the router does not have to download it again—the software download occurs only when the service provider specifies a new software image filename in the DOCSIS configuration file.

If the Cisco uBR924 router cannot download the new image, it retries the download, up to a maximum of 16 attempts. If the router still cannot download the image, it falls back to its previous software image and attempts to go online with that image.

The service provider can also force the Cisco uBR924 router to download new software by putting a new image filename in the DOCSIS configuration file and resetting the router. This should be done only after warning the customer that the modem will be offline for a period of several minutes.

Note Because it can take several minutes for this download to be accomplished and for the Cisco uBR924 router to repeat its power-on sequence, the desired software image can also be installed on the router at the warehouse. In this case, the DOCSIS configuration files for each router should also be updated with the proper filename.

Cisco IOS Configuration File

The DOCSIS configuration file uses the type 43 Vendor-Specific Options field to specify that the Cisco uBR924 router should download a Cisco IOS configuration file. The router's console port is automatically disabled as part of this process to prevent users at the remote site from reconfiguring the router.

Note Downloading a Cisco IOS configuration file is not usually required for plug-and-play bridging. Instead, it is normally used to configure the advanced feature sets that are described in the other chapters of this guide.

Using the Vendor-Specific Information Field

Table 2-3 shows the values that would be entered in the Vendor-Specific Information Field (VSIF) to download a Cisco IOS configuration file and automatically disable the console port.

Table 2-3 Downloading a Cisco IOS Configuration File (with console port disabled)

Field	Value
Subtype	128
Length	(number of characters in the filename)
Filename	Complete filename, including path, for the Cisco IOS configuration file on the TFTP servers specified in the DOCSIS configuration file. **Note** The Cisco IOS configuration file can contain only global configuration mode commands, not Privileged EXEC commands.

Table 2-4 shows the values that would be entered in the Vendor-Specific Information Field (VSIF) to specify a CLI command that should be executed after the Cisco uBR924 cable access router processes the DOCSIS configuration file and comes online.

Table 2-4 Specifying CLI Commands

Field	Value
Subtype	131
Length	(number of characters in the command)
CLI Command	The ASCII characters of one CLI command, as you would type it at the CLI prompt. To specify multiple commands, use this option once for each command. **Note** You can specify only global configuration mode commands, not Privileged EXEC commands, in this field.

Tip The VSIF option to include CLI commands in the DOCSIS configuration file should be used to specify a very limited number of commands for specialized applications. To perform a more substantial configuration of the router, use VSIF option 128 to download a Cisco IOS configuration file. Also see Appendix A, "Using Cisco IOS Software."

Sample Configuration for DOCSIS-Compliant Bridging

The following shows a typical Cisco IOS configuration for a Cisco uBR924 router that is operating in "plug and play" DOCSIS-compliant bridging mode.

```
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 directed-broadcast
 no ip route-cache
 bridge-group 59
 bridge-group 59 spanning-disabled
!
interface cable-modem0
 ip address dhcp
 no ip directed-broadcast
 no ip route-cache
 bridge-group 59
 bridge-group 59 spanning-disabled
!
ip classless
no ip http server
no service finger
!
!
line con 0
 transport input none
line vty 0 4
!
end
```

This configuration shows the following requirements for DOCSIS-compliant bridging:

- IP routing is disabled.
- No IP address is assigned to the cable interface; instead, the **ip address dhcp** command indicates that a DHCP server assigns an IP address to the cable interface. The Ethernet interface uses the same IP address because the router is acting as a bridge between the two interfaces, making them part of the same IP network—when the router is in DOCSIS-bridging mode, the IP addresses are automatically assigned during the provisioning process.

Configuring the Attached CPE Devices

In its "plug-and-play" bridging mode, the Cisco uBR924 router does not need any additional configuration to support the computers or other CPE devices that will access the Internet through the router's connection to the cable network. However, the PCs and CPE devices must be configured to support DHCP allocation of IP addresses.

Each computer and CPE device performs this configuration differently. For Windows 95, for example, you would open up the Network control panel, select the computer's TCP/IP Ethernet adapter, and set the IP address configuration to "Obtain and IP address automatically."

Reconfiguring DOCSIS-Compliant Bridging

To reconfigure the Cisco uBR924 router to support DOCSIS-compliant bridging after it has been configured for routing, log in to the Cisco uBR924 router, enter global configuration mode, and enter the following commands:

	Command	Purpose
Step 1	uBR924(config)#**no ip routing**	Disable IP routing on the Cisco uBR924 router.
Step 2	uBR924(config)#**int e 0**	Enter interface configuration mode for the Ethernet interface.
Step 3	uBR924(config-if)# **no ip address**	Remove the IP address from the Ethernet interface.
Step 4	uBR924(config-if)# **no ip route-cache**	Remove the high-speed switching caches for IP routing.
Step 5	uBR924(config-if)# **bridge-group** *bridge-group*	Assign the Ethernet interface to a bridge spanning group (choose an arbitrary integer from 1–63).
Step 6	uBR924(config-if)# **bridge-group** *bridge-group* **spanning-disabled**	Disable the spanning tree on the Ethernet interface.
Step 7	uBR924(config-if)# **exit**	Exit the interface configuration mode for the Ethernet interface.
Step 8	uBR924(config)# **int c 0**	Enter interface configuration mode for the cable interface.
Step 9	uBR924(config-if)# **no ip address**	Remove the IP address from the cable interface.
Step 10	uBR924(config-if)# **no keep alive**	Disable keepalive messages on the cable interface.
Step 11	uBR924(config-if)# **no ip route-cache**	Remove the high-speed switching caches for IP routing.
Step 12	uBR924(config-if)# **cable modem compliant bridge**	Enable DOCSIS-compliant bridging.
Step 13	uBR924(config-if)# **bridge-group** *bridge-group*	Assign the cable interface to the same bridge spanning group used for the Ethernet interface.
Step 14	uBR924(config-if)# **bridge-group** *bridge-group* **spanning-disabled**	Disable the spanning tree on the cable interface.
Step 15	uBR924(config-if)# **Ctrl-Z**	Return to privileged EXEC mode.
Step 16	uBR924# **copy running-config startup-config**	Save the configuration to nonvolatile RAM.
Step 17	uBR924# **show startup-config**	Display the configuration file that was just created.

CHAPTER 3

Advanced Data-Only Configurations

This chapter describes how to configure the Cisco uBR924 cable access router for data operation with features beyond those supported in the default operation mode of "plug and play" DOCSIS bridging. The following configurations are described:

Depending on the Cisco IOS software image being used and the feature sets it supports, these configurations could be combined.

Tip Use the commands shown in this chapter to set up a typical Cisco uBR924 router for the desired feature. Then save the configuration into a configuration file that can be downloaded to the router during power-on or reset.

Caution Incorrectly configuring the Cisco uBR924 cable access router can cause loss of network connectivity. Before attempting to reconfigure the router, print the last working configuration, and ensure remote configuration is enabled for the site.

If the router does not connect to the network after you have reconfigured it, enter the cable downstream saved frequency from the printout, and then clear the interface. Power off and then power on the router.

If powering off the router does not correct the problem after a few minutes, give the **write erase** and **copy startup-config running-config** commands; then enter the correct saved downstream frequency. If network connectivity is not restored, contact your network management, provisioning, or billing system administrator to reload the software applicable to your network.

Data-Only Routing

The Cisco uBR924 router must be configured for routing mode to use advanced features such as IPSec encryption and firewall protection. The routing mode is also required if the PCs attached to the Cisco uBR924 router are on a private network or on a different subnet than the subnet used by the CMTS.

The following steps are required to configure the routing mode on the Cisco uBR924 router:

- Disable DOCSIS-compliant bridging on the cable interface with the **no cable modem compliant bridge** interface command.
- Remove the bridge group on the cable and Ethernet interfaces with the **no bridge group** interface command.
- Configure the RIPv2 routing protocol (or static routes) on the cable and Ethernet interfaces.

To configure the Cisco uBR924 router, log in to the router, enter global configuration mode, and enter the following commands:

	Command	Purpose
Step 1	uBR924(config)#**int c 0**	Enter interface configuration mode for the cable interface.
Step 2	uBR924(config-if)# **no cable-modem compliant bridge**	Disable DOCSIS-compliant bridging.
Step 3	uBR924(config-if)# **no bridge group** *number*	Remove the bridge group.
Step 4	uBR924(config-if)# **ip address dhcp**	Configure the cable interface to receive an IP address from the DHCP server.
Step 5	uBR924(config-if)# **exit**	Return to global configuration mode.
Step 6	uBR924(config)#**int e 0**	Enter interface configuration mode for Ethernet 0.
Step 7	uBR924(config-if)# **no bridge group** *number*	Remove the bridge group.
Step 8	uBR924(config-if)# **ip address** *ip-address subnet-mask*	Enter the Ethernet interface's IP address and subnet mask.
Step 9	uBR924(config-if)# **exit**	Return to global configuration mode.
Step 10	uBR924(config)# **ip routing**	Enable IP routing for the router.
Step 11	**To use RIPv2:**	
	uBR924(config)#**router rip**	Enter router configuration mode.
	uBR924(config-router)# **version 2**	Enable RIP version 2 routing.
	uBR924(config-router)# **network** *cable-network-number*	Enable routing on the cable interface's IP network.
	uBR924(config-router)# **network** *Ethernet-network-number*	Enable routing on the Ethernet interface's IP network.
	uBR924(config-router)# **exit**	Return to global configuration mode.
Step 12	uBR924(config)# **no cdp run**	(Optional) Disable the Cisco Discovery Protocol (CDP) on the router. CDP is a proprietary protocol for the discovery of Cisco routers running protocols other than TCP/IP; because DOCSIS cable data networks are primarily TCP/IP networks, CDP is not necessary on the Cisco uBR924 router.
Step 13	uBR924(config)# **ip default-gateway** *ip-address*	Set the default gateway for routing (typically, this is the CMTS).

	Command	Purpose
Step 14	uBR924(config)# **ip classless**	(Optional) Enable the forwarding of packets that are destined for unrecognized subnets to the best supernet route.
Step 15	uBR924(config)# **ip route 0.0.0.0 0.0.0.0** *ip-address*	(Optional) Establish a static route so that all packets without an established route are forwarded to the default gateway (typically the *ip-address* should be the IP address for the CMTS), regardless of any routing metrics.
Step 16	uBR924(config-if)# **Ctrl-z**	Return to privileged EXEC mode.
Step 17	uBR924# **copy running-config startup-config** Building configuration...	Save the configuration to nonvolatile memory so that it will not be lost in the event of a reset, power cycle, or power outage.
Step 18	uBR924# **show startup-config**	Display the configuration file that was just created.
Step 19	uBR924# **reload**	Resets the router and cable interface to enable IP routing mode.

To verify that routing is enabled, enter the **show startup-config** command. The following example shows a sample configuration file for basic data-only routing mode; the relevant commands are shown in bold.

```
version 12.1
service config
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Router
!
clock timezone - 4
ip subnet-zero
!
voice-port 0
!
voice-port 1
!
interface Ethernet0
 ip address 172.16.0.1 255.255.0.0
 no ip directed-broadcast
 ip rip send version 2
 ip rip receive version 2
!
interface cable-modem0
 ip address dhcp
 no ip directed-broadcast
 ip rip send version 2
 ip rip receive version 2
 no cable-modem compliant bridge
!
 router rip
 version 2
 network 10.0.0.0
 network 172.16.0.0
!
ip classless
no ip http server
```

```
no service finger
!
!
line con 0
 transport input none
line vty 0 4
!
end
```

Note The above configuration assumes that the DHCP server assigns an IP address to the cable interface that is in the class A private network (10.0.0.0).

Routing with DHCP Server

When in routing mode, the Cisco uBR924 router can act as a DHCP server for the CPE devices it is connecting to the cable network. A service provider then does not have to be concerned about providing IP addresses to all of the PCs at a subscriber's site; instead, the provider supplies a pool of IP addresses that the Cisco uBR924 router then allocates to the PCs as needed.

Note The Cisco uBR924 router must be configured for routing mode to act as a DHCP server. If in bridging mode, you can configure the router to proxy DHCP client requests to the DHCP server at the headend by giving the **cable helper-address** *dhcp-server-ip-address* **host** interface configuration command. (The **ip helper-address** and **ip forward-protocol** interface configuration commands can also be used for this purpose.)

To configure the Cisco uBR924 router to act as a DHCP server, log in to the router, enter global configuration mode, and enter the following commands:

	Command	Purpose
Step 1	uBR924(config)# **ip dhcp pool** *pool-name*	Create an address pool for the DHCP server named *pool-name* and enter DHCP configuration mode.
Step 2	uBR924(config-dhcp)# **network** *IP-network-number subnet-mask*	Specify the network number and subnet mask for the IP address pool. These IP addresses should be part of the subnet provided by the CMTS cable interface. For example, **network 10.17.91.0 255.255.255.0** reserves the IP addresses 10.17.91.1–10.17.91.254 for CPE devices.
Step 3	uBR924(config-dhcp)# **domain-name** *domain-name*	The domain name that should be assigned to CPE devices (for example, **cisco.com**).
Step 4	uBR924(config-dhcp)# **dns-server** *ip-address*	The IP address for the DNS server provided by the service provider that will service the DNS requests from the CPE devices. More than one DNS server can be specified.
Step 5	uBR924(config-dhcp)# **default-router** *ip-address*	The IP address for the default router for the CPE devices (typically, this is the CMTS). More than one default router can be specified.
Step 6	uBR924(config-dhcp)# **exit**	Return to global configuration mode.
Step 7	uBR924# **show startup-config**	Display the configuration file that was just created.

To verify that the DHCP server is enabled, enter the **show startup-config** command. A sample configuration file for a Cisco uBR924 router acting as a DHCP server is shown below. The relevant commands are shown in bold.

```
version 12.1
service config
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Router
!
clock timezone - 4
ip subnet-zero
!
ip dhcp pool Clients
 network 192.168.100.0 255.255.255.0
 domain-name cisco.com
 dns-server 192.168.100.17
 default-router 192.168.101.1
!
voice-port 0
!
voice-port 1
!
interface Ethernet0
 ip address 192.168.100.1 255.255.0.0
 no ip directed-broadcast
 ip rip send version 2
 ip rip receive version 2
!
interface cable-modem0
 ip address dhcp
 no ip directed-broadcast
 ip rip send version 2
 ip rip receive version 2
 no cable-modem compliant bridge
!
 router rip
 version 2
 network 10.0.0.0
 network 192.168.100.0
!
ip classless
no ip http server
no service finger
!
!
line con 0
 transport input none
line vty 0 4
!
end
```

Note The above configuration assumes that the DHCP server assigns an IP address to the cable interface that is in the class A private network (10.0.0.0).

NAT/PAT Configuration

When using a Cisco IOS image that supports the Easy IP feature, the Cisco uBR924 router supports Network Address Translation (NAT) and Port Address Translation (PAT). This allows a private network that is connected to the router to use the same IP address when communicating through the cable interface to the Internet or other public networks.

When NAT/PAT are enabled on the cable access router, the "inside" network is the private network connected to the router's Ethernet interface, and the "outside" network is the network accessed through the cable network (such as the Internet or a company's larger network). Each inside address is typically an IP address in the RFC1918 private network space (10.0.0.0, 172.16.0.0, and 192.168.100.0) and is translated to an external IP address that is valid in the outside network.

Note NAT/PAT can be used only in routing mode.

The following commands show a typical configuration. (These steps assume that the router has already been configured for routing mode, as described in "Data-Only Routing" section on page 3-2.)

	Command	Purpose
Step 1	uBR924(config)# **ip nat inside source list** *list-id* **interface cable-modem0 overload**	Enable translation of the inside source addresses—the "inside" addresses are translated before being presented to the "outside" network. The *list-id* specifies an access-list that defines the IP addresses that will be used, and **overload** specifies that multiple inside IP addresses can use the same outside IP address (but using different port numbers to unique identify each inside host).
Step 2	uBR924(config)# **interface Ethernet0**	Enter interface configuration mode for the router's Ethernet interface.
Step 3	uBR924(config-if)# **ip nat inside**	Specify that the Ethernet is the "inside" of the NAT/PAT translation.
Step 4	uBR924(config-if)# **exit**	Exit interface configuration mode.
Step 5	uBR924(config)# **interface cable-modem0**	Enter interface configuration mode for the router's cable interface.
Step 6	uBR924(config-if)# **ip nat outside**	Specify that the cable interface is the "outside" of the NAT/PAT translation.
Step 7	uBR924(config-if)# **exit**	Exit interface configuration mode.
Step 8	uBR924(config)# **access-list** *list-id* **permit** *address mask*	Creates the access list specified by the *list-id* parameter in the **ip nat inside source** command. The address and mask values should specify IP addresses that belong to the private IP network space being used by the Ethernet interface.
Step 9	uBR924# **copy running-config startup-config** Building configuration...	Save the configuration to nonvolatile memory so that it will not be lost in the event of a reset, power cycle, or power outage.
Step 10	uBR924# **show startup-config**	Display the configuration file that was just created.

Note Additional options, such as static IP address translation, are possible when using NAT/PAT. For more information about the Easy IP and NAT/PAT feature set, see the *Dial-Related Addressing Services* documentation, available on CCO and the Documentation CD-ROM.

The following configuration shows an example of a Cisco uBR924 router in routing mode that performs NAT/PAT translation on all IP addresses connected to the router's Ethernet interface. The external IP address is overloaded so that multiple IP addresses on the internal network can use the same external IP address over the cable interface; different port numbers are used to uniquely identify each device on the Ethernet interface. The relevant commands are shown in bold.

```
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 192.168.1.1. 255.255.255.0
 ip nat inside
!
interface cable-modem0
 ip nat outside
 no cable-modem compliant bridge
!
ip routing
ip default-gateway 10.1.1.1
ip classless
no ip http server
no service finger
ip route 0.0.0.0 0.0.0.0 10.1.1.1
!
access-list 1 permit 192.168.1.0 0.0.0.255
!
!
line con 0
line vty 0 4
 login
!
end
```

Note The above configuration assumes that the DHCP server assigns an IP address to the cable interface that is in the class C private network (192.168.100.0).

NAT/PAT Configuration with DHCP Proxy

The NAT/PAT feature can also be used with the **cable-modem dhcp-proxy nat** command, so that the router obtains the IP address used for the NAT pool for the Ethernet interface from the DHCP server. This allows the service provider to dynamically provide this IP address in the same manner as for the cable interface.

In addition to using the the **cable-modem dhcp-proxy nat** command, you must also use the following NAT configuration commands:

- Use the **ip nat inside** interface command to configure the Ethernet interface as the "inside" interface.
- Use the **ip nat outside** interface command to configure the cable interface as the "outside" interface.
- Specify the **overload** option with the **ip nat** global configuration command because the NAT pool created by the **cable-modem dhcp-proxy** command contains only one IP address.

The following commands show a typical configuration. (These steps assume that the router has already been configured for routing mode, as described in "Data-Only Routing" section on page 3-2.)

	Command	Purpose
Step 1	UBR924(config)# **ip nat inside source list** *list-id* **interface cable-modem0 overload**	Enables translation of the inside source addresses—the "inside" addresses are translated before being presented to the "outside" network. The *list-id* specifies an access-list that defines the IP addresses that will be used, and **overload** specifies that multiple inside IP addresses can use the same outside IP address (but using different port numbers to unique identify each inside host).
Step 2	UBR924(config)# **interface Ethernet0**	Enters interface configuration mode for the router's Ethernet interface.
Step 3	UBR924(config-if)# **ip nat inside**	Specifies that the Ethernet is the "inside" of the NAT/PAT translation.
Step 4	UBR924(config-if)# **exit**	Exits interface configuration mode.
Step 5	UBR924(config)# **interface cable-modem0**	Enters interface configuration mode for the router's cable interface.
Step 6	UBR924(config-if)# **cable-modem dhcp-proxy nat** *pool-name*	Specifies the name of the NAT pool to be created using the IP address and subnet mask supplied by the DHCP server. The *pool-name* can be any arbitrary string. **Note** This is equivalent to giving the **ip nat pool** command, using the IP address and subnet mask supplied by the DHCP server.
Step 7	UBR924(config-if)# **ip nat outside**	Specifies that the cable interface is the "outside" of the NAT/PAT translation.
Step 8	UBR924(config-if)# **exit**	Exits interface configuration mode.

	Command	Purpose
Step 9	UBR924(config)# **access-list** *list-id* **permit** *address mask*	Creates the access list specified by the *list-id* parameter in the **ip nat inside source** command. The address and mask values should specify IP addresses that belong to the private IP network space being used by the Ethernet interface.
Step 10	UBR924# **copy running-config startup-config**	Saves the configuration to nonvolatile memory so that it will not be lost in the event of a reset, power cycle, or power outage.
Step 11	UBR924# **show startup-config**	Displays the configuration file that was just created.

Note For more information about the Easy IP and NAT/PAT feature set, see the *Dial-Related Addressing Services* documentation, available on Cisco.com and the Documentation CD-ROM.

The following configuration for the Cisco uBR924 cable access router shows an example of a cable access router in routing mode that performs NAT/PAT translation using the DHCP proxy to obtain its NAT address pool. The relevant commands are shown in bold.

Note Do not enter the **ip nat pool** command manually. The router automatically generates this command when it obtains the NAT address pool from the DHCP server.

```
version 12.1
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Router
!
!
ip nat inside source list 1 interface cable-modem0 overload
clock timezone - -4
!
!
interface Ethernet0
 ip address 192.168.1.1 255.255.255.0
 ip nat inside
!
interface cable-modem0
 ip nat outside
 no cable-modem compliant bridge
 cable-modem dhcp-proxy nat nat-pool
!
ip routing
ip default-gateway 10.1.1.1
! The following command is automatically added when the router obtains
!  the DHCP-provided IP addresses for the NAT pool
ip nat pool nat-pool 10.15.0.10 10.15.0.10 netmask 255.255.0.0
! The following command must be manually entered
ip nat inside source list 1 pool nat-pool overload
ip classless
no ip http server
no service finger
ip route 0.0.0.0 0.0.0.0 10.1.1.1
```

```
access-list 1 permit 192.168.1.0 0.0.0.255
!
!
line con 0
line vty 0 4
 login
!
end
```

Note The above configuration assumes that the DHCP server assigns an IP address to the cable interface that is in the class C private network (192.168.0.0).

Using NAT and DHCP Proxy and Copying Configuration Files

Most service providers typically create a standard configuration file for their cable modems, verify it, and then copy the working configuration as needed to other cable modems. This can cause problems with Cisco uBR924 cable access router when using the **cable-modem dhcp-proxy** command to create a NAT address pool for NAT/PAT translation.

The reason is that the default router configuration is for DOCSIS-compliant bridging, which includes two **bridge-group 59** commands for each interface. To use the **cable-modem dhcp-proxy** command, you must put the router into routing mode, which means removing the **bridge-group** commands with the equivalent **no bridge-group** commands.

However, because **no bridge-group** is the default for these CLI commands, they are not saved in the running configuration. So when you save the Cisco IOS configuration file and copy it to other Cisco uBR924 cable access router, the router is only partially configured for routing mode and continually resets its interfaces.

In addition, whenever you use the **cable-modem dhcp-proxy** command to create a NAT pool, the router automatically adds the appropriate **ip nat pool** commands to the configuration when it receives the actual IP addresses from the DHCP server. The IP addresses specified in this command are particular to each user and should not be copied to other routers.

To avoid this problem, use the following procedure to create a Cisco IOS configuration file that uses the **cable-modem dhcp-proxy** command to create a NAT address pool for NAT/PAT address translation:

Step 1 Create and test a working configuration on a Cisco uBR924 cable access router.

Step 2 After you have created a standardized configuration, save it to memory, and then copy the Cisco IOS configuration file to the TFTP server that will be used to copy the file to the other cable access routers.

Step 3 Open the Cisco IOS configuration file with a text editor and add the following lines underneath each interface:

```
no bridge-group 59
no bridge-group 59 spanning-disabled
```

Step 4 Remove the **ip nat pool** command.

For example, the following are the relevant lines in a typical DHCP proxy NAT configuration for the Cisco uBR924 cable access router:

```
interface Ethernet0
 ip address 192.168.1.1 255.255.255.0
 ip nat inside
```

```
 load-interval 30
!
interface cable-modem0
 ip nat outside
 load-interval 30
 no cable-modem compliant bridge
 cable-modem dhcp-proxy nat nat-pool
!
ip nat pool nat-pool 10.15.0.10 10.15.0.10 netmask 255.255.0.0
```

When you copy this configuration file to the TFTP server, modify this portion of the configuration file to add the **no bridge-group** commands under each interface and to remove the **ip nat pool** command:

```
interface Ethernet0
 ip address 192.168.1.1 255.255.255.0
 ip nat inside
 load-interval 30
 no bridge-group 59
 no bridge-group 59 spanning-disabled
!
interface cable-modem0
 ip nat outside
 load-interval 30
 no cable-modem compliant bridge
 cable-modem dhcp-proxy nat nat-pool
 no bridge-group 59
 no bridge-group 59 spanning-disabled
!
```

Note Be sure to remove the **ip nat pool** command.

IPSec (56-bit) Example

IPSec encryption provides end-to-end encryption of IP traffic across unprotected public networks such as the Internet. To use IPSec, the Cisco uBR924 cable access router must meet the following prerequisites:

- The Cisco uBR924 router must be using a Cisco IOS Release 12.0(5)T or higher image that supports the IPSec feature set.
- The Cisco uBR924 router must be configured for routing mode.
- The Cisco uBR924 router and endpoint must both support IPSec encryption and be configured for the same encryption policy. (The endpoint is typically an IPSec gateway such as a peer router, PIX firewall, or other device that can be configured for IPSec.)

Note Images that support encryption are subject to United States government export controls and have limited distribution. Strong encryption images to be installed outside the United States may require an export license. Contact your sales representative or distributor for more information, or send an e-mail to export@cisco.com.

Note Cisco IOS Release 12.1(5)T, 12.2(2), or greater is required to support GRE IP tunnels.

The configuration of the Cisco uBR924 router for IPSec encryption depends on the application involved, such as whether the IPSec encryption is part of a virtual private network (VPN) and whether the Cisco uBR924 router should encrypt traffic to one or more than one peer end-point. A technique that would work well for a small network might not scale well for a large network—for example, using pre-shared authentication keys works for networks of up to 10 or so nodes, but larger networks should use RSA public key signatures and digital certificates.

Note For more information about IPSec, as well as related topics such as Internet Key Exchange (IKE), Internet Security Association Key Management Protocol/Oakley variation (ISAKMP/Oakley), and digital certificates, see the "Additional Documentation" section on page 3-15.

The following shows the commands needed to configure the Cisco uBR924 router for IPSec encryption with one peer router, using pre-shared keys.

	Command	Purpose
Step 1	uBR924(config)# **crypto isakmp enable**	Enable the use of ISAKMP/IKE on the Cisco uBR924 router.
Step 2	uBR924(config)# **crypto isakmp policy** *priority-number*	Creates an IKE policy with the specified priority-number (1–10000, where 1 is the highest priority) and enters ISAKMP policy configuration command mode.
Step 3	uBR924(config-isakmp)# **encryption des**	Specifies that 56-bit DES encryption be used. to encrypt the data.
Step 4	uBR924(config-isakmp)# **hash md5**	Specifies the MD5 (HMAC variant) hash algorithm for packet authentication.
Step 5	ubr924(config-isakmp)# **group 1**	Specifies the 768-bit Diffie-Hellman group for key negotiation.
Step 6	uBR924(config-isakmp)# **authentication pre-share**	Specifies that the authentication keys are pre-shared, as opposed to dynamically negotiated using RSA public key signatures.
Step 7	uBR924(config-isakmp)# **lifetime** *seconds*	Defines how long each security association should exist before expiring (60 seconds to 86,400 seconds).
Step 8	uBR924(config-isakmp)# **exit**	Exits ISAKMP policy configuration command mode.
Step 9	uBR924(config)# **crypto isakmp key** *shared-key* **address** *ip-address*	Specifies the pre-shared key that should be used with the peer at the specific IP address. The key can be any arbitrary alphanumeric key up to 128 characters long—the key is case-sensitive and must be entered identically on both routers. **Note** You can also specify a pre-shared key using the **crypto key public-chain dss** command. See the description of this command in the *Cisco Encryption Technology Commands* document, available on CCO and the Documentation CD-ROM.

	Command	Purpose
Step 10	uBR924(config)# **crypto isakmp identity hostname**	Sets the ISAKMP identity of the router to its host name concatenated with the domain name (for example, **ubr924.cisco.com**).
Step 11	uBR924(config)# **crypto ipsec transform-set** *transform-set-name transform1 transform2 transform3*	Establishes the transform set to be used for IPSec encryption. Up to three transformations can be specified for a set, such as **ah-md5-hmac esp-des esp-md5-hmac**.
Step 12	uBR924(config)# **crypto map** *crypto-map-name* **local-address cable-modem0**	Creates the specified crypto map and applies it to the cable interface.
Step 13	uBR924(config)# **crypto map** *crypto-map-name* **10 ipsec-isakmp**	Creates a crypto map numbered 10 and enters the crypto map configuration mode.
Step 14	uBR924(config-crypto)# **set peer** *ip-address*	Identifies the IP address for the destination peer router.
Step 15	uBR924(config-crypto)# **set transform**-set *transform-set-name*	Sets the crypto map to use the transform set created previously.
Step 16	uBR924(config-crypto)# **match address** *access-list-number*	Sets the crypto map to use the access list that will specify the type of traffic to be encrypted. **Note** Access lists 100 and 101 cannot be used because they are reserved for DOCSIS use.
Step 17	uBR924(config-crypto)# **exit**	Exits crypto map configuration mode.
Step 18	uBR924(config)# **int c 0**	Enters interface configuration mode for the cable interface.
Step 19	uBR924 (config-if)# **crypto map** *crypto-map-name*	Applies the crypto map created above to the cable interface.
Step 20	uBR924 (config-if)# **access-list** *access-list-number* **permit ip host** *ubr924-ip-address peer-ip-address filter-mask*	Creates an access list to identify the traffic that will be encrypted. (This should match the access list created above.)
Step 21	uBR924(config-if)# **Ctrl-z**	Return to privileged EXEC mode.
Step 22	uBR924# **copy running-config startup-config** Building configuration...	Save the configuration to nonvolatile memory so that it will not be lost in the event of a reset, power cycle, or power outage.
Step 23	uBR924# **show startup-config**	Display the configuration file that was just created.

Note To enable IPSec encryption, the peer router must also be configured for IPSec encryption, using the identical parameters used on the Cisco uBR924 router.

Sample Configuration

The following configuration shows a typical IPSec configuration with the following parameters:

- The IKE policy is defined as policy priority 1 with the following parameters:

  - 56-bit DES-CBC encryption (the default)
  - MD5 (HMAC variant) hash algorithm
  - Pre-shared authentication keys
  - 768-bit Diffie-Hellman group (the default)
  - Security association lifetime of 5,000 seconds (approximately 83 minutes).
- The pre-shared key has the value 1234567890 (normally keys would be much more complex than this simple example)
- IPSec encryption is being done on traffic sent from the cable interface on the Cisco uBR924 router (at IP address 10.1.0.25).
- One single peer is defined—the router at IP address 30.1.1.1.
- IPSec encryption is applied to all traffic that matches the contents of access list 200.

IPSec-related commands are shown in bold.

```
version 12.1
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
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 1234567890 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 200
!
interface Ethernet0
 ip address 192.168.100.1 255.255.255.0
 no ip directed-broadcast
!
interface cable-modem0
 ip address dhcp
 no ip directed-broadcast
 no keepalive
 no cable-modem compliant bridge
 crypto map test-ipsec
router rip
 version 2
 network 10.0.0.0
 network 192.168.100.0
!
ip classless
no ip http server
```

```
no service finger
!
access-list 200 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
```

Note The above configuration assumes that the DHCP server assigns an IP address to the cable interface that is in the class A private network (10.0.0.0).

Additional Documentation

Establishing IPSec encryption between two or more end-points requires a thorough understanding of the Internet Key Exchange (IKE) mechanism, which is a form of the ISAKMP/Oakley (Internet Security Association Key Management Protocol) that is used for IPSec encryption. Digital certificates must also be understood if this mechanism is going to be used for authentication. Finally, if IPSec will be used as part of a virtual private network (VPN), those concepts must be understood as well.

For general information on these subjects, see the following information in the product literature and IP technical tips sections on CCO:

- *Deploying IPSec*—Provides an overview of IPSec encryption and its key concepts, along with sample configurations. Also provides a link to many other documents on related topics.
- *Certificate Authority Support for IPSec Overview*—Describes the concept of digital certificates and how they are used to authenticate IPSec users.
- *An Introduction to IP Security (IPSec) Encryption*—Provides a step-by-step description of how to configure IPSec encryption.

The following technical documents, available on CCO and the Documentation CD-ROM, also provide more in-depth configuration information:

- *Cisco IOS Release 12.1 Security Configuration Guide*—Provides an overview of Cisco IOS security features.
- *Cisco IOS Release 12.0 Security Command Reference*—Provides a reference for each of the Cisco IOS commands used to configure IPSec encryption and related security features.
- *Cisco IOS Software Release 12.1 Command Summary*—Summarizes the Cisco IOS commands used to configure all Release 12.0 security features.

Note Additional documentation on IPSec becomes available on CCO and the Documentation CD-ROM as new features and platforms are added.

IPSec (3DES) Example

The IPSec 3DES encryption feature set is identical to the IPSec encryption feature set except that it supports the 168-bit Triple DES (3DES) standard in addition to the standard 56-bit IPSec encryption. The 168-bit encryption feature set requires a Cisco IOS image that supports it and provides a level of security suitable for highly sensitive and confidential information such as financial transactions and medical records.

Note Cisco IOS images with strong encryption (including, but not limited to, 168-bit [3DES] data encryption feature sets) are subject to United States government export controls and have limited distribution. Strong encryption images to be installed outside the United States may require an export license. Customer orders may be denied or subject to delay due to United States government regulations. When applicable, the purchaser or user must obtain local import and use authorizations for all encryption strengths. Contact your sales representative or distributor for more information, or send an e-mail to export@cisco.com.

Configuration for 3DES encryption is identical to that for standard IPSec, except that the transformation set should specify **esp-3des** instead of **esp-des**. For example, the following configuration is identical to the configuration shown in "IPSec (56-bit) Example" section on page 3-11, except for the line in bold:

```
version 12.1
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
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 1234567890 address 30.1.1.1
crypto isakmp identity hostname
!
crypto ipsec transform-set test-transform ah-md5-hmac esp-3des 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 200
!
interface Ethernet0
 ip address 192.168.100.1 255.255.255.0
 no ip directed-broadcast
!
interface cable-modem0
 ip address dhcp
 no ip directed-broadcast
 no keepalive
 no cable-modem compliant bridge
 crypto map test-ipsec
router rip
```

```
 version 2
 network 10.0.0.0
 network 192.168.100.0
!
ip classless
no ip http server
no service finger
!
access-list 200 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
```

Note The above configuration assumes that the DHCP server assigns an IP address to the cable interface that is in the class A private network (10.0.0.0).

L2TP Example

When the Cisco uBR924 router is using a software image that supports the Layer 2 Tunnel Protocol (L2TP), the router can function as an L2TP network server (LNS), which is one part of a virtual private dialup network (VPDN). In this configuration, the router creates a secure connection with another router that is functioning as an L2TP access concentrator (LAC)—traffic sent between the two routers is protected from interception or modification, even when it travels across public networks such as the Internet.

Note The Cisco uBR924 cable access router does not support the L2TP feature in Cisco IOS Release 12.1(3)T and above.

Note The computer connected to the Cisco uBR924 router must be running software, such as Windows 98, that supports VPDN connections.

Configuration of a VPDN can be very complex, depending on the networks being used and how many peer devices will be establishing VPDN connections. The following table shows the minimum configuration needed for a typical VPDN configuration on a Cisco uBR924 router using the L2TP protocol (the LAC must be similarly configured).

Note Cisco IOS Release 12.1(5)T, 12.2(2), or greater is required to support GRE IP tunnels.

	Command	Purpose
Step 1	uBR924(config)# **vpdn enable**	Enable VPDN services so that the router will look for tunnel definitions.
Step 2	uBR924(config)# **vpdn-group 1**	Create a unique VPDN group (1–3000) to which VPDN attributes can be assigned, and enter VPDN configuration mode.
Step 3	uBR924(config-vpdn)# **accept dialin l2tp virtual-template 1 remote L2TP_LAC**	Configure the VPDN group to accept a incoming request using the L2TP protocol from the remote peer named L2TP_LAC.
Step 4	uBR924(config-vpdn)# **l2tp ip tos reflect**	(Optional) Preserve the type of service (TOS) bits in the original packets.
Step 5	uBR924(config-vpdn)# **exit**	Return to global configuration mode.
Step 6	uBR924(config)# **no l2tp tunnel authentication**	Disable L2TP tunnel authentication.
Step 7	uBR924(config)# **interface Virtual-Template1**	Create a virtual access interface from the virtual template and enter interface configuration mode.
Step 8	uBR924(config-if)# **ip unnumbered Ethernet0**	Enable IP traffic on the virtual access interface without requiring a specific IP address for the interface.
Step 9	uBR924(config-if)# **no ip directed-broadcast**	Disable the forwarding of directed broadcasts on this interface to prevent some common hacker attacks.
Step 10	uBR924(config-if)# **peer default ip address pool dialup**	Obtain an IP address from the default dialup IP address pool.
Step 11	uBR924(config-if)# **ppp authentication chap**	Enables the Challenge Handshake Authentication Protocol (CHAP) on the interface to allow verification of the remote end.
Step 12	uBR924(config-if)# **Ctrl-z**	Return to privileged EXEC mode.
Step 13	uBR924# **copy running-config startup-config** Building configuration...	Save the configuration to nonvolatile memory so that it will not be lost in the event of a reset, power cycle, or power outage.
Step 14	uBR924# **show startup-config**	Display the configuration file that was just created.

Note For more details on the L2TP feature, see the *Layer 2 Tunnel Protocol* and *L2TP Dialout* feature modules, available on CCO and the Documentation CD-ROM.

The following sections show sample configurations for the Cisco uBR924 router acting as the LNS. The relevant commands are in bold.

```
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 192.168.100.1 255.255.255.0
 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 dhcp
 no ip directed-broadcast
no cable-modem compliant bridge
!
router rip
 version 2
 network 10.0.0.0
 network 192.168.100.0
!
ip local pool dialup 192.168.100.100
ip classless
no ip http server
no service finger
!
line con 0
 transport input none
line vty 0 4
 login
!
end
```

Note The above configuration assumes that the DHCP server assigns an IP address to the cable interface that is in the class A private network (10.0.0.0).

CHAPTER 4

Voice over IP Configurations

This chapter provides an overview of Voice over IP (VoIP) operations on the Cisco uBR924 cable access router. It also describes how to configure the Cisco uBR924 router for basic VoIP operation in both bridging and routing modes. This chapter contains the following sections:

Note The configurations shown in this chapter can be combined with most of the data-only configurations shown in Chapter 3, "Advanced Data-Only Configurations." All voice configurations assume that the CMTS and associated servers, gateways, and gatekeepers have been configured accordingly.

Overview

When using a Cisco IOS image that contains voice support, the Cisco uBR924 cable access router supports Voice over IP (VoIP), which transmits voice and fax calls over a TCP/IP network such as the Internet. Depending on the services purchased from the cable service provider, subscribers can place and receive calls without using the local telco exchange carrier.

The Cisco uBR924 router has two voice ports that support two simultaneous voice and fax calls from each subscriber site, but multiple telephones and fax devices can be connected to each of the two VoIP telephone lines (provided that the 5 REN limit for each telephone line is not exceeded). Telephones at each subscriber site must support touch-tone dialing; rotary dialing is not supported. Special telephone features such as call waiting, forwarding, and conferencing are supported only when using Cisco IOS images that support those features.

Note Fax devices—standard Group III and computer-based Group III machines up to 14,400 baud—are supported in Cisco IOS Release 12.0(5)T and higher images that support VoIP. However, in general, fax/modem cards are not supported over VoIP links. You must be using a Cisco IOS image that supports voice and have purchased the appropriate feature license before being able to make voice calls using the Cisco uBR924 router.

Introduction

The Cisco uBR924 router uses packets to transmit and receive digitized voice over an IP network. Voice traffic is supported in both the DOCSIS-bridging and routing modes.

Note When the router is acting in DOCSIS-bridging mode, a voice call originating from the router's Ethernet interface cannot terminate on another device attached to that same Ethernet interface; it must terminate on a device that is reached through the cable interface. The router must be operating in routing mode to allow calls to both originate and terminate on the Ethernet interface.

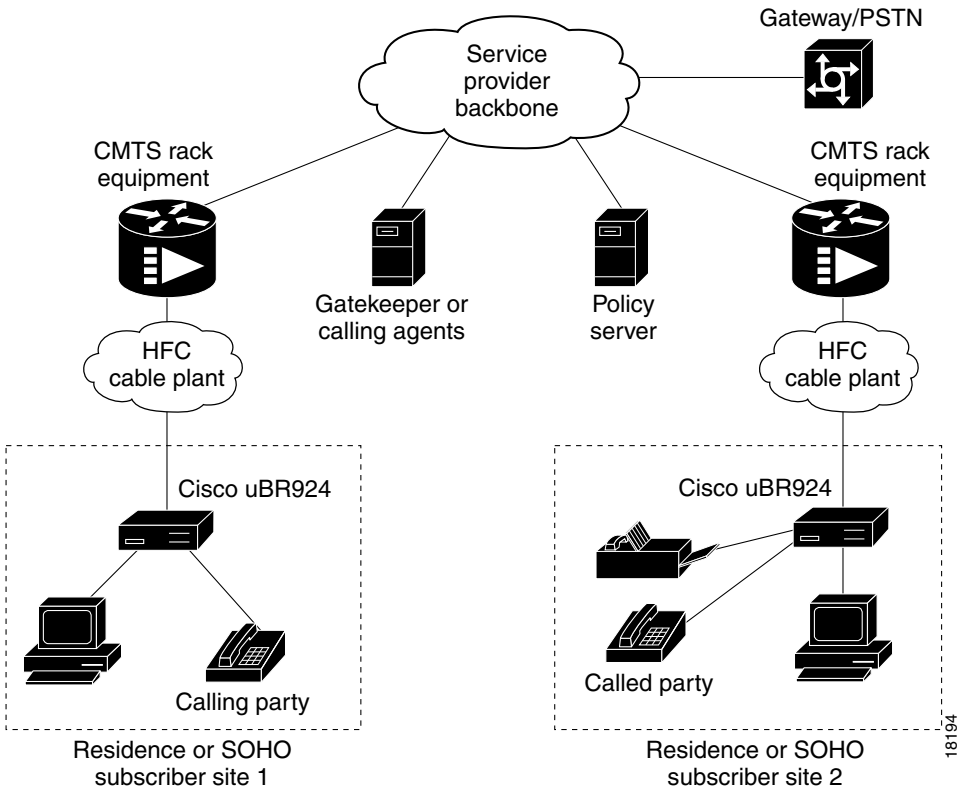
Voice signals are packetized and transported in compliance with the following protocols:

- H.323v2—Second version of an International Telecommunications Union (ITU) standard that specifies call signaling and control protocols for an IP data network. Supported on Cisco IOS Release 12.0(4)XI and higher voice images.
- Simple Gateway Control Protocol (SGCP) Version 1.1—A signaling protocol under review by the Internet Engineering Task Force (IETF). Supported on Cisco IOS Release 12.0(7)T and higher voice images.
- Media Gateway Control Protocol (MGCP) Version 0.1—A proposed IETF voice control protocol intended to eventually supersede the existing SCGP 1.1 protocol. Supported on Cisco IOS Release 12.1(3)T and higher voice images.

Note In Cisco IOS Release 12.1(3)T, the MGCP 0.1 and SGCP 1.1 protocols have been merged on the Cisco uBR924 router so that the router can respond efficiently to either protocol. The MGCP and SGCP protocols cannot be used if the H.323v2 protocol is used.

Figure 4-1 illustrates a broadband cable system that supports VoIP transmission.

Figure 4-1 Simplified VoIP Network



The CMTS at the headend routes IP telephony calls from the point of origination to the destination, transmitting them along with other traffic (both voice and data). To route voice calls across the local IP network to a destination on the Internet or the public switched telephone network (PSTN), the Cisco uBR924 router and CMTS deploy IP telephony as a local-loop bypass service. One of the following routing methods is then used, depending on the protocol being used:

- If using H.323v2, the Cisco uBR924 acts as the H.323v2 gateway that forwards the voice packets to the CMTS, which then sends them to a telephony gatekeeper. The gatekeeper transmits the packets to their ultimate destination.
- If using SGCP or MGCP, the Cisco uBR924 router acts as the residential gateway that forwards the voice packets to the CMTS, which then connects to the external call agent (SGCP or MGCP) or media gateway controller (MGCP). The call agent or controller determines how to transmit the call across the network to the trunking gateway that will be its ultimate destination.

The gateway at the destination typically interconnects the IP network to the public switched telephone network (PSTN) so that calls can be made to any phone, not just those that are part of the IP telephony network.

Voice calls are digitized, encoded, compressed, and packetized in an originating gateway; and then, decompressed, decoded, and reassembled in the destination gateway. A server maintains subscriber profiles and policy information. See the Cisco service provider voice documentation set if you have Cisco gatekeeper, gateway, or other applicable products.

Caution In certain countries, the provisioning of voice telephony over the Internet or use of these products may be prohibited and/or subject to laws, regulations or licenses, including requirements applicable to the use of the products under telecommunications and other laws and regulations; customer must comply with all such applicable laws in the country where the customer intends to use the product.

Voice Handling

With IP telephony, telephone calls can be delivered at rates as low as 8 kbps in a packet format using compression algorithms. Depending on the software release used, the Cisco uBR924 cable access router supports the following algorithms:

- G.711 A-Law—64000 bps PCM uncompressed encoding, using the A-Law standard used in most of the world except for North America and a few other countries.
- G.711 Mu-Law—64000 bps PCM uncompressed encoding, using the Mu-Law standard used in North America and a few other countries.
- G.729—8000 bps compressed CS-ACELP encoding (default for telephone calls).

Caution Because voice 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 are used. Digital Signal Processors (DSPs) provide the stream-to-packet and packet-to-stream conversion, as well as voice processing capabilities. Typical voice processing services include echo cancellation, voice compression, Voice Activity Detection (VAD) or silence compression, and Dual Tone Multi-Frequency (DTMF) tone detection and generation.

Quality of Service Support

Data traffic typically is sent only on a “best effort” basis, and if a packet is lost or delayed, it can be easily retransmitted without significantly affecting the connection. Such delays and losses are unacceptable, however, for real-time traffic such as voice calls.

For this reason, the CMTS and Cisco uBR924 router assign separate service identifiers (SIDs) for the voice and data traffic flows. Each SID has a separate class of service (CoS) that determines how its traffic flow is handled, allowing voice traffic to have a higher priority than the data traffic.

The CMTS and router can use different traffic shaping mechanisms to ensure that the higher priority voice traffic always has the bandwidth it needs. This allows voice calls (and other real-time traffic) to share the same channel as data traffic, without the quality of the voice calls being degraded by bursty data transmissions.

Note Separate CoS flows are available only when the router is connected to a CMTS that supports multiple classes of service per router. In addition, the router’s configuration file must enable multiple classes of service.

The DOCSIS 1.0 specification does not support multiple CoS flows, so this flow technique is not

available when the Cisco uBR924 router interoperates with a DOCSIS 1.0 CMTS. In this situation, voice and data traffic are both transmitted on a "best effort" basis. This may cause poorer voice quality and lower data throughput when calls are being made from the router's telephone ports.

The Cisco uBR924 router supports the following service classes:

- The first CoS in the router's configuration file is configured as the "Tiered Best Effort Type Class" and is the default CoS for data traffic. The class has no minimum upstream rate specified for the channel.

  This service class is assigned to the primary SID for the router. In addition to being used for data traffic, the router uses this SID for all MAC message exchanges with the CMTS, as well as for SNMP management traffic.

  All traffic using this SID is transmitted on a "best effort" basis, but data traffic within this class can be prioritized into eight different priority levels; although all data traffic still has lower priority than the voice traffic, this allows certain data traffic (such as MAC messages) to be given higher priority than other data traffic. The CMTS system administrator defines the traffic priority levels and must include the traffic priority fields in the configuration file downloaded to the Cisco uBR924.

- The second and third CoS are for the first and second voice ports, respectively, which are assigned to the secondary SIDs used for the voice ports. If using a Cisco IOS image that supports dynamic multi-SID assignment, these secondary SIDs are automatically created when a call is placed from one of the voice ports; when the call terminates, the secondary SID associated with it is deleted. If the Cisco IOS image does not support multi-SIDs, static SIDs are created for each of the voice ports during the power-on provisioning process, permanently reserving the bandwidth needed for the voice traffic.

  The CMTS system administrator typically configures these secondary classes of service so that they have higher QoS classes for use by higher priority voice traffic. These classes should also have a minimum upstream data rate specified for the channel to guarantee a specific amount of bandwidth for the corresponding traffic flows. When static SIDs are used, that bandwidth is always reserved for voice calls; however, when dynamic multi-SID assignment is used, that bandwidth is reserved only when the voice calls are active.

H.323v2 Protocol

In architectures using the VoIP H.323v2 protocol stack, the session application manages two call legs for each call: a telephony leg managed by the voice telephony service provider and the VoIP leg managed by the cable system operator—the VoIP service provider. Use of the H.323v2 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 setup, the session application creates a conference between them. The opposite leg's transmit routine for voice packets is given to each provider. The CMTS router passes data to the gateway and gatekeeper. The H.323v2 protocol stack provides signaling via H.225 and feature negotiation via H.245.

Note For more information on using H.323v2, see the document *H.323 Version 2 Support*, available on CCO and the Documentation CD-ROM.

To make and receive H.323 calls, the Cisco uBR924 router must be configured for the following:

- The IP address of the gateway for the destination dialed—In Cisco uBR924 IOS Release 12.0(4)XI or higher interim builds, configure these IP addresses statically via the command-line interface (CLI) using **voip dial peer group** commands. When running Cisco IOS Release 12.0(5)T or higher interim images on Cisco gatekeeper products, the router obtains these addresses dynamically from the gatekeeper using the Registration, Admission, and Status (RAS) protocol.
- The telephone numbers of the attached devices—In Cisco IOS Release 12.0(4)XI or higher interim builds, you configure these IP addresses statically via the CLI **pots port** commands. When using Cisco Network Registrar (CNR) version 3.0 or higher with the **relay.tcl** and **setrouter.tcl** scripts, and Cisco gatekeeper products in your network running Cisco IOS Release 12.0(5)T or higher images, 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.323v2 RAS gateway support.

Note To support voice configurations involving Cisco gatekeeper products using RAS, Cisco IOS Release 12.0(5)T or higher images with gatekeeper support are required. 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 and MGCP Protocol Stack

When using a Cisco IOS Release 12.0(5)T or higher image with voice support, the Cisco uBR924 router supports the Simple Gateway Control Protocol (SGCP). When using a Cisco IOS Release 12.1(3)T or higher image with voice support, the Cisco uBR924 router also supports the MGCP protocol, which is intended to eventually supersede the SGCP protocol. Both MGCP and SGCP are signaling protocols that interact with a remote call agent (CA) to provide call setup and teardown for VoIP calls.

Using the call agent, SGCP and MGCP communicate with the voice gateways, dynamically resolving and routing calls. This creates a distributed system that enhances performance, reliability, and scalability while still appearing as a single VoIP gateway to external clients.

The remote call agent also provides the signaling and feature negotiation that would otherwise be provided by the Cisco uBR924 router when using the H.323v2 protocol. Similarly, the call agent also provides the mapping of IP addresses to telephone numbers, eliminating the dial plan mapper and static configurations that are required on the router when using the H.323v2 protocol.

The SGCP and MGCP protocols implement the gateway functionality using both trunk and residential gateways. The Cisco uBR924 router functions in this mode as a residential gateway with two endpoints.

SGCP and MGCP can preserve Signaling System 7 (SS7) style call control information as well as additional network information such as routing information and authentication, authorization, and accounting (AAA) security information. SGCP and MGCP allow voice calls to originate and terminate on the Internet, as well as allowing one end to terminate on the Internet and the other to terminate on a telephone on the PSTN.

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

H.323v2 Static Bridging Configuration

When the Cisco uBR924 router is running in DOCSIS-bridging mode and using a Cisco IOS image with voice support, it can route voice calls using an H.323v2 static dialing map. This requires the following minimum configuration:

- Create a local dial peer for each voice port that will receive incoming calls. This requires configuring each voice port on the router with the phone numbers for the devices attached to those voice ports. The Cisco uBR924 router uses these numbers to determine which voice port should receive the call. Typically, the complete phone number or extension is specified for each port; when the Cisco uBR924 router receives an incoming call, all digits in the number are matched and stripped off, and the voice port is connected to the call.

Note The voice ports on the Cisco uBR924 router support only FXS devices.

- Configure a remote dial peer for each possible destination for outgoing calls. This requires specifying the phone number(s) for the destination devices. Use the following guidelines for what numbers to enter:
  - For a single telephony device, such as a one-line phone or fax machine, enter the complete phone number or extension.
  - To direct a group of numbers to a specific destination—such as the extensions used on a remote PBX—enter a pattern matching the prefix used for those lines; asterisks can be used to match any number of digits and a period matches a single digit. For example, "**572***" matches any phone numbers starting with 572 while "**572.**" matches the numbers 5720–5729.

  You must also specify the IP address for the destination host that will deliver the call to the telephony device (or if the destination device is an IP telephone, the IP address for that telephone). You can optionally specify an IP precedence level for the type of service (ToS) bits in the IP header to signify that these voice packets should be given higher priority in transit across the IP network.

  If not being done by the CoS, you can also specify which coding/decoding (CODEC) algorithm should be used.

These functions are done using the **dial-peer** command, as shown in the following table:

	Command	Purpose
Step 1	**To configure incoming calls on voice port V1:** uBR924(config)# **dial-peer voice** *id-number* **pots**	Specify a unique *id-number* for this incoming dial-peer and enter dial-peer configuration mode.
Step 2	uBR924(config-dial-peer)# **destination-pattern** *digits*	Specify the telephone number(s) associated with this voice port.
Step 3	uBR924(config-dial-peer)# **port 0**	Specify that voice port V1 is attached to this telephony equipment.
Step 4	uBR924(config-dial-peer)# **dtmf-relay** [**cisco-rtp**] [**h245-signal**] [**h245-alphanumeric**]	Optionally configure the dial peer to support out of band signaling of DTMF tones.
Step 5	uBR924(config-dial-peer)# **exit**	Exit dial-peer configuration mode.
Step 6	**To configure incoming calls on voice port V2:** uBR924(config)# **dial-peer voice** *id-number* **pots**	Specify a unique *id-number* for this incoming dial-peer and enter dial-peer configuration mode.
Step 7	uBR924(config-dial-peer)# **destination-pattern** *digits*	Specify the telephone number(s) associated with this voice port.

	Command	Purpose
Step 8	uBR924(config-dial-peer)# **port 1**	Specify that voice port V2 is attached to this telephony equipment.
Step 9	uBR924(config-dial-peer)# **dtmf-relay** [**cisco-rtp**] [**h245-signal**] [**h245-alphanumeric**]	Optionally configure the dial peer to support out of band signaling of DTMF tones.
Step 10	uBR924(config-dial-peer)# **exit**	Exit dial-peer configuration mode.
Step 11	**Repeat for each possible outgoing destination:** uBR924(config)# **dial-peer voice** *id-number* **voip**	Specify a unique *id-number* for this outgoing dial-peer and enter dial-peer configuration mode.
Step 12	uBR924(config-dial-peer)# **destination-pattern** *digits*	Specify the telephone number(s) associated with this dial-peer.
Step 13	uBR924(config-dial-peer)# **session target** [**ipv4:***ipaddress* | **dns:***hostname*]	Specify the destination IP address or hostname for this dial-peer. This could be the IP address or hostname for either an IP telephone or another router or host providing voice services.
Step 14	uBR924(config-dial-peer)# **ip precedence** *number*	(Optional) Specify an IP packet precedence level (1-5) for packets carrying calls to this dial peer (1–5, where 5 is the highest precedence for normal IP flows).
Step 15	uBR924(config-dial-peer)# **code** [**g711alaw** | **g711ulaw** | **g729r8**]	(Optional) Specify the codec algorithm to be used for these calls. The default is g711r8 (8Kbps compression; A-Law and Mu-Law are 64Kbps compression).
Step 16	uBR924(config-dial-peer)# **dtmf-relay** [**cisco-rtp**] [**h245-signal**] [**h245-alphanumeric**]	Optionally configure the dial peer to support out of band signaling of DTMF tones.
Step 17	uBR924(config-dial-peer)# **exit**	Exit dial-peer configuration mode.
Step 18	uBR924# **copy running-config startup-config** Building configuration...	Save the configuration to nonvolatile memory so that it will not be lost in the event of a reset, power cycle, or power outage.
Step 19	uBR924# **show startup-config**	Display the configuration file that was just created.

Note The ID numbers assigned using the **dial-peer voice** command must be unique but they are local to the Cisco uBR924 router. These numbers are used only when configuring each particular dial peer and have no meaning when dialing numbers or routing calls.

The following example shows a Cisco uBR924 router set up to support bridging and a static H.323 dial map with the following characteristics:

- Voice port V1 is connected to a telephony device that receives calls for the number 4123.
- Voice port V2 is connected to a telephony device that receives calls for the number 4124.
- Outgoing calls to the numbers 6000—6999 are routed to the dial peer at IP address 10.1.71.65.
- Outgoing calls to the numbers 7000—7999 are routed to the dial peer at IP address 10.1.71.75. These calls are sent with an IP ToS precedence of “5” and using the G.711 Mu-law codec algorithm.

The commands that set up the H.323v2 dial map are shown in bold:

```
version 12.1
no service pad
```

```
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname ubr924
!
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 4123
 port 0
!
dial-peer voice 2 pots
 destination-pattern 4124
 port 1
!
dial-peer voice 1001 voip
 destination-pattern 6...
 session target ipv4:10.1.71.65
 dtmf-relay cisco-rtp h245-signal h245-alphanumeric
!
dial-peer voice 1002 voip
 destination-pattern 7...
 ip precedence 5
 codec g711ulaw
 session target ipv4:10.1.71.75
 dtmf-relay cisco-rtp h245-signal h245-alphanumeric
!
!
interface Ethernet0
 no ip directed-broadcast
 no ip route-cache
 bridge-group 59
 bridge-group 59 spanning-disabled
!
interface cable-modem0
 ip address dhcp
 no ip directed-broadcast
 no ip route-cache
 cable-modem downstream saved channel 537000000 26
 bridge-group 59
 bridge-group 59 spanning-disabled
!
!
ip classless
no ip http server
no service finger
!
!
line con 0
 exec-timeout 0 0
 transport input none
line vty 0 4
 login
end
```

H.323v2 Static Routing Configuration

When the Cisco uBR924 router is operating in routing mode, the configuration of an H.323v2 static dial map uses the same commands as those given in the "H.323v2 Static Bridging Configuration" section on page 4-7. The only difference is that calls can terminate and originate on the Ethernet interface, which is not possible in DOCSIS-bridging mode.

The following sample configuration shows a Cisco uBR924 router set up for a static H.323v2 dial map with the following characteristics:

- Local dial peer 1 specifies that voice port V1 is connected to a telephone or fax machine with the number 6101.
- Local dial peer 2 specifies that voice port V2 is connected to a telephone or fax machine with the number 6102.
- Remote dial peer 101 specifies that calls to numbers 6200–6299 should be routed to IP address 10.1.71.62.
- Remote dial peers 102 and 103 specify that calls to numbers 6101 and 6102 should be routed to IP address 24.1.61.5, which is the IP address for the Cisco uBR924 router's Ethernet interface. This allows the router to complete calls between voice ports V1 and V2.

The commands related to the dial map are in bold.

```
version 12.1
no service pad
service timestamps debug uptime
service timestamps log uptime
!
hostname ubr924
!
!
!
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 62..
 session target ipv4:10.1.71.62
 dtmf-relay cisco-rtp
!
dial-peer voice 102 voip
```

```
 destination-pattern 6101
 session target ipv4:24.1.61.5
!
dial-peer voice 103 voip
 destination-pattern 6102
 session target ipv4:24.1.61.5
 dtmf-relay cisco-rtp
!
!
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 dhcp
 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
!
no ip classless
ip route 0.0.0.0 0.0.0.0 10.1.71.1
no ip http server
no service finger
!
!
line con 0
 exec-timeout 0 0
 transport input none
line vty 0 4
 login
!
!
end
```

Note The above configuration assumes that the DHCP server assigns an IP address to the cable interface that is in the class A private network (10.0.0.0).

H.323v2 Dynamic Mapping Configuration

When using a Cisco IOS image that supports voice, the Cisco uBR924 router supports using the Registration, Admission, and Status (RAS) protocol to allow a remote gatekeeper to translate phone numbers (E.164 addresses) to the IP addresses of specific dial peers. This allows the gatekeeper to maintain a central database of dial peers, so that this information does not have to be entered into static dial maps on every router that is acting as a voice gateway.

Note The Cisco uBR924 router can use H.323v2 dynamic mapping in either DOCSIS-bridging mode or routing mode.

The example shown in this section assumes that Cisco Network Registrar (CNR) version 3.0 or higher is being used as the DHCP server. CNR assigns the E.164 addresses to local voice ports and uses DHCP to define the E.164 addresses-to-port assignments.

The gatekeeper can be a Cisco router, such as the Cisco 3620, with a Cisco IOS image that supports the gatekeeper function. The Cisco uBR924 router acts as the H.323v2 gateway and creates the dial peers, starts H.323 RAS gateway support, and registers the E.164 addresses with the gatekeeper. The gatekeeper resolves the remote peers' IP addresses when the router sends a request using RAS.

Note Support for RAS and H.323v2 in Cisco gatekeeper products is found in Cisco IOS Release 12.0(5)T or higher. Support for multiple classes of service when using Cisco uBR7200 CMTS equipment is found in Cisco 12.0(4)XI or higher.

If you are not using CNR or Cisco gatekeeper products running Cisco IOS Release 12.0(5)T software, use a static dial-map as shown in the previous H.323 configurations ("H.323v2 Static Bridging Configuration" and "H.323v2 Static Routing Configuration").

You must do the following to configure the Cisco uBR924 router for dynamic mapping:

- Configure the local dial-peers—This is done in the same way as for a static H.323v2 dial map.
- Configure the remote dial-peers—This is done in the same way as for a static H.323v2 dial map, except that instead of specifying a target IP address or host name, you specify **ras** as the target.
- Enable the VoIP gateway function using the **gateway** global configuration command.
- Configure the cable modem interface to be the gateway interface.

These functions are done using the commands shown in the following table:

	Command	Purpose
Step 1	**To configure incoming calls on voice port V1:** uBR924(config)# **dial-peer voice** *id-number* **pots**	Specify a unique *id-number* for this incoming dial-peer and enter dial-peer configuration mode.
Step 2	uBR924(config-dial-peer)# **destination-pattern** *digits*	Specify the telephone number(s) associated with this voice port.
Step 3	uBR924(config-dial-peer)# **port 0**	Specify that voice port V1 is attached to this telephony equipment.
Step 4	uBR924(config-dial-peer)# **dtmf-relay** [**cisco-rtp**] [**h245-signal**] [**h245-alphanumeric**]	Optionally configure the dial peer to support out of band signaling of DTMF tones.
Step 5	uBR924(config-dial-peer)# **exit**	Exit dial-peer configuration mode.
Step 6	**To configure incoming calls on voice port V2:** uBR924(config)# **dial-peer voice** *id-number* **pots**	Specify a unique *id-number* for this incoming dial-peer and enter dial-peer configuration mode.
Step 7	uBR924(config-dial-peer)# **destination-pattern** *digits*	Specify the telephone number(s) associated with this voice port.
Step 8	uBR924(config-dial-peer)# **port 1**	Specify that voice port V2 is attached to this telephony equipment.
Step 9	uBR924(config-dial-peer)# **dtmf-relay** [**cisco-rtp**] [**h245-signal**] [**h245-alphanumeric**]	Optionally configure the dial peer to support out of band signaling of DTMF tones.
Step 10	uBR924(config-dial-peer)# **exit**	Exit dial-peer configuration mode.

	Command	Purpose
Step 11	**Repeat for each possible outgoing destination:** uBR924(config)# **dial-peer voice** *id-number* **voip**	Specify a unique *id-number* for this outgoing dial-peer and enter dial-peer configuration mode.
Step 12	uBR924(config-dial-peer)# **destination-pattern** *digits*	Specify the telephone number(s) associated with this dial-peer.
Step 13	uBR924(config-dial-peer)# **session target ras**	Specify that RAS will be used to resolve the destination for the dial-peer.
Step 14	uBR924(config-dial-peer)# **dtmf-relay** [**cisco-rtp**] [**h245-signal**] [**h245-alphanumeric**]	Optionally configure the dial peer to support out of band signaling of DTMF tones.
Step 15	uBR924(config-dial-peer)# **exit**	Exit dial-peer configuration mode.
Step 16	uBR924(config)# **gateway**	Enable the VoIP gateway on the Cisco uBR924 router.
Step 17	uBR924(config)# **interface cable-modem 0**	Enter interface configuration mode for the cable interface.
Step 18	uBR924(config-if)# (enter appropriate cable interface configuration commands)	Enter whatever commands are needed to configure the cable interface such as IP address, downstream channel, whether DOCSIS-bridging is enabled, and so forth.
Step 19	uBR924(config-if)# **h323-gateway voip interface**	Specify that the cable interface is the H.323 Gateway VoIP interface.
Step 20	uBR924(config-if)# **h323-gateway voip id** *gatekeeper-id* **ipaddr** *IP-address port-number*	Identify the RAS gatekeeper by specifying its gatekeeper ID (which must match the ID configured on the gatekeeper), its IP address, and the port number which services gateway requests.
Step 21	uBR924(config-if)# **h323-gateway voip h323-id** *interface-id*	Specify the H.323 ID for this interface. This ID is any string that uniquely identifies this gateway to the gatekeeper. Typically, this is the gateway's name and domain (such as "**ubr924@cisco.com**").
Step 22	uBR924(config-if)# **h323-gateway voip tech-prefix** *prefix*	(Optional) Specify a technology prefix to identify the type of service this gateway can provide. If more than one service is being provided, give this command for each separate technology prefix. (The prefix is defined at the gatekeeper and can up to 11 characters long, with the pound sign (#) as the last character.)
Step 23	uBR924(config-if)# **exit**	Exit interface configuration mode.
Step 24	uBR924# **copy running-config startup-config** Building configuration...	Save the configuration to nonvolatile memory so that it will not be lost in the event of a reset, power cycle, or power outage.
Step 25	uBR924# **show startup-config**	Display the configuration file that was just created.

Note For additional information on the gateway configuration commands, see the document *Configuring H.323 VoIP Gateway for Cisco Access Platforms*, available on CCO and the Document CD-ROM.

The following configuration shows a Cisco uBR924 router configured for routing mode and using RAS dynamic mapping with the following characteristics:

- The router's V1 voice port is connected to a telephone or fax machine with the number 1000, and the V2 voice port is connected to a telephone or fax machine with the number 1001.
- Four remote dial-peers are configured, with the numbers 1000, 1001, 2000, and 2001. All use the G.711 Mu-Law CODEC and the RAS protocol is used to resolve their number-address mapping. (The local dial-peer numbers, 1000 and 1001 are included as remote dial-peers to allow the router to forward calls between the two local dial-peers, as well as between local and remote dial-peers; the router must be in routing mode to support this.)
- The cable interface is configured as the gatekeeper interface, using the gatekeeper named **gatekeeper3620** at the IP address **10.1.70.50** and at port **1719**. The router identifies itself as the gateway named **uBR924** with a tech-prefix of **1#**.

The commands related to the dial mapping are in bold.

```
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 host-routing
!
voice-port 0
!
voice-port 1
!
dial-peer voice 1 pots
 destination-pattern 1000
 port 0
!
 dial-peer voice 2 pots
 destination-pattern 1001
 port 1
!
dial-peer voice 10 voip
 destination-pattern 1001
 codec g711ulaw
 session target ras
!
dial-peer voice 20 voip
 destination-pattern 1000
 codec g711ulaw
 session target ras
!
dial-peer voice 30 voip
 destination-pattern 2000
 codec g711ulaw
 session target ras
!
dial-peer voice 40 voip
 destination-pattern 2001
 codec g711ulaw
session target ras
!
gateway
```

```
!
!
interface Ethernet0
 ip address 24.1.0.1 255.255.0.0
 no ip directed-broadcast
 no ip mroute-cache
!
interface cable-modem0
 ip address dhcp
 no ip directed-broadcast
 no ip mroute-cache
 no keepalive
 cable-modem downstream saved channel 477000000 56
 no cable-modem compliant bridge
 h323-gateway voip interface
 h323-gateway voip id gatekeeper3620 ipaddr 10.1.70.50 1719
 h323-gateway voip h323-id uBR924
 h323-gateway voip tech-prefix 1#
!
router rip
 version 2
 network 10.0.0.0
 network 24.0.0.0
!
ip classless
no ip http server
no service finger
!
!
line con 0
 transport input none
line vty 0 4
!
end
```

Note The above configuration assumes that the DHCP server assigns an IP address to the cable interface that is in the class A private network (10.0.0.0).

SGCP Configuration

When using Cisco IOS Release 12.0(7)T or higher and a software image that supports voice, the Cisco uBR924 router can use the SGCP protocol for routing voice calls. This transfers the dial mapping to an external call agent, so that the VoIP gateways do not have to be individually configured with the dial mappings.

Note The Cisco uBR924 router can use SGCP in either DOCSIS-bridging mode or routing mode.

You must do the following to configure the Cisco uBR924 router for a dynamic mapping configuration:

- Enable SGCP operation on the Cisco uBR924 router.
- Specify the SGCP call agent's IP address.
- Configure the local dial-peers to be SCGP applications.
- Optionally enable the sending of SNMP traps for SGCP.

Note No configuration of remote dial-peers is needed when using SGCP.

These functions are done using the commands shown in the following table:

	Command	Purpose
Step 1	**To configure incoming calls on voice port V1:** uBR924(config)# **dial-peer voice** *id-number* **pots**	Specify a unique *id-number* for this incoming dial-peer and enter dial-peer configuration mode.
Step 2	uBR924(config)# **application SGCPAPP**	Specify that this dial-peer is handled as an SGCP application.
Step 3	uBR924(config-dial-peer)# **destination-pattern** *digits*	Specify the telephone number(s) associated with this voice port.
Step 4	uBR924(config-dial-peer)# **port 0**	Specify that voice port V1 is attached to this telephony equipment.
Step 5	uBR924(config-dial-peer)# **exit**	Exit dial-peer configuration mode.
Step 6	**To configure incoming calls on voice port V2:** uBR924(config)# **dial-peer voice** *id-number* **pots**	Specify a unique *id-number* for this incoming dial-peer and enter dial-peer configuration mode.
Step 7	uBR924(config)# **application SGCPAPP**	Specify that this dial-peer is handled as an SGCP application.
Step 8	uBR924(config-dial-peer)# **destination-pattern** *digits*	Specify the telephone number(s) associated with this voice port.
Step 9	uBR924(config-dial-peer)# **port 1**	Specify that voice port V2 is attached to this telephony equipment.
Step 10	uBR924(config-dial-peer)# **exit**	Exit dial-peer configuration mode.
Step 11	ubr924(config)# **sgcp**	Enable SGCP operations on the router.
Step 12	ubr924(config)# **sgcp call-agent** *ip-address* [*port*]	Specify the IP address and optional UDP port number for the SGCP call-agent. If no port number is given, the default of 2427 (the well-known SGCP port number) is used.
Step 13	uBR924(config)# **snmp-server enable traps xgcp**	(Optional) If SNMP management is used for this router, specify that SGCP and related traps be sent to the SNMP manager.
Step 14	uBR924# **copy running-config startup-config** Building configuration...	Save the configuration to nonvolatile memory so that it will not be lost in the event of a reset, power cycle, or power outage.
Step 15	uBR924# **show startup-config**	Display the configuration file that was just created.

The following configuration shows a Cisco uBR924 router configured in DOCSIS-bridging mode that uses SGCP for the routing of its voice calls. The relevant commands are shown in bold.

```
version 12.1
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname ubr924
```

```
!
!
clock timezone - 0 6
ip subnet-zero
no ip routing
ip domain-name cisco.com
ip name-server 4.0.0.32
!
sgcp
sgcp call-agent 10.186.1.36
!
xgcp snmp sgcp
!
!
voice-port 0
!
voice-port 1
!
dial-peer voice 100 pots
 application SGCPAPP
 destination-pattern 5551212
 port 0
!
dial-peer voice 101 pots
 application SGCPAPP
 destination-pattern 5551213
 port 1
!
process-max-time 200
!
interface Ethernet0
 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 dhcp
 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
no service finger
!
!
line con 0
 transport input none
line vty 0 4
 login
!
end
```

MGCP Configuration

When using Cisco IOS Release 12.1(3)T and higher software images that support voice, the Cisco uBR924 router can use the MGCP protocol for routing voice calls. This transfers the dial mapping to an external call agent or to a Media Gateway Controller, so that the VoIP gateways do not have to be individually configured with the dial mappings.

Note The Cisco uBR924 router can use MGCP in either DOCSIS-bridging mode or routing mode.

You must do the following to configure the Cisco uBR924 router for MGCP routing of voice calls:

- Enable MGCP operation on the Cisco uBR924 router.
- Specify the MGCP call agent's IP address.
- Configure the local dial-peers to be MCGP applications.
- Optionally specify the MGCP packages to be supported.
- Optionally change a number of MGCP parameters.

Note No configuration of remote dial-peers is needed when using MGCP.

These functions are done using the commands shown in the following table:

	Command	Purpose
Step 1	**To configure incoming calls on voice port V1:** uBR924(config)# **dial-peer voice** *id-number* **pots**	Specify a unique *id-number* for this incoming dial-peer and enter dial-peer configuration mode.
Step 2	uBR924(config)# **application MGCPAPP**	Specify that this dial-peer is handled as an MGCP application.
Step 3	uBR924(config-dial-peer)# **port 0**	Specify that voice port V1 is attached to this telephony equipment.
Step 4	uBR924(config-dial-peer)# **exit**	Exit dial-peer configuration mode.
Step 5	**To configure incoming calls on voice port V2:** uBR924(config)# **dial-peer voice** *id-number* **pots**	Specify a unique *id-number* for this incoming dial-peer and enter dial-peer configuration mode.
Step 6	uBR924(config)# **application MGCPAPP**	Specify that this dial-peer is handled as an MGCP application.
Step 7	uBR924(config-dial-peer)# **port 1**	Specify that voice port V2 is attached to this telephony equipment.
Step 8	uBR924(config-dial-peer)# **exit**	Exit dial-peer configuration mode.
Step 9	ubr924(config)# **mgcp**	Enable MGCP operations on the router.
Step 10	ubr924(config)# **mgcp call-agent** *ip-address* [*port*] [**service-type sgcp** | **mgcp**]	Specify the IP address and optional UDP port number for the MGCP call-agent. If no port number is given, the default is 2427. The default **service-type** is **mgcp**, but **sgcp** can be specified to ignore RSIP error messages.

	Command	Purpose
Step 11	ubr924(config)# **mgcp dtmf-relay** { **codec** | **low-bit-rate** } **mode** { **cisco** | **out-of-band** }	(Optional) Enables the accurate forwarding of touchtone digits during a voice call. Use **codec** to specify the G.711 codec or **low-bit-rate** to specify the G.729 codec. Use a **mode** of **cisco** to transmit the tones with the Cisco proprietary method; if the remote gateway is not a Cisco router, use **out-of-band** instead.
Step 12	ubr924(config)# **mgcp ip-tos** { **high-reliability** | **high-throughput** | **low-cost** | **low-delay** | **precedence** *value* }	(Optional) Enable IP Type of Services (TOS) for the voice connections, and specify the value for the IP precedence bit (the default IP precedence is 3).
Step 13	ubr924(config)# **mgcp max-waiting-delay** *value*	(Optional) Specify the number of milliseconds to wait after a restart (default of 3000) before connecting with the call agent. If used, these values should be staggered among gateways to avoid having large numbers of gateways connecting with the call agent at the same time after a mass restart.
Step 14	ubr924(config)# **mgcp modem passthru** { **cisco** | **ca** }	(Optional) Enable the transmission and reception of modem and fax data. If the remote gateway is a Cisco router, specify **cisco**; otherwise, specify **ca** (default) to allow the data to pass-through the call-agent.
Step 15	ubr924(config)# **mgcp package-capability** { **line-package** | **dtmf-package** | **gm-package** | **rtp-package** }	(Optional) Specify that the Cisco uBR924 router supports a particular package capability. Give this command multiple times to enable multiple packages. Use this command before using the **mgcp default-package** command.
Step 16	ubr924(config)# **mgcp default-package** { **line-package** | **dtmf-package** | **gm-package** }	(Optional) Specify the default package type for the media gateway; defaults to **line-package**.
Step 17	ubr924(config)# **mgcp playout** { **adaptive** *init-value min-value max-value* | **fixed** *init-value* }	(Optional) Change the jitter buffer packet size in milliseconds for MGCP calls, using either an adaptive range or a fixed value. The default is **adaptive 60 4 200**.
Step 18	ubr924(config)# **mgcp request retries** *count*	(Optional) Specify the number of times a call request message is transmitted to a call agent before timing out. The default is 3 times.
Step 19	ubr924(config)# **mgcp request timeout** *timeout*	(Optional) Specify the number of milliseconds to wait for a response to a request before retransmitting or timing out the request. The default is 500 milliseconds.
Step 20	ubr924(config)# **mgcp restart-delay** *value*	(Optional) Specify the value (in seconds) used in Restart in Progress (RSIP) messages to indicate the delay before the connection is torn down. The default delay is 0 seconds.
Step 21	ubr924(config)# **mgcp vad**	(Optional) Enable Voice Activity Detection (VAD) to turn silence suppression on. The default disables VAD.

	Command	Purpose
Step 22	uBR924# **copy running-config startup-config** Building configuration...	Save the configuration to nonvolatile memory so that it will not be lost in the event of a reset, power cycle, or power outage.
Step 23	uBR924# **show startup-config**	Display the configuration file that was just created.

The following configuration shows a Cisco uBR924 router configured in DOCSIS-bridging mode that uses MGCP for controlling its voice calls. The relevant commands are shown in bold.

```
version 12.1
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname ubr924
!
!
clock timezone - 0 6
ip subnet-zero
no ip routing
ip domain-name cisco.com
ip name-server 10.0.0.32
!
 mgcp
 mgcp call-agent 10.186.1.36
 mgcp modem passthru ca
 mgcp package-capability dtmf-package
 mgcp package-capability line-package
 mgcp default-package line-package
!
xgcp snmp sgcp
!
!
voice-port 0
!
voice-port 1
!
dial-peer voice 100 pots
 application MGCPAPP
 port 0
!
dial-peer voice 101 pots
 application MGCPAPP
 port 1
!
process-max-time 200
!
interface Ethernet0
 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 dhcp
 no ip directed-broadcast
 no ip route-cache
 no ip mroute-cache
 bridge-group 59
```

```
 bridge-group 59 spanning-disabled
!
ip classless
no ip http server
no service finger
!
!
line con 0
 transport input none
line vty 0 4
 login
!
end
```

Using Cisco IOS Software

This appendix describes the basics about using the Cisco IOS software that is installed on every Cisco uBR924 cable access router. This appendix describes the following topics:

Caution Before attempting to reconfigure the Cisco uBR924 cable access router at a subscriber site, contact your provisioning or billing system administrator to ensure remote configuration is allowed. To ensure proper levels of service for all customers, service providers typically disable remote configuration of the cable modems on their system and allow only the configuration that is specified by the cable provisioning or billing system.

If remote configuration is disabled, any changes you make do not remain in effect after the Cisco uBR924 router is powered off and on. Instead, the router returns to its previous configuration. In some cases, these settings will cause the cable interface to disconnect and may be lost when the cable interface is reset.

Accessing the Router's Command-Line Interface

The Cisco uBR924 router's command-line interface (CLI) can be accessed either through a Telnet connection over a TCP/IP network or by a direct connection to the router's console port. See the following sections for more information.

Note The Cisco uBR924 router also supports accessing the CLI through the Cisco web server, but this feature is automatically disabled when the Cable Monitor is active. See Appendix B, "Using the Cable Monitor Tool" for details.

Connecting Using Telnet

If the Cisco uBR924 router has successfully booted up and is operational and online, its CLI interface can be accessed by establishing a Telnet connection. Telnet can be used from any computer or terminal that has TCP/IP connectivity with the Cisco uBR924 router—the TCP/IP connectivity can exist either through the Ethernet interface or the cable interface.

Note As a security measure, you can enter EXEC mode during a Telnet session only if an enable password has been set on the router. If an enable password has not been set, you can only display the current configuration when you log in using Telnet; to change the configuration you must log in through the router's console port.

Caution Care must be taken if you use a laptop computer to make a Telnet connection through the Cisco uBR924 router's Ethernet interface, either by connecting the laptop directly to one of the router's Ethernet ports or by connecting the laptop to a hub that is connected to one of the router's Ethernet ports. If the laptop computer will not be regularly used at the subscriber site, you should power cycle the Cisco uBR924 router after you use the CLI and save your configuration changes.

Power cycling the Cisco uBR924 router ensures the laptop computer does not remain in the router's list of allowable Customer Premises Equipment (CPE) devices at the subscriber site. Reinitialization of the cable interface clears out the bridge table and resets the counter that specifies the number of CPE devices being bridged. This is particularly important when the Cisco uBR924 router is configured to operate in a DOCSIS-compliant bridging mode.

If the headend is a Cisco uBR7200 series universal broadband router, the system administrator at the headend might have to issue the **clear cable modem host** *mac address* command to remove the laptop computer from its list of CPE devices.

This behavior is required by the DOCSIS 1.0 specification.

Connecting to the Console Port

The router's CLI is available by connecting directly to the console port on the back panel of the router. The console port is an EIA/TIA-232 serial interface configured as data communications equipment (DCE) and uses an RJ-45 connector. The port is wired the same as Cisco's other routers and uses the same console kit and cable.

The console port can be accessed by any computer or terminal with an RS-232 serial port set for 9600 baud, 8 data bits, no parity, 1 stop bit (9600 8N1). Unless the router's default configuration has been changed, your terminal software should be set to emulate an ANSI, VT100, or compatible terminal.

Note Typically, the console port is disabled when the CMTS downloads a Cisco IOS configuration file to the router. If this is the case, the CLI can be accessed only through a Telnet connection.

Understanding the Command-Line Interface

The Cisco IOS command-line interface (CLI) is a text-based interface available on every Cisco router that uses the Cisco IOS software. This allows a network administrator to quickly configure any of Cisco's many different models of routers without having to learn a unique interface for each.

The following guidelines apply to the CLI:

- The CLI is case-insensitive—for example, you can enter either **SHOW VERSION** or **show version** to display the Cisco uBR924 router's software revision.
- You can abbreviate commands and keywords to the minimum number of characters that define a unique abbreviation. For example, you can abbreviate the **show** command to **sh** (but you cannot abbreviate the show command to just **s** because several other commands also start with the letter **s**).
- If you enter an unrecognized command, the router assumes the command is actually the host name of a PC or other router and tries to open a Telnet connection to it. If the router cannot find that host, the connection will eventually time out and the CLI prompt will be redisplayed.
- By default, if a command displays more than one screen of data, it pauses the screen and displays **--More--** at the bottom of the screen. You can advance one line at a time by pressing the Return key, advance one screen at a time by pressing the spacebar, or quit by pressing **q**.
- As a general rule, every configuration command can be disabled by prefixing the command with the keyword **no**. For example, IP routing is enabled with the **ip routing** command; IP routing is disabled with the **no ip routing** command.
- The CLI on the Cisco uBR924 router can be accessed either through a Telnet connection or through a serial connection with its console port. (Web browser access to the CLI is not supported on the Cisco uBR924 router when the Cable Monitor is active.)

These additional topics are covered in the sections that follow:

- The CLI contains many different command modes that allow access to different areas of the Cisco uBR924 router's configuration. Certain commands are available only in a specific command mode. See "Command Modes" section on page A-3.
- The question mark character (?) displays a list of the available commands and can be used to display help about a specific command. See "Context-Sensitive Help" section on page A-6.
- You can use the command history feature to quickly recall and edit previous commands. See "Command History Features" section on page A-7.
- When commands produce long displays, you can use output modifiers to select which parts of the display you want to see. See "Using Output Modifiers" section on page A-8.

Command Modes

The Cisco IOS software has many different modes of operation—each mode contains its own set of commands that either display or configure a particular aspect of the Cisco uBR924 router's configuration. When you initially log in to the Cisco uBR924 router, you enter user EXEC mode, which provides a limited number of commands that can only display information about the router; you cannot change the router's configuration in user EXEC mode.

To change the router's configuration, you must enter privileged EXEC mode or one of the other configuration modes. Each command mode has a unique prompt so that you can easily see which mode you are in.

Table A-1 shows the most common modes that are used on the Cisco uBR924 router:

Table A-1 Cisco uBR924 Router Command Modes

Command Mode	Function	Access Method	Prompt[1]
User EXEC	Contains a limited number of commands that only display information about the Cisco uBR924 router.	Log in.	Router>
Privileged EXEC	Contains a larger number of display commands, as well as other commands that can change the configuration of the router. Also provides access to the global configuration mode.	From user EXEC mode, enter the **enable** command.	Router#
Global configuration	Contains commands that can change the operation of the Cisco uBR924 router at a system level and provides access to the interface configuration mode.	From privileged EXEC mode, enter the **configure terminal** command.	Router(config)#
Interface configuration	Contains commands that change the operation of the router's Ethernet and cable interfaces.	From global configuration mode, enter the **interface** *interface-num* command.	Router(config-if)#

1. The prompt always displays the router's hostname. The default hostname is "Router" but this can be changed with the global configuration **hostname** command.

Table A-1 lists the command modes in the order they must be accessed. You must log in to a higher-level mode before accessing the next lower mode. For example, before you can enter global configuration mode, you must first log in to user EXEC mode and then privileged EXEC mode. Then you can enter global configuration mode, and if desired, log in to interface configuration mode.

To leave a command mode and return to the previous mode, enter either the **exit** or **end** command. See the following sections for more details on each command mode.

Note For complete information on using the CLI, see the *Configuration Fundamentals Configuration Guide*, available on CCO and the Documentation CD-ROM.

User EXEC Mode

When you log in to the Cisco uBR924 router, you automatically enter the user EXEC command mode, which contains commands that only display some parts of the router's configuration. In general, user EXEC commands allow you to connect to remote devices, change terminal settings on a temporary basis, perform basic tests, and list system information.

The user-level prompt consists of the router's name followed by a right angle bracket (>):

```
Router>
```

To leave user EXEC mode and log out of the Cisco uBR924 router, enter the **logout** or **exit** command.

Privileged EXEC Mode

Before you can enter any commands that change the Cisco uBR924 router's configuration, you must enter privileged EXEC mode. In this mode you can change certain router parameters, use more detailed **show** commands, and other configuration modes to change the operation of the router and its interfaces.

To access the privileged EXEC mode, enter the **enable** command from user EXEC mode. You are then prompted for a password, if one has been set for the privileged EXEC mode. The password is not displayed on the screen and is case sensitive. The prompt changes to the router's host name followed by the pound sign (#) to indicate you are now in privileged EXEC mode.

Note If an enable password has not been set, privileged EXEC mode can be accessed only from the router console, not through a Telnet connection.

The following example shows how to access privileged EXEC mode:

```
Router> enable
Password: <password>
Router#
```

To return from privileged EXEC mode to user EXEC mode, use the **disable** or **exit** command.

Global Configuration Mode

The global configuration mode contains commands that change configuration parameters that affect the operation of the entire Cisco uBR924 router, such as routing and bridging functions, as opposed to changing the operation of a single interface. To log in to global configuration mode, enter the **configure terminal** from privileged EXEC mode. The prompt changes to the router's host name followed by "(config)#" to indicate you are now in global configuration mode.

The following example shows how to access global configuration mode:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
```

To exit global configuration mode and return to privileged EXEC mode, enter the **exit** or **end** command, or type Ctrl-Z.

Interface Configuration Mode

The interface configuration mode configures features for an individual interface. The Cisco uBR924 cable access router supports the following interfaces:

- Ethernet0—Ethernet interface on the back panel of the router
- cable-modem0—Cable interface that connects to the cable network
- Loopback0—Internal interface used primarily for debugging

To log in to interface configuration mode, enter the **interface** command followed by the name of the interface to be configured. The prompt changes to the router's host name followed by "(config-if)#" to indicate you are now in interface configuration mode.

For example, to configure the cable interface on the Cisco uBR924 router, enter the following commands from global configuration mode:

```
Router(config)# interface cable-modem 0
Router(config-if)#
```

To exit interface configuration command mode and return to global configuration mode, enter the **exit** command, or type Ctrl-Z.

Context-Sensitive Help

The Cisco IOS CLI contains a context-sensitive help feature that can display a list of the commands that are available for the current command mode. The context-sensitive help can also display the syntax for a particular command, as well as complete a partially entered command.

Table A-2 shows the different ways you can access the context-sensitive help:

Table A-2 Context-Sensitive Help for the Command -Line Interface

Command	Purpose
help	Obtain a brief description of the help system in any command mode.
?	List all commands available for a particular command mode.
*partial-command***?**	Obtain a list of commands that begin with a particular character string. (Do not enter a space before the question mark.)
partial-command<**Tab**>	Complete a partial command name. (Do not enter a space before entering the tab character.)
command **?**	List a command's associated keywords. (A space must precede the question mark.)
command keyword **?**	List a keyword's associated arguments. (A space must precede the question mark.)

The context-sensitive help displays only the commands and options that are appropriate for the current command mode. For example, to display the available show commands in the user EXEC mode, enter **show ?** as shown in the following example:

```
ubr924> show ?

  backup            Backup status
  bootflash:        display information about bootflash: file system
  call              Show Calls
  cca               CCA information
  class-map         Show QoS Class Map
  clock             Display the system clock
  compress          Show compression statistics
  dial-peer         Dial Plan Mapping Table for, e.g. VoIP Peers
  dialer            Dialer parameters and statistics
  exception         exception informations
  flash:            display information about flash: file system
  gateway           Show status of gateway
  history           Display the session command history
  hosts             IP domain-name, lookup style, nameservers, and host table
  location          Display the system location
  num-exp           Number Expansion (Speed Dial) information
  policy-map        Show QoS Policy Map
  ppp               PPP parameters and statistics
  queue             Show queue contents
  queueing          Show queueing configuration
  radius            Shows radius information
  rmon              rmon statistics
  sessions          Information about Telnet connections
  sgcp              Display Simple Gateway Control Protocol information
  snmp              snmp statistics
  template          Template information
  terminal          Display terminal configuration parameters
  traffic-shape     traffic rate shaping configuration
```

```
  translation-rule  Show translation rule table
  users             Display information about terminal lines
  version           System hardware and software status
  voice             Voice port configuration & stats
ubr924>
```

Entering the same **help** command in privileged EXEC or global configuration mode would display a different list of **show** commands. The following shows how to display a list of available commands that start with "t":

```
ubr924> t?
telnet  terminal  traceroute  tunnel
ubr924>
```

Command History Features

The CLI command history feature remembers the commands that you have entered during the current session. You can use this feature to repeat or change previous commands without retyping them. See the following sections for more information.

Displaying the Command History

To recall commands from the history buffer, use one of the commands shown in Table A-3.

Table A-3 Recalling Previous Commands

Command	Purpose
Press **Ctrl-P** or the up arrow key.[1]	Recall commands in the history buffer, beginning with the most recent command. Repeat to recall successively older commands.
Press **Ctrl-N** or the down arrow key.[1]	Return to more recent commands in the history buffer after recalling commands with **Ctrl-P** or the up arrow key. Repeat to recall successively more recent commands.
show history	List the last several commands you have just entered (user EXEC mode only).

1. The arrow keys function only on ANSI-compatible terminals such as VT100s.

Editing Previous Commands

When you display a previous command using **Ctrl-P** or **Ctrl-N,** you can edit that command to correct any errors or to change a parameter. This allows you to quickly give a series of similar commands without having to retype each command.

Table A-4 shows the most commonly used editing commands.

Table A-4 Editing Previous Commands

Command[1]	Purpose
Press **Ctrl-A**	Move to the beginning of the line.
Press **Ctrl-B**	Move back one character.
Press **<Esc>-B**	Move back to the previous word.

Table A-4 Editing Previous Commands

Command[1]	Purpose
Press **Ctrl-D**	Delete the character at the cursor position.
Press **Ctrl-E**	Move to the end of the line.
Press **Ctrl-F**	Move forward one character.
Press **<Esc>-F**	Move forward one word.
Press **Ctrl-K**	Delete all characters from the cursor to the end of the line.
Press **Ctrl-U** or **Ctrl-X**	Delete all characters from the cursor to the beginning of the line.
Press **Ctrl-W**	Delete a single word.

1. These editing commands are similar to those used in the EMACS text editor.

Note Additional editing commands are given in the *Configuration Fundamentals Configuration Guide*, available on CCO and the Documentation CD-ROM.

Command History Buffer Size

By default, the command history feature stores the 10 most recent commands in its history buffer. You can change the size of this buffer for the current terminal session with the terminal history command:

```
ubr924> terminal history size 20
ubr924>
```

The **terminal no history size** command resets the number of lines saved in the history buffer to the default of 10 lines.

Using Output Modifiers

Many of the Cisco uBR924 router's commands output a great deal of information that takes many screens to display. You can use the Cisco IOS software's output modifiers to filter the output of almost any command, so that you can display only those lines you are interested in.

The output modifier feature is invoked by using the pipe symbol (|). To use this feature, enter a command as normal but add a space and the pipe symbol at the end of the command line. Then add one of the keywords

Table A-5 Using Output Modifiers

Command	Purpose
begin *regular expression*	Display the first line that matches the regular expression and then all other lines that follow that line.
include *regular expression*	Display all lines that match the regular expression.
exclude *regular expression*	Display all lines except those that match the regular expression.

The following example shows how the output from the **show ip traffic** command is filtered to display only those lines that include the word "error":

```
ubr924>show ip traffic | include error
         0 format errors, 0 checksum errors, 1 bad hop count
  Rcvd: 0 format errors, 0 checksum errors, 0 redirects, 4 unreachable
  Total: 0/0, 0 checksum errors, 0 format errors
  Total: 0/0, Format errors: 0/0, Checksum errors: 0/0
  Rcvd: 134 total, 0 checksum errors
  Rcvd: 23 total, 0 checksum errors, 9 no port
  Rcvd: 17 total, 0 checksum errors, 1 no port
```

Understanding Cisco IOS Configuration Files

Cisco IOS configuration files are text files that contain Cisco IOS commands to configure the Cisco uBR924 router when it boots up and is first configured. These commands are the same commands that could be given manually at the router's CLI interface; however, putting them in a configuration file avoids having to retype them whenever the router is reset.

Downloading the Configuration File

Usually, the Cisco IOS configuration file is specified as part of the DOCSIS configuration file. In this situation, the service provider creates and maintains both the DOCSIS and Cisco IOS configuration files for the routers, and those files are stored on TFTP servers located at the provider's headend plant.

The Cisco uBR924 router automatically loads the DOCSIS configuration file when it is connected to a cable network and powered on. If the DOCSIS configuration file specifies that a Cisco IOS configuration file is to be loaded, the router uses the TFTP protocol to download that file and then executes the file so that the non-DOCSIS routing and interface parameters are correctly configured.

When the DOCSIS configuration file specifies that a Cisco IOS configuration file should be downloaded, the Cisco uBR924 router automatically takes the following steps to ensure that the configuration cannot be changed by the user at the remote site:

1. Terminates any current Telnet sessions.
2. Disables console access.
3. Deletes the current Cisco IOS configuration, if any.
4. Downloads the Cisco IOS configuration file.
5. After configuring itself according to the commands in the Cisco IOS configuration file, the router comes online and starts sending traffic.

If the DOCSIS configuration file does not specify that a Cisco IOS configuration file should be loaded, the network administrator can log in to the router's CLI interface and manually load the file using the **copy tftp** command. (In this situation, console access is not disabled, allowing users at the remote site to modify the configuration if desired.)

Note The DOCSIS configuration file is a binary file that must be in the specific format given by the DOCSIS 1.0 specification; it configures DOCSIS and cable-related parameters. The Cisco IOS configuration file is a text file that can be in any arbitrary format, as long as the lines in that file contain valid commands that could be given at the router's CLI interface. Typically, the Cisco IOS configuration file sets routing parameters and whatever other parameters are needed for special feature sets, such as the voice over IP (VoIP) or firewall features.

Startup and Run-Time Configuration Files

The startup configuration file is a Cisco IOS configuration file stored in the router's non-volatile Flash memory and is automatically run whenever the router is reset or powered-on. When a DOCSIS configuration file specifies that a Cisco IOS configuration file should be downloaded, that Cisco IOS configuration file automatically becomes the startup configuration file.

The run-time configuration file is the Cisco IOS configuration file that the router is currently using as it operates. When a router is first powered-on or reset, the run-time configuration file is the same as the startup configuration file.

However, when you make configuration changes to the router, either by using the CLI or by using SNMP commands, the run-time configuration file is updated with those changes. Over time, the run-time configuration file has a different configuration than the startup configuration file. Resetting the router automatically erases the run-time configuration and restores the startup configuration.

If you want to save your changes to the router's configuration, you must save the run-time configuration as the startup configuration file. To do so, enter the following global configuration command:

```
copy running-config startup-config
```

Note Any changes you make to either the startup or run-time configuration are automatically overwritten when the router is rebooted if the DOCSIS configuration file specifies that a new Cisco IOS configuration file must be downloaded from the TFTP server. If this is the case, you must also manually update the Cisco IOS configuration file on the TFTP server to preserve any configuration changes you make.

To restore the startup configuration without resetting the router, give the following global configuration command:

```
copy startup-config running-config
```

Displaying the Configuration Files

The startup and run-time configuration files can be displayed with the following global configuration commands:

```
show startup-config
show running-config
```

The Cisco uBR924 router displays the appropriate configuration file in a format that you can capture and save on a TFTP server so it can be downloaded to another router.

Note The configuration files do not contain any commands that restore the router to its default values. For example, if you enable IP routing with the "**ip routing**" command, this is not saved in the configuration files because this is the default configuration. However, if you disable IP routing with the "**no ip routing**" command, this is saved in the configuration file.

The **show** command uses exclamation marks (!) to create blank lines as spacers. These extra lines do not affect the functionality of the router but exist only to make the configuration files more readable.

File Format

The Cisco IOS configuration file is an ASCII text file that contains any Cisco IOS configuration commands to configure the Cisco uBR924 router. The router is automatically put into the global configuration mode when the file is executed, but if you use any commands for any other command modes, you must give the appropriate global configuration command to enter that other command mode first.

For example, to configure the cable interface on the Cisco uBR924 router, you must first enter interface mode with the following command:

```
interface cable 0
```

You can use exclamation marks (!) to create comments and blank lines in your own configuration files. These comments and blank lines are not preserved when the file is loaded into the router. However, they are useful for communicating information to other administrators who might be working with the files on the TFTP server.

Useful Commands

Table A-6 lists some of the most commonly used commands for the Cisco uBR924 router.

Table A-6 Useful Commands

Command	Command Mode	Purpose
banner	global configuration	Displays and configures the login banners that appears when a user first logs in and when a user moves to a different command mode.
configure terminal	user EXEC	Enters global configuration mode.
copy startup-config running-config	global configuration	Configures the router with its boot-up configuration file.
enable	user EXEC	Enters privileged EXEC mode.
exit	all modes	Leaves the current command mode and returns to the next higher level. If currently in user EXEC mode, logs you out of the router.
hostname	global configuration	Sets the router's hostname.
logout	user EXEC	Logs out of user EXEC mode and the Cisco uBR924 router.
show flash	user EXEC	Displays the content of the router's Flash memory, which contains the Cisco IOS software image that was loaded.
show history	user EXEC	Displays the most recently entered commands.
show interfaces	user EXEC	Displays the configuration and status of each of the router's interfaces.
show ip arp	user EXEC	Displays the contents of the router's current Address Resolution Protocol (ARP) table.

Table A-6 Useful Commands (continued)

Command	Command Mode	Purpose
show ip dhcp server statistics	user EXEC	Displays the contents of the router's DHCP database.
show ip interface	user EXEC	Displays the IP configuration and status for the router's Ethernet and cable interfaces.
show ip protocols	user EXEC	Displays the IP routing protocol parameters and status.
show ip rip database	user EXEC	Displays the contents of the Routing Information Protocol (RIP) database.
show ip route	user EXEC	Displays the contents of the router's current IP routing table.
show ip traffic	user EXEC	Displays statistics for the IP traffic sent through the router.
show protocols	user EXEC	Displays the currently configured protocols for each interface.
show running-config	privileged EXEC	Displays the active configuration.
show startup-config	privileged EXEC	Displays the configuration loaded into the router at boot-up.
show version	user EXEC	Displays the Cisco uBR924 software and hardware versions.

Using the Cable Monitor Tool

This appendix describes the Cisco uBR924 cable access router's Cable Monitor tool. The Cable Monitor is part of the router's onboard software that provides a web-based diagnostic tool for easy access to configuration and status information about the router, without requiring access to the router's command line interface (CLI).

Note The Cable Monitor is available in Cisco IOS Release 12.1(1)T and later releases.

Technicians and subscribers can access the tool in the following ways:

- When the Cisco uBR924 router has established connectivity with the CMTS over the cable interface, a service technician can use a web browser to remotely access the router and display the desired information.
- When the cable network is not operational and the Cisco uBR924 router is not online, the subscriber can access the tool with a PC connected to the router's Ethernet ports. Technicians can then prompt the user for the information they need to determine the source of the problem.

The Cable Monitor operates in two modes:

- Basic Mode—In basic mode, the Cable Monitor displays the current LED colors and status, as well as the results of the router's initialization routines (its power-on self-tests and its registration with the CMTS). This provides a quick status check of the router, as well as what stage of the initialization process is failing (if any).
- Advanced Mode—In advanced mode, the Cable Monitor also displays status and configuration information about the router's voice ports, the DOCSIS MAC layer, and cable interface, as well as performance statistics. Technicians with the proper login ID and password can also display advanced debug information that collects the output of the most commonly used troubleshooting commands.

Note The Cable Monitor is a read-only tool—it cannot be used to modify or reconfigure the Cisco uBR924 router. However, some of the information displayed in the advanced mode could be used to defeat the router's security. This information is available only to users who enter the enable password. Cisco recommends that an encrypted enable password be set on all Cisco uBR924 routers deployed at subscriber sites. Passwords (along with SNMP community strings) should be different for each router, using a non-trivial pattern. If an enable password is not being used at a subscriber's site, the Cable Monitor should be run only in the basic mode.

The following sections describe the Cisco uBR924 router's Cable Monitor:

Enabling the Cable Monitor

By default, the Cable Monitor is disabled. To allow technicians and subscribers to access the Cable Monitor, it must be enabled using the **ip http** global configuration command as follows:

	Command	Purpose
Step 1	ubr924(config)# **ip http cable-monitor** {**basic** | **advance**} [*URL-IP-address URL-mask*]	Immediately enable the Cable Monitor in either basic or advanced mode. Optionally specify the IP address and subnet mask for the Cable Monitor; these parameters also define the IP address pool used by the temporary DHCP server when the cable interface goes down.
Step 2	ubr924(config)# **ip http port** *http-port*	(Optional) Specify the TCP port number to use for web server (HTTP) requests. The default is the well-known web server port of 80.

Tip If the router is operating in routing mode, and the cable interface is up, you can also access the Cable Monitor by entering the IP address for the Ethernet interface into your web browser.

When the Cable Monitor is enabled, it also automatically enables the Cisco web server (giving the equivalent of the **ip http server** command). However, while the Cable Monitor is active, it disables all other access to the Cisco web server, preventing the user from accessing the CLI commands that are normally available when the Cisco web server is active. When the Cable Monitor is active, the Cisco web server can be used only for displaying the Cable Monitor pages.

Note If the Cable Monitor is not enabled on the Cisco uBR924 router, Cisco recommends that the Cisco web server be disabled, using the **no ip http server** configuration command.

Configuration Modes

The **ip http cable-monitor basic** command enables the Cable Monitor and puts it in basic mode. In this mode, the Cable Monitor displays information only about the router's current status, whether it has successfully completed all of its initialization routines, and cable performance statistics.

The **ip http cable-monitor advance** command enables the Cable Monitor and puts it in advanced mode. In this mode, the Cable Monitor displays the router's current status, the status of its initialization routines, the status of the voice ports, the router's basic configuration, and performance statistics. If an

enable password is set, users who can supply the enable password can also view detailed debugging and troubleshooting configuration information; if an enable password is not set, all users can view this information.

Caution To ensure a secure system, the advanced mode should not be used unless a secure encrypted enabled password is configured on the Cisco uBR924 router.

By default, the Cable Monitor is configured with the IP address 192.168.100.1, which is a Class C address in the private IP address space reserved for private networks. If a device on the subscriber's private network is already using this IP address, use the *URL-IP-address* and *URL-mask* optional parameters to specify another IP address.

For example, to enable the Cable Monitor for advanced mode with the private IP address of 10.0.1.2 and the default HTTP port of 80, use the following command:

ip http cable-monitor advance 10.0.1.2 255.0.0.0

Note This command can be included in the Cisco IOS configuration file that is downloaded to the router at power-on during the DOCSIS provisioning.

Security Considerations

The Cable Monitor is a read-only tool that cannot be used to change the configuration of the Cisco uBR924 router. The debug page in advanced mode, however, does display information that could be used to defeat the router's security. This page is password-protected, requiring users to enter the enable password before displaying it; however, if an enable password has not been set, any user can display the debug page, which could reveal SNMP community strings and other configuration information.

For this reason, the following guidelines should be used when developing a security policy for the router:

- If the Cable Monitor is being used in advanced mode, an encrypted enable password must be set. Otherwise, all users can view the debug page, which displays the router's complete configuration, including SNMP community strings.
- If no enable password is set, so as to prevent remote configuration of the router via Telnet, then the Cable Monitor must be used only in basic mode.

Note Since downloading a Cisco IOS configuration file during the provisioning process automatically disables the console port, all remote configuration of the Cisco uBR924 router using the CLI is disabled when an enable password is not set. In this situation, the only way to change the router's configuration is through SNMP or by resetting the router and uploading a new configuration file. The Cable Monitor, however, must not be run in advanced mode when no enable password has been set because this would allow unauthorized users to view SNMP community strings and use SNMP to change the router's configuration.

Disabling the Cable Monitor

To disable the Cable Monitor, use the **ip http** global configuration command as follows:

	Command	Purpose
Step 1	ubr924(config)# **no ip http cable-monitor**	Immediately disable the Cable Monitor, preventing any web server access to its web pages. This also automatically disables access to the Cisco web server (which is equivalent to giving the **no ip http server** command).

Note The Cable Monitor is disabled by default, so the **no ip http cable-monitor** command does not need to be included in the Cisco IOS configuration file that is downloaded to the router at power-on during the DOCSIS provisioning. However, the Cisco web server is enabled by default; if this is not desirable, you should include the **no ip http server** command in the Cisco IOS configuration file that is downloaded to the Cisco uBR924 router.

When disabling the Cable Monitor, the console might display warning messages similar to the following:

```
% monitor-209.165.202.131 is not in the database.
% monitor-192.168.100.1 is not in the database.
% Range [209.165.202.131, 209.165.202.131] is not in the database.
% Range [192.168.100.1, 192.168.100.1] is not in the database.
```

These messages can be ignored because they are simply confirming that the IP addresses used for the Cable Monitor are no longer being used for that purpose.

Note The Cable Monitor can also be disabled by giving the **no ip http server** command, which disables all web server access. However, this is not recommended because it does not release the system resources that are specifically allocated to the Cable Monitor.

Accessing the Cable Monitor

The Cable Monitor can be accessed either through the cable interface (typically by technicians at the headend or the service provider's network operations center) or through the Ethernet interface (typically by subscribers when the cable interface has gone down). See the following sections for more information.

Note You must be using a web browser that supports frames to access the Cable Monitor pages.

Through the Cable Interface when the Cable Interface is Operational

During normal operations—when the Cisco uBR924 router is online and has connectivity with the CMTS through the cable interface—service technicians at the headend can access the Cable Monitor by doing the following:

Step 1 Start a web browser on a PC or workstation at the headend that has TCP/IP connectivity with the Cisco uBR924 router.

Step 2 Type in a URL with the IP address assigned to the cable interface on the Cisco uBR924 router. This is typically an address in the service provider's IP address space.

For example, if the Cisco uBR924 router has been assigned the IP address of 209.165.202.131 by the service provider, a technician at the headend would use the following URL to access the Cable Monitor:

http://209.165.202.131

If a port number other than the default of 80 has been assigned to the Cable Monitor, that port number must be included as part of the URL. For example, if the Cisco uBR924 router has been assigned the IP address of 209.165.202.131 and a port number of 8080 by the service provider, a technician at the headend would use the following URL to access the Cable Monitor:

http://209.165.202.131:8080

Tip If the router is operating in routing mode, and the cable interface is up, you can also access the Cable Monitor by entering the IP address for the Ethernet interface into your web browser.

Through the Ethernet Interface when the Cable Interface is Not Operational

When the Cisco uBR924 router loses connectivity with the CMTS at the headend and detects that its cable interface is not operational, the router automatically switches into a diagnostic mode and does the following:

- Activates a temporary DHCP server to assign IP addresses in the IP network that is defined by the IP address and subnet mask given with the **ip http cable-monitor** command (the default address pool is the Class C private network 192.168.100.0).
- When a PC or other workstation connected to the router's Ethernet ports makes a DHCP request, the router assigns an IP address and default gateway from this address space so that the PC can communicate with the Cable Monitor on the router.

Note The PC or workstation can be rebooted to force it to make a DHCP request. If using a Windows 95 or Windows 98 system, you can also use the **winipcfg** utility to send a DHCP release and renew request.

- When the router detects any web server requests, it automatically redirects them to the Cable Monitor.
- The router's DHCP server renews these IP addresses every 30 seconds as long as the cable interface is down.
- When the cable interface is back up, the router returns to normal operation, using the configuration that existed before it switched into diagnostics mode. (At this point, the PC or workstation that accessed the Cable Monitor can be rebooted to restore its configuration, or you can wait from 30 to 60 seconds for the PC to automatically issue a DHCP renew request. Windows 95 or Windows 98 users can also use the **winipcfg** utility.)

When the cable interface is down, users at the subscriber site can use the following procedure to access the Cable Monitor to aid in troubleshooting the problem with the cable network:

Step 1 If necessary, connect a PC to one of the Ethernet ports on the Cisco uBR924 router.

Step 2 If necessary, configure the PC so it obtains its IP address from a DHCP server—on Windows 95 computers, display the Network Control Panel, click the TCP/IP component for the computer's Ethernet adapter, click the **IP Address** tab under Properties, and click **Obtain an IP address automatically**.

Note Since most PCs are configured to use a DHCP server, this step is not usually necessary. However, if the PC is normally assigned a static IP address, you should copy down its IP address and default gateway address before reconfiguring it to use a DHCP server.

Step 3 Reboot the PC so that it obtains an IP address from the Cisco uBR924 router.

Step 4 Start a web browser on the PC and enter any arbitrary URL, such as **http://anything**. The Cisco uBR924 router redirects the request to the Cable Monitor, which displays its home page.

Note In the default configuration, the static IP address 192.168.100.1 is reserved for the Cable Monitor while in diagnostic mode. If desired, subscribers (or technicians who visit the subscriber's site) can enter the URL **http://192.168.100.1** as a bookmark for the Cable Monitor. If a different IP address has been assigned to the Cable Monitor, users should enter that value as the bookmarked address.

Step 5 When the cable interface resumes normal operations, reconfigure the PC (if necessary) to restore its previous TCP/IP configuration. Then wait from 30 to 60 seconds or reboot the PC to restore normal operations.

Sample Pages

Table B-1 lists each of the web pages displayed by the Cable Monitor, the modes in which the pages are displayed, and a short description of each page's information.

Table B-1 Cable Monitor Pages

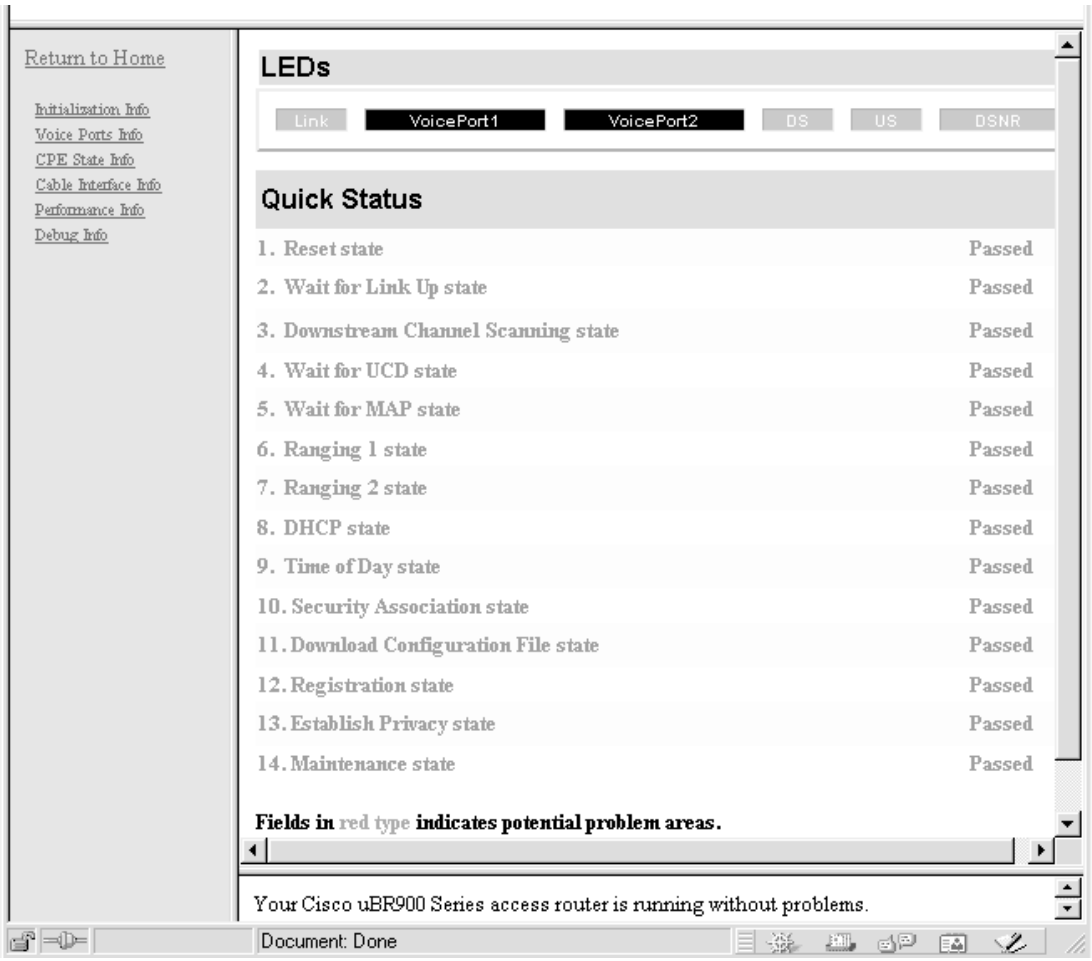
Cable Monitor Page	Modes Available	Description
Home Page	Basic and Advanced	Displays current status and initialization information.
Initialization Information	Advanced Only	Displays more detailed initialization information.
Voice Ports Information	Advanced Only	Displays status and configuration information for the router's voice ports.
CPE State Information	Advanced Only	Displays the basic configuration for the router.
Cable Interface Information	Advanced Only	Displays the current status and configuration of the cable interface.
Performance Information	Basic and Advanced	Displays performance statistics for the router.
Debug Information Page	Advanced Only (requires enable password)	Displays advanced configuration information.

The following sections describe each page in more detail.

Home Page

The Cable Monitor home page displays the current status of the LEDs on the front panel of the Cisco uBR924 router and summarizes the status of the router's registration process with the CMTS. Figure B-1 shows a typical home page when the Cable Monitor is configured for advanced mode.

Figure B-1 Cable Monitor Home Page



Note Figure B-1 shows the home page when the Cable Monitor is configured for advanced mode; in this mode, the left side displays links for all available pages. When the Cable Monitor is configured for basic mode, the left side displays only the link for the Performance Information page.

The top of the Cable Monitor home page displays the current status of the LEDs on the front panel of the Cisco uBR924 router:

- Link—If green, indicates that the cable interface is operational. If black, indicates that the cable interface is not receiving a signal, typically because of a break in the cable connection.
- Voice Port 1—If green, indicates that a call is active on voice port 1. If black, indicates that voice port 1 is not in use.

- Voice Port 2—If green, indicates that a call is active on voice port 2. If black, indicates that voice port 2 is not in use.
- US—If green, indicates that the router has established connectivity with the CMTS and is operating within 6 dB of the desired upstream power level. If black, indicates that the upstream power level is not within the desired power level.
- DS—If green, indicates that the router is locked and communicating on a downstream channel.
- DSNR—If green, indicates that the router is receiving a quality downstream signal (this is a signal that has a signal-to-noise ratio (SNR) that is 5 dB or more above the downstream lock threshold). If black, indicates that noise on the downstream has exceeded the minimum recommended threshold, and the signal is currently within 5 dB of failing due to excessive noise.

The Quick Status section of the home page summarizes the information that is displayed on the Initialization Information page, described in the next section.

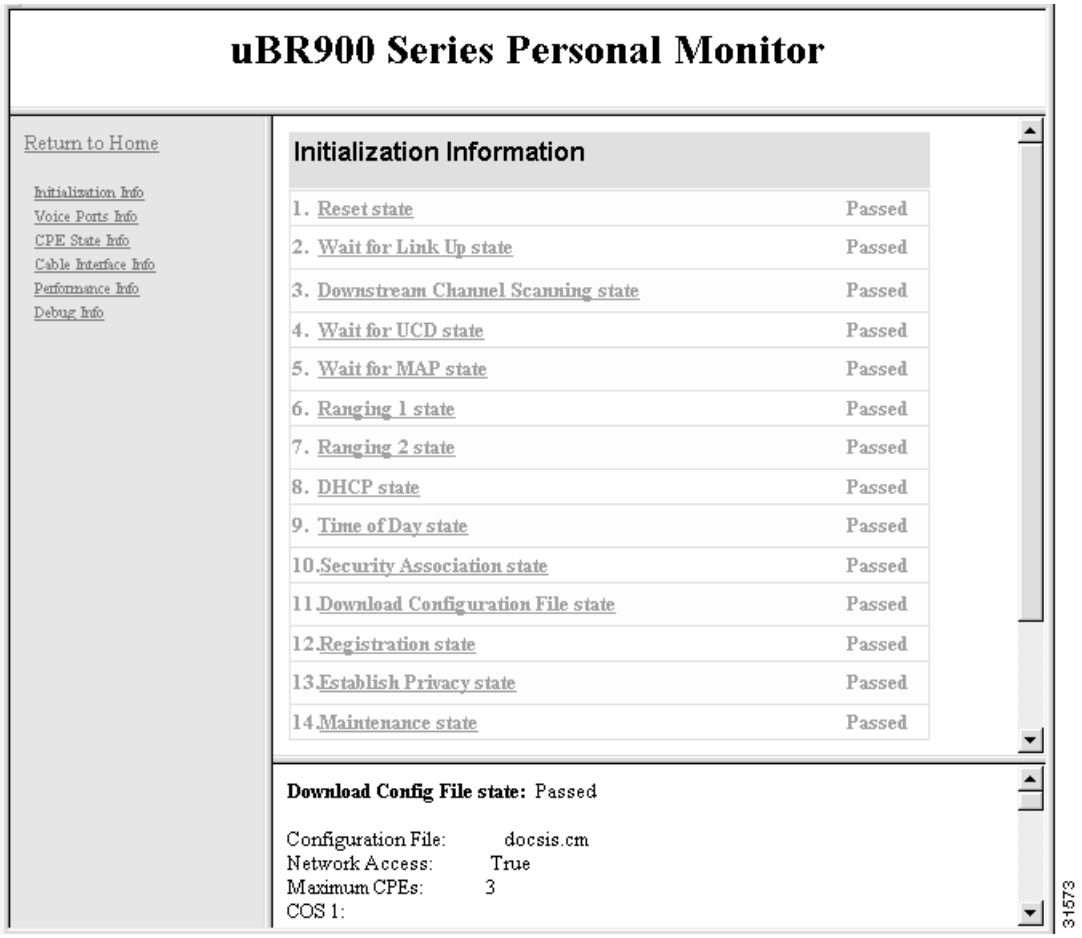
Initialization Information

The Initialization Information page is available to advanced users only and displays the same information shown in the Quick Status section of the Home Page. This information summarizes the router's power-on initialization and registration process using the following color codes:

- Stages that passed are shown in green.
- Any stage that failed is shown in red.
- Stages that were not reached because of the failure of a previous stage are shown in black.

Figure B-2 shows a display for a Cisco uBR924 router that has successfully registered and come online.

Figure B-2 Initialization Information Page



This page provides detailed information on the state changes when the Cisco uBR924 router tries to establish communication and registration with the CMTS. All stages must show "Passed" before the router can come online.

Clicking on the name of the stage displays more information, if available, in the bottom half of the window. For example, clicking stage 11, "Download Configuration File state," displays the name of the configuration file that was downloaded to the router and the configuration parameters it contained.

The following is the normal progression of states that would be displayed if the Cisco uBR924 router registers successfully with the CMTS:

- Reset state—The router boots the Read-Only Memory (ROM) from its Flash memory, performs a self-test, initializes processor hardware, and boots the Cisco IOS release image stored in Flash memory.
- Wait for link up state—The router checks the cable interface and determines whether a DOCSIS-compliant signal exists.
- Downstream frequency scanning state—The router acquires a temporary downstream channel by matching the clock sync signal that is regularly sent out by the CMTS in the downstream frequency range. If this stage passes, click this link to display the following information:
  - Downstream ID
  - Downstream Frequency
  - Downstream Symbol Rate
  - Downstream QAM Mode
  - Signal to Noise Ratio Estimate
  - Downstream Lock Threshold
  - Downstream Search
- Wait for Upstream Channel Descriptor (UCD) state—The router waits for an Upstream Channel Descriptor (UCD) message from the CMTS and configures itself for the upstream frequency specified in that message. If this stage passes, click this link to display the following information:
  - Upstream ID
  - Upstream Frequency
  - Mini-Slot Size
- Wait for MAP state—The router waits for the next upstream bandwidth allocation map message (MAP), which are regularly sent from the CMTS, to find the next available shared request timeslot.
- Power ranging first state—The router then uses the MAP timeslot to send a ranging request message to the CMTS, communicating the router's user ID (UID, which is its unique MAC address), using a temporary Service Identifier (SID) of 0 (zero) to indicate it has not yet been allocated an upstream channel. If this stage passes, click this link to display the following information:
  - Ranging Offset
  - Power Level
  - Ranging Response SID Assigned
  - Adjust Transmit Power
- Power ranging second state—In reply to the router's 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.
- DHCP state—After the next MAP message broadcast, the router uses a shared require timeslot to invoke the Dynamic Host Configuration Protocol (DHCP) to establish IP connectivity with the TCP/IP network at the headend. The DHCP server sends a response with the following information:
  - Assigned IP Address
  - Network Mask
  - TFTP Server IP Address
  - Time Server IP Address

  - Time Zone Offset
  - Configuration File Name
- Time of Day (TOD) state—The router configures itself for the specified IP address and gets the current date and time from the specified ToD server.
- Security association state—Reserved for future use.
- Download configuration file state—Using the TFTP protocol, the router downloads the specified DOCSIS configuration file and configures itself for the appropriate parameters. The DOCSIS configuration file contains the following parameters:
  - Configuration File
  - Network Access
  - Maximum CPEs
  - Class of Service information—Depending on the software image installed, up to four classes of service (CoS) are displayed. The following information is shown for each CoS:

    Assigned SID

    Max Downstream Rate

    Max Upstream Rate

    Upstream Priority

    Min Upstream Rate

    Max Upstream Burst

    Privacy Enable

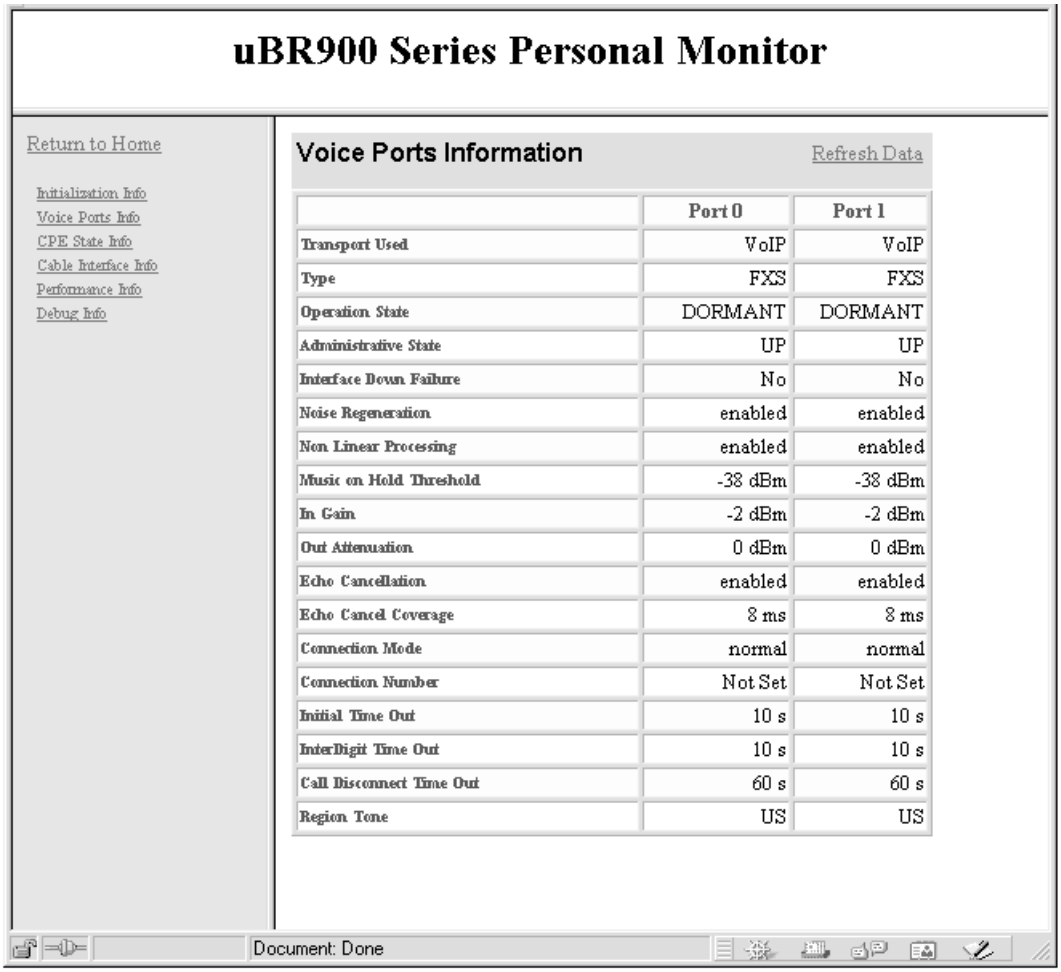
Note For more information on these parameters, see the "DOCSIS Configuration File" section on page 2-3.

- Registration state— The router sends another registration request to the CMTS containing the CoS parameters given in the DOCSIS configuration file. 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.
- Establish baseline privacy state—If BPI security has been enabled, the router negotiates the BPI parameters with the CMTS.
- Maintenance state—The router enters the maintenance state, passing traffic on the cable interface to and from the CMTS, and responding to periodic maintenance messages from the CMTS.

Voice Ports Information

The Voice Ports Information page summarizes the current status of the two voice ports on the Cisco uBR924 router. Figure B-3 shows a typical Voice Ports Information page.

Figure B-3 Voice Ports Page



Note The Voice Ports Information page has valid information only when the Cisco uBR924 router is running a software image with voice support.

The Voice Ports Information page displays the same information that is shown using the **show voice port** command:

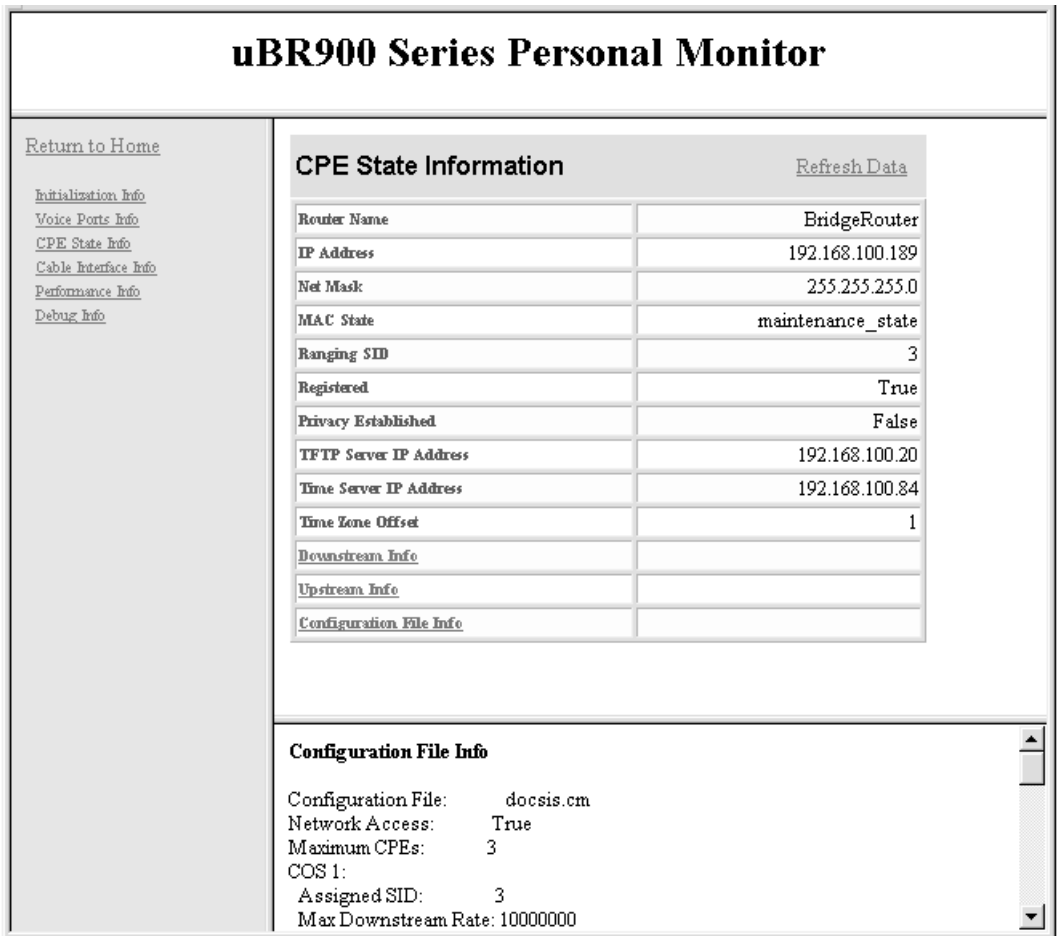
- Transport Used—The type of network being used to make calls on each voice port:
  - VoIP—The voice call is using Voice over IP transmitted over the cable interface (default).
  - Analog—The voice call is using the PTSN cutover port, indicating that the cable interface is down or that power was temporarily interrupted to the router.
- Type—The type of voice port (always “FXS” for the Cisco uBR924 router).
- Operation State—The current functional status of the voice port:

  - UP—The port is online and currently making a call.
  - DOWN—The port is online but is not currently making a call.
  - TESTING—The port is in the middle of a test procedure, either its power-on self-test or a test manually initiated by a technician.
  - UNKNOWN—The port is an unknown state. This might indicate you are using an out of date software image.
  - DORMANT—The port is not currently in use.
  - NOT PRESENT—The port is not present. Either the voice port hardware has failed or a software image with voice support has been loaded on a Cisco cable access router that does not support voice ports.
- Administrative State—The configuration of the voice port:
  - UP—The port is enabled and ready to accept and make calls.
  - DOWN—The port is disabled and cannot accept or make calls.
  - TESTING—The port has been put into test mode, typically by a technician who is manually testing the port.
- Interface Down Failure—Whether the voice port is currently experiencing an interface down failure.
- Noise Regeneration—Whether background noise should be played to fill silent gaps.
- Non Linear Processing—Whether non-linear echo cancellation is enabled for this port.
- Music on Hold Threshold—The current music-on-hold threshold (-7 0dB to -30 dB) for the port.
- In Gain—The amount of input gain (-6 dB to 14 dB) inserted at the receiver side of the port.
- Out Attenuation—The amount of output attenuation (0 dB to 14 dB) inserted at the transmit side of the port.
- Echo Cancellation—Whether echo cancellation is enabled for this port.
- Echo Cancel Coverage—The amount of time to be covered with echo cancellation (8, 16, 24, or 32 milliseconds)
- Connection Mode—The connection mode of the voice port.
- Connection Number—The full E.164 telephone number used to establish a connection.
- Initial Time Out—The maximum amount of time the port waits for an initial input digit after going off-hook (0 to 120 seconds).
- InterDigit Time Out—The maximum DTMF interdigit duration (0 to 120 seconds).
- Call Disconnect Time Out—The maximum amount of time the port waits to disconnect a call after the remote side hangs up (0 to 120 seconds).
- Region Tone—The type of ringing tone (cptone) generated by the port, as defined by locale (2-letter ISO-3166 country code).

CPE State Information

This page summarizes how the Cisco uBR924 router has been configured at the MAC (physical) layer. Figure B-4 shows a typical CPE State Information page.

Figure B-4 CPE State Information Page



The following information is shown in the CPE State Information page:

- Router Name—Shows the hostname assigned to the router.
- IP Address—Shows the IP address assigned to the router's cable interface.
- Net Mask—Shows the subnet mask for the cable interface.
- MAC State—Indicates the current MAC layer state (during normal operation, this is "maintenance_state"). The following are the possible MAC layer states; they correspond to the states shown in the Initialization Information page:
  - wait_for_link_up_state—Wait for Link Up state
  - ds_channel_scanning_state—Downstream Channel Scanning state
  - wait_ucd_state—Wait for UCD state
  - wait_map_state—Wait for MAP state
  - ranging_1_state—Ranging 1 state

  - ranging_2_state—Ranging 2 state
  - dhcp_state—DHCP state
  - establish_tod_state—Time of Day state
  - security_association_state—Security Association state
  - configuration_file_state—Download Configuration File state
  - registration_state—Registration state
  - establish_privacy_state—Establish Privacy state
  - maintenance_state—Maintenance state
- Ranging SID—The SID assigned to the router by the CMTS.
- Registered—Indicates whether the router successfully registered with the CMTS.
- Privacy Established—Indicates whether the router established a BPI security session with the CMTS.
- TFTP Server IP Address—Shows the IP address for the TFTP server that downloaded the DOCSIS configuration file to the router.
- Time Server IP Address—Shows the IP address for the ToD server that provided the correct time-of-day to the router.
- Time Zone Offset—Shows the time zone that the router has been configured to use.
- Downstream Info—Click this link to display the following downstream characteristics:
  - DS ID—The Downstream ID assigned to the router.
  - DS Frequency—The frequency in MHz of the downstream assigned to the router.
  - DS Symbol Rate—The symbol rate currently used on the downstream.
  - DS QAM Mode—The bandwidth used on the downstream (64 QAM or 25 6QAM).
  - Signal-to-Noise Ratio Estimate—The current SNR calculated for the downstream.
  - DS Lock Threshold—The minimum SNR signal that the router requires to maintain a lock on the downstream signal.
- Upstream Info—Click this link to display the following upstream characteristics:
  - US ID—The Upstream ID assigned to the router.
  - US Frequency—The frequency in MHz of the upstream assigned to the router.
  - US Power Level—The target power level that the router should be using on the upstream.
  - US Symbol Rate—The symbol rate currently used on the upstream.
  - Ranging Offset—The delay correction, in units of 6.25 microseconds, that the router must apply to the CMTS Upstream Frame Time to synchronize upstream transmissions.
  - Mini-Slot Size—The size of the DOCSIS mini-slots in units of 6.25 microseconds. Possible values are 2, 4, 8, 16, 32, 64, or 128.
  - Change Count—The DOCSIS configuration change count, which tracks how many times the UCD parameters for a router have changed.
- Configuration File Info—Click this link to display the contents of the DOCSIS configuration file that the router downloaded during its power-on provisioning.

Cable Interface Information

The Cable Interface Information page provides information on the Cisco uBR924 router's cable interface and the quality of its signal. When the cable interface is not operational, the information provided is based on the live values last available.

Figure B-5 shows a typical Cable Interface page.

Figure B-5 Cable Interface Information Page

The following information is displayed on the Cable Interface page:

- IP Address—The IP address assigned to the cable interface during DOCSIS provisioning.
- Network Mask—The subnet mask assigned to the cable interface during DOCSIS provisioning.
- MAC Address—The MAC (physical) layer address assigned to the router at the factory.
- Signal Quality—The signal quality interprets the signal-to-noise ratio (SNR) as follows:
  - Unreliable link (displayed in red)—SNR is 2,000 above the lock threshold; the link is likely to fail or go offline intermittently.
  - Poor link (displayed in yellow)—SNR is 4,000 above the lock threshold; the link may occasionally go offline intermittently.
  - Acceptable link (displayed in green)—SNR is 6,000 above the lock threshold; the link is good.

- Signal to Noise Ratio Estimate—The current SNR value used to determine the Signal Quality.
- Lock Threshold—The lock threshold value used to determine the Signal Quality.
- Power Level—The current upstream power level that the router is using.

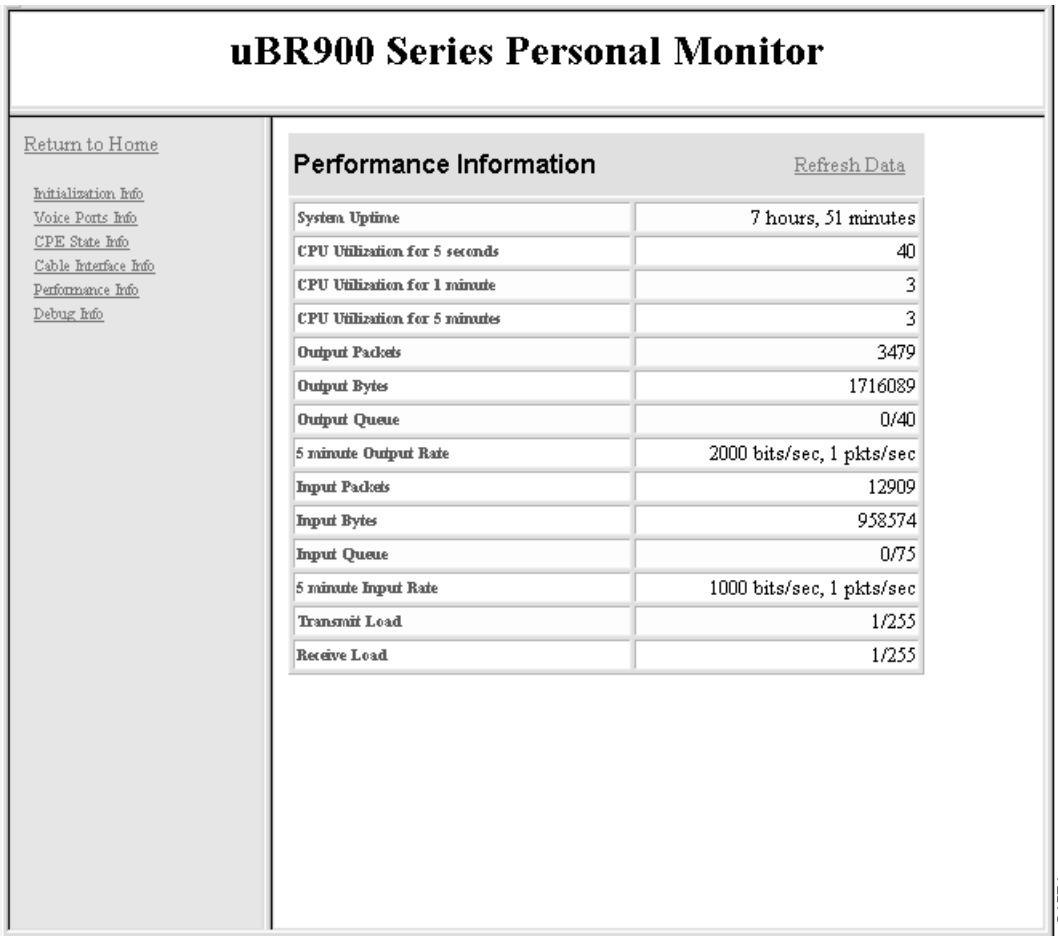
The following are errors encountered by the router at the MAC layer:

- Mac Resets—The number of times that the router has reset its MAC layer.
- Sync Lost—The number of times that the router has lost sync on the cable interface and the link has gone down.
- Invalid Maps—The number of invalid MAPs that the router has received from the CMTS.
- Invalid UCDs—The number of invalid UCDs that the router has received from the CMTS.
- Invalid Ranging Response—The number of invalid ranging responses that the router has received from the CMTS.
- Invalid Registration Response—The number of invalid registration responses that the router has received from the CMTS. Typically, an invalid registration response is due to either an authentication failure or a class of service failure.
- T1 Timeouts—The number of times that the router timed out waiting for a UCD message from the CMTS.
- T2 Timeouts—The number of times that the router timed out waiting for a broadcast ranging response from the CMTS.
- T3 Timeouts—The number of times that the router timed out waiting for a ranging response from the CMTS.
- T4 Timeouts—The number of times the router has reinitialized its MAC layer because it did not receive a Periodic Ranging opportunity from the CMTS.
- Range Aborts—The number of times that the CMTS has instructed the router to abort a ranging attempt, typically because of excessive ranging or excessive power levels.

Performance Information

This page is available to all users and provides basic performance statistics for the Cisco uBR924 router. Figure B-6 shows a typical Performance Information page.

Figure B-6 Performance Information Page



The following information is displayed on the Performance Information page:

- System Uptime—The total time since the router was last reset or powered on.
- CPU Utilization for 5 seconds—The average CPU load (0 to 100%) for the past 5 seconds.
- CPU Utilization for 1 minute—The average CPU load (0 to 100%) for the past 1 minute.
- CPU Utilization for 5 minutes—The average CPU load (0 to 100%) for the past 5 minutes.
- Output Packets—The total number of MAC layer packets output on the upstream at the cable interface.
- Output Bytes—The total number of bytes output on the upstream at the cable interface.
- Output Queue—The current state of the output queue, shown as a ratio of the number of packets currently in the queue over the maximum size of the queue.

- 5 minute Output Rate—The average output rate over the past five minutes, in both bits per second and packets per second. For example, “10/40” shows that 10 packets are currently in the queue, which can hold 40 packets.
- Input Packets—The total number of MAC layer packets received on the downstream at the cable interface.
- Input Bytes—The total number of bytes output on the downstream at the cable interface.
- Input Queue—The current state of the input queue, shown as a ratio of the number of packets currently in the queue over the maximum size of the queue. For example, “13/75” shows that 13 packets are currently in the queue, which can hold 75 packets.
- 5 minute Input Rate—The average input rate over the past five minutes, in both bits per second and packets per second.
- Transmit Load—The current transmit load, shown as a ratio of the packets currently in the transmit buffer over the size of the buffer.
- Receive Load—The current receive load, shown as a ratio of the packets currently in the receive buffer over the size of the buffer.

Debug Information Page

This page displays the output of the **show tech-support** command, which includes the output of the following CLI commands:

- **show version**—Displays the hardware configuration, software image names and version, register settings, and the boot image.
- **show running-config**—Displays the configuration the router is currently using.
- **show stacks**—Displays the stack usage of the router's processes and interrupt routines, including the reason for the last system reboot.
- **show interfaces**—Displays the status and configuration of the router's Ethernet and cable interfaces.
- **show controllers**—Displays the current state, configuration, and register information for each controller that the Cisco uBR924 router uses to move data between the cable and Ethernet interfaces.
- **show controller c0 mac state**—Displays the MAC layer configuration for the cable interface.
- **show voice port**—Displays the configuration of each voice port.
- **show dial-peer voice**—Displays the remote and local dial-peers that have been configured on the router.
- **show gateway**—Displays the gateway configuration (if any).
- **show call active voice**—Displays the contents of the active call table, which shows statistics for the voice calls currently in progress.
- **show call history voice**—Displays the call history table, which lists all voice calls connected through the router's voice ports.
- **show region**—Displays information about the memory regions in the router.
- **show process memory**—Displays details about how tasks are using the router's memory.
- **show process cpu**—Displays details about how tasks are using the router's CPU.
- **show buffers**—Displays the usage of the different memory buffers on the router.

If an enable password has been set, the user must enter the level 15 user ID and password to access this page. If no enable password has been set, this page is accessible to all users.

Note Cisco recommends that an encrypted enable password be set on all Cisco uBR924 routers that are deployed at subscriber sites. If an encrypted enable password is not being used at a subscriber's site, the Cable Monitor should not be enabled in advanced mode because the Debug Information page displays information, such as the SNMP community strings, that could be used to defeat the router's security.

Figure B-7 shows a typical Debug Information page.

Figure B-7 Debug Information Page

Using the ROM Monitor

This appendix describes the Cisco uBR924 cable access router ROM monitor, which helps you isolate and troubleshoot possible hardware problems when installing the router. The ROM monitor is the first software to run when the Cisco uBR924 router is powered-on or reset; it is permanently part of the Cisco uBR924 router and is always available, regardless of the release of Cisco IOS software that has been downloaded to the router.

This appendix describes:

Caution Users and system administrators do not need to access the ROM monitor during normal operation of the Cisco uBR924 router. The ROM monitor should be used only by trained service technicians or under the direction of a Cisco TAC engineer. Many of the commands available in the ROM monitor put the router in a diagnostic or non-functional state—do not enter any commands in the ROM monitor unless you thoroughly understand their function and how to reverse their effects so you can restore the router to normal operations.

Entering the ROM Monitor

The ROM monitor initializes the processor hardware and boots the main operating system software. The ROM monitor version introduced in the Cisco IOS Release 12.0(4)XI timeframe displays as follows:

```
rommon 2 > i
System Bootstrap, Version 12.0(19990506:181223)[sjacobso-jac-xi26 2504] DEVELOPMENT
SOFTWARE
Copyright (c) 1994-1999 Cisco Systems, Inc.
UBR924 platform with 16384 Kbytes of main memory
```

The ROM monitor main memory information is shown below:

```
 rommon 3 > meminfo
Main memory size: 16 MB
Available main memory starts at 0x14000, size 16304 KB
I/O (packet) memory size: 512 KB
NVRAM size: 16 KB
```

To default to booting at the ROM monitor while running the system software, reset the configuration register to 0x0 by entering the following Cisco IOS global configuration command:

Router(config)# **config-reg 0x0**

The new configuration register value, 0x0, takes effect after the router is rebooted with the **reload** Privileged EXEC command. If you set the configuration to 0x0, you will have to manually boot the system from the console each time you reload the router.

Note After you have entered the ROM monitor, you can return to the normal boot mode by changing the configuration register value to **0x2103**, using the **confreg 0x2102** ROMMON command. Then reboot the system using the **reset** ROMMON command.

Command Conventions

Following are ROM monitor command conventions:

- Brackets [ ] denote an optional field. If a minus option is followed by a colon (for example: [-s:]), you must provide an argument for the option.
- A word in italics means that you must fill in the appropriate information.
- All address and size arguments to the memory-related commands are assumed to be hexadecimal (no “0x” prefix or “h” suffix needed).
- The options [-bwl] for the memory-related commands provide for byte, word, and longword operations. The default is word.
- You can invoke the memory-related commands by typing the command with no arguments. This causes the utility to prompt you for parameters. This option is available for the commands marked as prompting.
- You can place more than one command (except the repeat command) on a line by using the “;” delimiter.

Commands

Enter **?** or ***help*** at the *rommon* > prompt to display a list of available commands and options:

```
rommon 12 > help

alias               set and display aliases command
boot                boot up an external process
confreg             configuration register utility
cont                continue executing a downloaded image
context             display the context of a loaded image
cookie              display contents of cookie PROM in hex
dev                 list the device table
dir                 list files in file system
dnld                serial download a program module
frame               print out a selected stack frame
help                monitor builtin command help
history             monitor command history
meminfo             main memory information
repeat              repeat a monitor command
reset               system reset
set                 display the monitor variables
stack               produce a stack trace
sync                write monitor environment to NVRAM
```

```
sysret              print out info from last system return
unalias             unset an alias
unset               unset a monitor variable
xmodem              x/ymodem image download
```

Note You can display additional details for a command by entering the command name with a **-?** option, which prints the command usage message.

The commands are listed and described in alphabetical order. Note that the ROM monitor commands are case-sensitive.

- **alias** [name=value]—Aliases a name to a value. The ROM monitor's version of command aliasing is based on the aliasing function built into the Korn shell. Aliasing allows you to abbreviate commands or to set up a command so that it is automatically run with certain options.

  If the value contains white space or other special characters, it must be quoted. If the value has a space as the last character the next command line word is also checked for an alias (normally only the first word on the command line is checked).

  The **alias** command is used to set new aliases and to view the aliases that are currently defined. For example, to display the currently set aliases, enter the alias command by itself:

  ```
  rommon 1 > alias
  r=repeat
  h=history
  ?=help
  b=boot
  ls=dir
  ```

  The following command creates the alias "bf" that performs the "boot from Flash memory" command:

  ```
  rommon 1 > alias bf "b flash:"
  ```

- **boot** or **b**—Boots an image. The **boot** command with no arguments boots the first image in boot Flash memory. You can include an argument, *filename*, to specify a file to be booted over the network using the Trivial File Transfer Protocol (TFTP). The local device (see the description of **b** *device* following) can be specified by entering the device specifier (*devid*). If the specified device name is not recognized by the ROM monitor, the system will attempt to boot the image (*imagename*) from a network TFTP server. Do not insert a space between *devid* and *imagename*. Options to the boot command are -x, load image but do not execute, and -v, verbose. The form of the **boot** command follows:

  boot [-xv] [*devid*] [*imagename*]

  b—Boots the default (first) system software.

  b *filename [host]*—Boots using a network TFTP server. When a host is specified, either by name or IP address, the boot command will boot from that source.

  b flash:—Boots the first file in Flash memory.

  b *device:*—Boots the first file found in the Flash memory device. The Flash memory device specified can be either *flash*:, to boot the Cisco IOS software, or *bootflash*:, to boot the boot image in Flash memory.

  b *device:name*—An extension of the above command, allows you to specify a particular filename in the Flash memory.

- **confreg** [*hexnum*]—Executing the **confreg** command with the argument *hexnum* changes the virtual configuration register to match the hex number specified. Without the argument, **confreg** dumps the contents of the virtual configuration register in English and allows the user to alter the contents. You are prompted to change or keep the information held in each bit of the virtual configuration register. In either case, the new virtual configuration register value is written into non-volatile memory (NVRAM, also known as Flash memory) and does not take effect until you reset or power cycle the router.

  The configuration register resides in Flash memory. The configuration register is identical in operation to other Cisco access servers. Enter **confreg** for the menu-driven system, or enter the new value of the register in hexadecimal.

Note The value is always interpreted as hexadecimal. The **confreg** utility will print a before and after view of the configuration register when used in menu-driven mode.

For example:

```
rommon 7 > confreg

 Configuration Summary
enabled are:
console baud: 9600
boot: the ROM Monitor

do you wish to change the configuration? y/n  [n]:  y
enable  "diagnostic mode"? y/n  [n]:  y
enable  "use net in IP bcast address"? y/n  [n]:
enable  "use all zero broadcast"? y/n  [n]:
enable  "ignore system config info"? y/n  [n]:
change console baud rate? y/n  [n]:  y
enter rate: 0 = 9600, 1 = 4800, 2 = 1200, 3 = 2400  [0]:  0
change the boot characteristics? y/n  [n]:  y
enter to boot:
 0 = ROM Monitor
 1 = the boot helper image
 2-15 = boot system
[0]:  0

 Configuration Summary
enabled are:
diagnostic mode
console baud: 9600
boot: the ROM Monitor

do you wish to change the configuration? y/n  [n]:

You must reset or power cycle for new config to take effect.
```

- **cont** [*-b*]**—**Continues a loaded image that has stopped. For example:

```
reboot> launch
 monitor: command "launch" aborted due to user interrupt
diagmon 7 > cont

reboot >
```

- **context—**Displays the CPU context at the time of the fault. The context from the kernel mode and process mode of a booted image is displayed, if available. For example:

```
rommon 6 > context
CPU Context:
```

```
d0 - 0x00000028      a0 - 0x0ff00420
d1 - 0x00000007      a1 - 0x0ff00000
d2 - 0x00000007      a2 - 0x02004088
d3 - 0x00000000      a3 - 0x020039e6
d4 - 0x00000000      a4 - 0x02002a70
d5 - 0x02003e8a      a5 - 0x02003f17
d6 - 0x00000000      a6 - 0x02003938
d7 - 0x00000001      a7 - 0x0200392c
pc - 0x02004adc     vbr - 0x02000000
```

- **cookie**—Displays the contents of the cookie PROM in hexadecimal format. For example:

```
rommon 1 > cookie
cookie:
01 01 00 00 0c 07 af 80 07 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

- **dev**—Lists boot device identifications on the router. For example:

```
rommon 10 > dev
Devices in device table:
   id  name
eprom:  eprom
flash:  PCMCIA slot 1
```

- **dir** *devid***—**Lists the files on the named device. For example:

```
rommon 11 > dir flash:
   File size                Checksum      File name
       65 bytes (0x41)       0xb49d       clev/oddfiles65
  2229799 bytes (0x220627)   0x469e       C5200-k.z
```

- **dlnd** [*-xv:*] [*args*]—Downloads in binary format through the console and executes. The -x option downloads, but does not execute. The -v option allows you to specify the verbose level. The optional arguments are passed to the downloaded program via the argc/argv mechanism (only when -x is not used). The exit value is the return value from the downloaded routine or the status of the download operation (success or failure) if the -x option is used.
- **frame [*number*]**—Displays an entire individual stack frame. Enter a number to indicate which frame to display. You can also specify a number to indicate which stack frame to display. Note that the default is 0 (zero), which is the youngest frame. For example:

```
rommon 6 > frame 2
Frame 02: FP = 0x02003960    RA = 0x020050ee
at 0x02003968 (fp + 0x08) = 0x02004f8d
at 0x0200396c (fp + 0x0c) = 0x0200f390
at 0x02003970 (fp + 0x10) = 0x02006afc
at 0x02003974 (fp + 0x14) = 0xc0a82983
at 0x02003978 (fp + 0x18) = 0x02003a7e
at 0x0200397c (fp + 0x1c) = 0x02002630
at 0x02003980 (fp + 0x20) = 0x00000000
at 0x02003984 (fp + 0x24) = 0x02000000
at 0x02003988 (fp + 0x28) = 0x0200c4a4
at 0x0200398c (fp + 0x2c) = 0x0200f448
```

- **history** or **h**—Displays the command history, that is, the last 16 commands executed in the monitor environment.
- **meminfo**—Displays the size (in bytes) the starting address, the available range of the main memory, the starting point and size of packet memory, and the size of non-volatile Flash memory. For example:

```
rommon 9 > meminfo
```

```
Main memory size: 8 MB. Packet memory size: 4 MB
Available main memory starts at 0xa000e001, size 0x7f1fff
Packet memory starts at 0xa8000000
NVRAM size: 0x20000
```

- **repeat [*number or string*] [*count*] or r**—Repeats the specified command. Without an argument, repeats the last command. The optional command number (from the history list) or match string specifies which command to repeat. In the case of the match string, the most recent command to begin with the specified string will be re-executed. If the string includes spaces, you must define it using quotes. The count option allows you to repeat the command more than once.
- **reset** or **i**—Resets and initializes the system, similar to power-on.
- **set**—Displays all the monitor variables and their values.
- **stack** *[num]*—Produces a stack trace of the num frames. The default is 5. The command dumps from the kernel stack and the process stack (if one is available) of a booted image. For example:

```
rommon 5 > stack 8
Stack trace:
PC = 0x02004adc
Frame 00: FP = 0x02003938    RA = 0x02005f2a
Frame 01: FP = 0x02003948    RA = 0x02005df0
Frame 02: FP = 0x02003960    RA = 0x020050ee
Frame 03: FP = 0x02003994    RA = 0x02004034
Frame 04: FP = 0x02003b00    RA = 0x00012ca6
```

- **sync**—Writes the working in-core copy of the environment variables and aliases to Flash memory so that they are read on the next reset.
- **sysret**—Displays the return information from the last booted system image. This includes the reason for terminating the image, a stack dump of up to eight frames, and if an exception is involved, the address where the exception occurred. For example:

```
rommon 8 > sysret
System Return Info:
count: 19,  reason: reset
pc:0x60043754,  error address: 0x0
Stack Trace:
FP: 0x80007e78, PC: 0x60043754
FP: 0x80007ed8, PC: 0x6001540c
FP: 0x80007ef8, PC: 0x600087f0
FP: 0x80007f18, PC: 0x80008734
```

- **unalias** ***name***—Removes name and its associated value from the alias list.

New and Changed Commands Reference

All cable-specific commands for the Cisco uBR924 cable access router in Cisco IOS Release 12.2(8) and later releases are described in the *Cable CPE Commands* chapter in the *Cisco Broadband Cable Command Reference Guide*, available on Cisco.com and the Customer Documentation CD-ROM. This chapter is regularly updated to include all command changes and additions.

Note To locate the documentation for the "related commands" mentioned in this chapter, use the Cisco IOS Release 12.2 command reference master index that is available on Cisco.com and the Documentation CD-ROM.

Commands Reserved for DOCSIS Use

In Cisco IOS Release 12.1(2)T and later releases, the following commands were removed from the CLI:

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

In Cisco IOS Release 12.1(2)T and later software releases, these commands are now reserved exclusively for DOCSIS use. These commands can appear in the router's Cisco IOS configuration file, but they cannot be given through the router's CLI.

Symbols

Numerics

A

B

C

D

E

F

G

H

I

L

M

N

O

P

Q

R

S

T

U

V