Overview

This chapter provides a basic understanding of the Cisco uBR905 and Cisco uBR925 cable access routers' software feature sets, as well as the processes used for provisioning the routers within a cable network and configuring them for different services. This chapter contains the following sections:

Note This manual describes the Cisco uBR905 and Cisco uBR925 cable access routers and feature sets as they exist in Cisco IOS Release 12.2(8)T.

Cisco IOS Software Release Feature Sets

The Cisco uBR905 and Cisco uBR925 cable access routers support 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 cable access router to transmit data traffic over the Hybrid Fiber Coax (HFC) cable network.

The Cisco uBR925 cable access router also supports voice traffic, 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 uBR925 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 uBR925 cable access router can route their calls over the Internet using either the H.323v2 (Gateway/Gatekeeper), Simple Gateway Control Protocol (SGCP), and Media Gateway Control Protocol (MGCP) 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 feature sets support data-only traffic for the Cisco uBR905 cable access router and both data and voice traffic for the Cisco uBR925 cable access router:

- 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 feature set is included in all Cisco IOS images available for the Cisco uBR905 and Cisco uBR925 cable access routers.
- Value Telecommuter —Adds IP routing support, Dynamic Host Configuration Protocol Server (DHCP) support, Network Address Translation and Port Address Translation (NAT/PAT), 56-bit DES IPSec encryption, and layer 2 tunneling support to DOCSIS-compliant bridging. 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. This is the default software image for the Cisco uBR905 and Cisco uBR925 cable access routers.
- Performance Telecommuter —Adds advanced 168-bit 3DES 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 the Cisco Secure Integrated Software (firewall) feature set to the functions provided by the Value Telecommuter image. This allows customers to establish secure connections across the Internet. This feature set also protects the office network from intrusion and interference and preserves the permanent high-speed access to the Internet.
- Performance Small and Branch Office—Adds advanced 168-bit 3DES 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 and preserves the permanent high-speed access to the Internet.

The following sections describe the feature sets in each of these categories. Descriptions of the features themselves are in the "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 1.0-compliant IP bridging and DOCSIS Baseline Privacy Interface (BPI) encryption. This 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.

This feature set also supports DOCSIS Baseline Privacy Interface (BPI) encryption, which provides 40-bit or 56-bit encryption of all Ethernet packets sent between the Cisco uBR905 and Cisco uBR925 cable access routers and the CMTS. BPI encryption provides a basic level of security for all information sent by CPE devices over the cable interface.

DOCSIS-compliant bridging (also referred to as "plug-and-play" bridging) is available in all images for the Cisco uBR905 and Cisco uBR925 cable access routers and is the routers' default configuration. 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 not available as a separate image because its feature set is incorporated in all other available images for the Cisco uBR905 and Cisco uBR925 cable access routers.

In DOCSIS-compliant bridging mode, the router acts as a transparent IP bridge for one or more customer premises equipment (CPE) devices. In this mode, it supports a maximum number of 254 CPE devices.

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 router can connect only one computer to the cable network.

Value Telecommuter

In addition to full DOCSIS 1.0 support (see Base IP DOCSIS-Compliant Bridging), the Value Telecommuter feature set provides the following features:

- Easy IP—This set of features simplifies the administration of IP addresses in a cable network by providing intelligent Dynamic Host Configuration Protocol Server (DHCP) functions, such as DHCP Relay Agent and DHCP Client functionality. The DHCP features provide intelligence and flexibility in the handling and distribution of IP addresses for the PCs and other CPE devices connected to the cable network.

  This feature set also supports Network Address Translation and Port Address Translation (NAT/PAT). The NAT/PAT features allow the customer to use private IP addresses on the local network, while still maintaining connectivity to the Internet.

- IPSec encryption—This feature 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. By default, the Cisco uBR905 and Cisco uBR925 cable access routers automatically use their onboard hardware accelerator for all IPsec encryption, which greatly improves the performance over software-based encryption.

Note IPSec encryption is in addition to BPI encryption. BPI encryption is done only on the traffic between the 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.

- Layer 2 Tunneling Protocol (L2TP)—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 essential components for virtual private networks (VPNs).

The Value Telecommuter features allow employees to establish secure high-speed Internet connections between the employees' homes and the business' local area network (LAN).

Performance Telecommuter

The Performance Telecommuter feature set includes all 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 IOS Firewall feature set to the DOCSIS 1.0 support, Easy IP, and 56-bit IPSec encryption feature sets, providing a wide range of security features for the Cisco uBR905 and Cisco uBR925 cable access routers. The 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.

Performance Small and Branch Office

The Performance Small and Branch Office feature set includes all the features found in the Value Small and Branch Office image, but adds 168-bit IPSec Triple Data Encryption Standard (3DES) encryption. This feature set allows employees who work with very sensitive information, such as medical and banking records, to work at home or a remote branch office, without compromising the integrity of the data that is transmitted over the network.

Feature Descriptions

This section describes the particular features that are contained in the feature sets supported by the Cisco uBR905 and Cisco uBR925 cable access routers. See the Release Notes for any particular release for information on which features are contained in a particular Cisco IOS image.

Authentication, Authorization, and Accounting

The authentication, authorization, and accounting (AAA) feature allows centralized servers to provide user authentication, authorization, and accounting. Compared to router-based authentication, AAA provides for increased flexibility and control of access configuration, scalability, the possibility of multiple backup servers, and standardized authentication methods, such as RADIUS. The type of authentication and authorization can be defined by creating method lists, and then applying those method lists to specific services or interfaces. More information on AAA is available in the Cisco IOS Security Configuration Guide, Release 12.2.

The AAA feature is supported in Cisco IOS Release 12.2(8)T and later 12.2 T releases.

Cable Monitor Web Diagnostics Tool

The Cable Monitor is a web-based diagnostic tool used to display the current status and configuration of the Cisco uBR905 and Cisco uBR925 cable access routers. 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 described in detail in Appendix B, “Using the Cable Monitor Tool.”

Cisco Cable Clock Card Support

The Cisco uBR925 cable access router automatically supports the use of the Cisco Cable Clock Card on the Cisco uBR7246 VXR universal broadband router. The Cisco Cable 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 supported only on the Cisco uBR925 cable access router.

Cisco IOS Firewall

The Cisco IOS Firewall feature set provides firewall-specific security features to the Cisco uBR905 and Cisco uBR925 cable access routers. When this feature is enabled, the router acts as a buffer between the Internet and other public networks and the private network that is connected to the router. Security is provided by access lists, as well as by examining incoming traffic for suspicious activity.

The firewall-specific 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 the most 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 only from 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.

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 *Cisco IOS Security Configuration Guide* and *Cisco IOS Security Command Reference* (available on the Documentation CD-ROM and Cisco.com).

DOCSIS-Compliant Bridging

DOCSIS-compliant bridging allows the 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 uBR905 and Cisco uBR925 cable access routers.

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 router and the cable operator's CMTS.

The BPI+ (BPI Plus) feature is an enhancement to the BPI feature and is based on the DOCSIS BPI+ Specification (SP-BPI+-I04-000407 or later revision), which is still in development. In addition to the regular BPI features, BPI+ provides more secure authentication of cable modems through the use of digital certificates. Also, a cable modem can use a digital signature to verify that the software image it has downloaded has not been altered or corrupted in transit.

Note The Cisco uBR925 cable access router contains the digital certificates required for BPI+ operation. However, BPI+ support will not be available until DOCSIS 1.1 is supported in a later release of Cisco IOS software.

Dynamic Host Configuration Protocol Server

The DHCP server on the 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.

Dynamic Host Configuration Protocol Proxy Support

The DHCP Proxy Support feature is useful in two situations:

- When the 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 assigning 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 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 described in detail in Appendix D, "New and Changed Commands Reference."

Enhanced Bridging

The Cisco uBR905 and Cisco uBR925 cable access routers can transparently bridge IP traffic between their cable interface and their four RJ-45 hub ports with 10BaseT Ethernet connectivity. Up to four coemputers can be directly connected to these hub ports. Additional computers can be connected to the 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. The Cisco uBR925 cable access router also supports enhanced bridging to the PC connected to its USB interface.

A maximum of 254 devices can be bridged in bridging mode, but no limit exists when the cable access router is operating in routing mode.

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 otherwise set. In this situation, the router can connect only one computer to the cable network, regardless of the actual number of computers that are connected to the router.

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 uBR925 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.

This feature is supported only for the Cisco uBR925 cable access router.

Note For more information on this feature, see the *Ecosystem Gatekeeper Interoperability Enhancements, Phase 2* feature module, available on Cisco.com 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 uBR925 router can be connected to either fax machines or voice telephones, allowing fax traffic to be sent as VoIP traffic.

This feature is supported only for the Cisco uBR925 cable access router.

H.323v2 (Gateway/Gatekeeper)

The Cisco uBR925 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 uBR925 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 and G.723.1) 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 Cisco.com 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 description of the **h323-gateway voip bind srcaddr** command for more information. In addition, the value of the H.225 TCP connection timeout timer is configurable.

This feature is supported only on the Cisco uBR925 cable access router.

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 uBR905 and Cisco uBR925 cable access routers.

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.

By default, the Cisco uBR905 and Cisco uBR925 cable access routers use their onboard hardware accelerator for all IPsec encryption and decryption. This offers greatly increased performance over software-based encryption techniques.

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 Layer 2 Forwarding (L2F) and Microsoft 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).

Note Cisco IOS Release 12.2(2)XA1, 12.2(2)T, or greater is required to support GRE IP tunnels.

Media Gateway Control Protocol

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 Simple Gateway Control Protocol (SGCP) 1.1 protocol. The MGCP 0.1 and SGCP 1.1 protocols have been merged on the Cisco uBR925 router so that the router can respond efficiently to either protocol.

The Cisco uBR925 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 uBR925 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 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 Cisco.com and the Documentation CD-ROM.

This feature is supported only on the Cisco uBR925 cable access router.

NetRanger Support—Cisco IOS Intrusion Detection

The Cisco uBR905 and Cisco uBR925 cable access routers support 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 Software Release 12.1(5)XT.

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 uBR905 and Cisco uBR925 cable access routers translate 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 router uses a unique port address to identify individual computers on the private network.

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 traffic usefulness.

Depending on the software image used, the Cisco uBR905 and Cisco uBR925 cable access routers support 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 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.

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 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 cable access 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 cable access router creates a SID that has the QoS parameters needed for that particular voice call. When the call ends, the router deletes the SID, releasing its bandwidth for use elsewhere.

Note Both the 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, Cisco IOS Release 12.1(1)T, or later is required on the Cisco uBR7200 series router to use these features.

Routing Information Protocol Version 2

When configured for routing mode, the Cisco uBR905 and Cisco uBR925 cable access routers default to using the Routing Information Protocol Version 2 (RIPv2). In routing mode the cable access router automatically configures itself to use the headend's IP address as its IP default gateway. This allows the 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.

Note The Cisco uBR905 and Cisco uBR925 cable access routers support only static routes and the RIPv2 routing protocol.

Secure Shell Version 1

The Cisco uBR905 and Cisco uBR925 cable access routers support 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. The cable access router can function as both an SSH server and an SSH client.

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 client must also support the same level of encryption.)

This feature is documented in the *Secure Shell Version 1 Support* feature module, available on Cisco.com 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 uBR925 cable access router functions as an SGCP residential gateway (RGW), not as the trunking gateway (TGW), which controls the telephone call.

Note The Cisco uBR925 cable access router supports both H.323 and SGCP call control, but only one method can be active at a time.

This feature is supported only on the Cisco uBR925 cable access router.

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.

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 12.2(2)XA1, 12.2(2)T, or greater is required to support GRE IP tunnels.

Universal Serial Bus Interface

The Cisco uBR925 cable access router supports a network connection to a PC using the Universal Serial Bus (USB) interface. This allows the router to connect to a PC with a USB interface, without having to open the unit and install an Ethernet network interface card (NIC). If supported by the PC and service provider, PCs can be connected to the router using both the Ethernet and USB interfaces.

In bridging mode, the USB and Ethernet interfaces both transparently bridge IP traffic over the cable interface. In routing mode, the USB and Ethernet interfaces can be separately routable.

Note The PC must be running Windows 98, Windows 98 Second Edition, Windows 2000, or Windows Millennium. Windows 95 and Windows NT do not support networking connections through a USB interface.

This feature is supported only on the Cisco uBR925 cable access router.

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 command 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 an IKE negotiation request 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, the firewall 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 requests new security associations if the current ones are expiring (based on the policy specified in the temporary crypto map entry). After all the corresponding security associations expire, the temporary crypto map entry is removed.

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

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 uBR905 and Cisco uBR925 cable access routers typically ship from the Cisco factory ready to work in the Base IP DOCSIS-Compliant Bridging data-only mode. However, before the 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 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 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 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 router initialization and boot time.)
- Any additional configuration on the router can be done in the following ways:

- 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 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 uBR905 and Cisco uBR925 cable access routers arrive 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 uBR905 Cable Access Router Hardware Installation Guide* or the *Cisco uBR925 Cable Access Router Hardware Installation Guide*, available on Cisco.com and the Documentation CD-ROM.

Supporting Multiple Classes of Service

In data-only mode, the Cisco uBR905 and Cisco uBR925 cable access routers typically use only one class of service (CoS) profile that provides best-effort delivery of data traffic. However, certain types of real-time traffic, such as voice traffic, require multiple CoS profiles so that they can be given a higher priority than normal data traffic. This allows the 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 cable access router is registered, using the CoS parameters in the DOCSIS configuration file. To support voice and other services in a DOCSIS 1.0 environment, the service provider typically specifies a primary CoS profile for best-effort data and secondary CoS profiles for higher-priority 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 and handling the MAC and maintenance messages. The other SIDs are secondary SIDs used for the higher-priority traffic, such as voice 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 uBR905 and Cisco uBR925 cable access routers are running DOCSIS 1.0+ software, the router does not need to request additional SIDs at registration time. Instead, the router can send an Unsolicited Grant (UG) request to the CMTS, which responds by assigning a SID for the additional traffic flow. This dynamically-created SID is assigned a secondary CoS profile that matches the type of traffic being sent. When that traffic ends, 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 usually must create and maintain multiple CoS profiles. Typically, different CoS profiles are used for voice and fax traffic, as well as other forms of real-time traffic, because these services have different service requirements.

The provider could either assign the same CoS profiles for all users, or create a number of different CoS profiles that provide different levels of service, depending on the services purchased. The 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 Cisco.com 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. UR addresses the needs of the following classes of users in the provisioning system implemented by the customer (typically a service provider):

- Subscriber—Signs up for network services for the first time, or augments existing services. The set of options for the subscriber is determined by the customer and changes between customers, even in the same industry.
- Administrator—Generates reports for individual users, generates system wide reports, and resolves provisioning system problems that subscribers may have.

- Configurer—Is responsible for making modifications to the templates and workflows that define a customer's solution. This role can also involve building interfaces to the customer's existing business systems.

UR 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 customized as needed to suit customer needs.
- Cable modem reset using SNMP.
- Preliminary set of Network Access Server (NAS) extensions to communicate with supported backend customer systems. This includes interfaces to a central LDAP directory and Network Registrar (using 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 cable access router using TFTP as part of the normal modem registration process.

MR includes the following features:

- Policy-based dynamic creation of DOCSIS configuration files
- Web-based user interface to define the policies for creating configuration files
- 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.

Cisco Network Registrar includes the following features:

- 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 uBR905 and Cisco uBR925 cable access routers, which are two-way devices that do not require telco-return services.