CHAPTER 1

Overview of Cisco uBR7200 Series Software

The Cisco uBR7200 series uses Cisco IOS® software to offer enhanced stability, features, performance and investment protection. This chapter summarizes system and software features of the Cisco uBR7200 series Cable Modem Termination System (CMTS). This chapter contains the following sections:

Section	Purpose
"Cisco IOS Releases and Images for the Cisco uBR7200 Series," page 2	Describes the supported Cisco IOS release trains, associated features, and latest Cisco IOS images for each recently supported train. One early step in CMTS feature configuration is to verify your Cisco IOS release train, the associated image and feature set. This section guides you in determining such information.
"Cisco uBR7200 Series Chassis Overview," page 8	Describes the Cisco uBR7200 series routers, and their supported hardware features and interoperability.
"Cisco uBR7200 Series Router Configuration Overview," page 15	Provides an overview of the hardware and interfaces that typically require configuration through Cisco IOS software.
"Supported Software Features for the Cisco uBR7200 Series," page 22	Describes the features and configuration utilities that are available on the Cisco uBR7200 series.
"DOCSIS and CMTS Interoperability," page 137	Provides an overview of DOCSIS NTSC and EuroDOCSIS cable plants, DOCSIS-compliant signals, and traffic engineering.

Cisco IOS Releases and Images for the Cisco uBR7200 Series

This section describes the supported releases, latest images, memory requirements, and major software features for the following Cisco IOS software:

- Determining Your Cisco IOS Software Release
- Upgrading to a New Software Release
- 12.3 BC Release Train Images and Requirements
- 12.2 BC Release Train Images and Requirements
- 12.2 CX Images and Requirements
- 12.1 EC Images and Requirements

To configure the CMTS for the first time, refer to Chapter 2, "Configuring the Cable Modem Termination System for the First Time."

For additional release information, refer to the *Cisco uBR7200 Series Software Release Notes* on Cisco.com:

http://www.cisco.com/en/US/docs/cable/cmts/ubr7200/release/notes/12_3bc/123BCu72.html

Determining Your Cisco IOS Software Release

To determine the version of Cisco IOS software running on the Cisco uBR7200 series universal broadband router, log in to the router and enter the **show version** command in User or privileged EXEC mode.

```
Router> show version

Cisco Internetwork Operating System Software
IOS (tm) Cisco IOS 12.2 BC Software (ubr7200-is-mz), Version Cisco IOS Release 12.2(4)BC1,
RELEASE SOFTWARE
```

Note Your display may vary according to your release and image.

Upgrading to a New Software Release

An upgrade is an order placed for a Cisco IOS feature set that contains more functionality than the feature set that you are replacing. An upgrade is not an "update." An update consists of installing a more recent version of the *same* feature set.

- **Exception**—If a feature set has been made obsolete, the next closest feature set on a more recent release is considered an update.

For general information about upgrading to a new software release, refer to the *Cisco IOS Upgrade Ordering Instructions* on Cisco.com. Also refer to Appendix A, "Installing or Upgrading Cisco IOS Software."

12.3 BC Release Train Images and Requirements

The Cisco 12.3 BC release train is the latest Cisco IOS release train to support the Cisco uBR7200 Series, and emphasizes additional features and performance specifically for the Cisco uBR7246VXR universal broadband router.

Table 1-2 displays the memory recommendations of the Cisco IOS feature sets for the Cisco uBR7200 series universal broadband routers for Cisco IOS Release 12.3(9a)BC. Cisco uBR7200 series routers are only available with a 48 MB or 128 MB of Flash disk memory on the I/O Controller cards. The UBR7200-NPE-G1 uses compact Flash disk only.

Note Flash disks, an alternative to linear Flash memory, are Flash memory-based devices that can be used as file storage media in the PCMCIA card slots of the I/O Controllers. Each I/O Controller has two PCMCIA slots and can be configured with up to 256 MB of Flash disk memory.

Table 1 Memory Recommendations for the Cisco uBR7200 Series Routers, Cisco IOS Release 12.3(9a)BC Feature Sets

Feature Set	Software Image	Recommended Flash Memory	Recommended DRAM Memory	Runs From
Two-Way Data/VoIP Images				
DOCSIS Two-Way	ubr7200-p-mz	32 MB Flash	256 MB DRAM	RAM
DOCSIS Two-Way IP Plus	ubr7200-is-mz	32 MB Flash	256 MB DRAM	RAM
DOCSIS Two-Way with BPI	ubr7200-k8p-mz	32 MB Flash	256 MB DRAM	RAM
DOCSIS Two-Way IP Plus with BPI	ubr7200-ik8s-mz	32 MB Flash	256 MB DRAM	RAM
DOCSIS Two-Way 3DES	ubr7200-k9p-mz	32 MB Flash	256 MB DRAM	RAM
DOCSIS Two-Way 3DES IP Plus	ubr7200-ik9s-mz	32 MB Flash	256 MB DRAM	RAM
Boot Image				
UBR7200 Boot Image	ubr7200-kboot-mz	None	None	—
UBR7200 Boot Image	ubr7200-boot-mz	None	None	—

The image subset legend for Table 1-2 is as follows:

- i = IP routing, MPLS-VPN support, and non-cable interface bridging, including Network Address Translation (NAT)
- k8 = DOCSIS Baseline Privacy
- p = IP routing with Intermediate System-to-Intermediate System (IS-IS) and Border Gateway Protocol (BGP); MPLS-VPN support; no bridging and no NAT
- s = “Plus” features: NAT and Inter-Switch Link (ISL)
- k9 = 3DES level of encryption

Note All images support all of the hardware listed in the “Supported Hardware on the Cisco uBR7200 Series” section on page 1-11, unless otherwise indicated.

Note A Cisco uBR7200 series router requires 256 MB of DRAM memory on the NPE processor card when HCCP redundancy is configured and the router is supporting more than 3,000 cable modems. Using less memory in these conditions results in temporary out-of-memory situations and incomplete synchronization between the Working and Protect interfaces.

12.2 BC Release Train Images and Requirements

Note Cisco IOS release 12.2(4)BC1 offers certified DOCSIS 1.1 support on the Cisco uBR7246 VXR router.

The 12.2 BC train is an interim release train that provides certified DOCSIS 1.1 two-way support on the Cisco uBR7246 VXR universal broadband router, along with support for selected new features. The latest release in this train, Cisco IOS Release 12.2(4)BC1, provides a migration path from the earlier Cisco IOS 12.2 XF releases, which included a subset of the features supported in these Cisco IOS release trains:

- Cisco IOS Release 12.0 SC
- Cisco IOS Release 12.1 EC
- Cisco IOS Release 12.1 CX1

Table 1-2 displays the memory recommendations of the Cisco IOS feature sets for the Cisco uBR7200 series universal broadband routers for Cisco IOS Release 12.2(15)BC1 and 12.2(15)BC2a. Cisco uBR7200 series routers are available with 48 MB or 128 MB of Flash disk memory on the I/O Controller cards. The UBR7200-NPE-G1 uses compact Flash disk only.

Note Flash disks, an alternative to linear Flash memory, are Flash memory-based devices that can be used as file storage media in the PCMCIA card slots of the I/O Controllers. Each I/O Controller has two PCMCIA slots and can be configured with up to 256 MB of Flash disk memory.

Note Cisco IOS release 12.2(4)BC1and later BC releases offer certified DOCSIS 1.1 support on the Cisco uBR7246 VXR router.

Table 1-2 Memory Recommendations for the Cisco uBR7200 Series Routers, Cisco IOS Release 12.2(15)BC1 and 12.2(15)BC2a Feature Sets

Feature Set	Software Image	Recommended Flash Memory	Recommended DRAM Memory	Runs From
Two-Way Data/VoIP Images				
DOCSIS Two-Way	ubr7200-p-mz	16 MB Flash 32 MB Flash[1]	128 MB DRAM	RAM
DOCSIS Two-Way IP Plus	ubr7200-is-mz	16 MB Flash 32 MB Flash[1]	128 MB DRAM	RAM
DOCSIS Two-Way with BPI	ubr7200-k8p-mz	16 MB Flash 32 MB Flash[1]	128 MB DRAM	RAM
DOCSIS Two-Way IP Plus with BPI	ubr7200-ik8s-mz	16 MB Flash 32 MB Flash[1]	128 MB DRAM	RAM
DOCSIS Two-Way 3DES	ubr7200-k9p-mz	16 MB Flash 32 MB Flash[1]	128 MB DRAM	RAM
DOCSIS Two-Way 3DES IP Plus	ubr7200-ik9s-mz	16 MB Flash 32 MB Flash[1]	128 MB DRAM	RAM
Boot Image				
UBR7200 Boot Image	ubr7200-kboot-mz	None	None	—
UBR7200 Boot Image	ubr7200-boot-mz	None	None	—

1. 32 MB of Flash is required for Cisco IOS Release 12.2(15)BC2a and later releases in the Cisco IOS BC train.

The image subset legend for Table 1-2 is as follows:

- i = IP routing, MPLS-VPN support, and non-cable interface bridging, including Network Address Translation (NAT)
- k8 = DOCSIS Baseline Privacy
- p = IP routing with Intermediate System-to-Intermediate System (IS-IS) and Border Gateway Protocol (BGP); MPLS-VPN support; no bridging and no NAT
- s = "Plus" features: NAT and Inter-Switch Link (ISL)
- k9 = 3DES level of encryption

Note All images support all of the hardware listed in the "Supported Hardware on the Cisco uBR7200 Series" section on page 1-11, unless otherwise indicated.

Note A Cisco uBR7200 series router requires 256 MB of DRAM memory on the NPE processor card when HCCP redundancy is configured and the router is supporting more than 3,000 cable modems. Using less memory in these conditions results in temporary out-of-memory situations and incomplete synchronization between the Working and Protect interfaces.

12.2 CX Images and Requirements

The 12.2 CX releases are based on Cisco IOS Release 12.2(15)BC1, which is a child of Cisco IOS Release 12.2(15)T. The 12.2 BC train is an interim release train that provides DOCSIS 1.1 two-way support, along with fixes for software caveats and support for selected new features.

The latest image in the 12.2 CX release train, Cisco IOS Release 12.2(15)CX1, provides two different boot images for the Cisco uBR7200 series routers:

- ubr7200-kboot-mz.122-15.CX.bin

  The "kboot" version of the boot image is a new version of the boot image software that can run only on the Cisco uBR7200-NPE-G1 processor and the UBR7200-I/O-2FE/E I/O controller, because it is too large to load on the other I/O controllers. This image contains support for almost all supported port adapters, allowing the Cisco uBR7246VXR router to boot over almost any type of WAN interface.

- ubr7200-boot-mz.122-15.CX.bin

  The "boot" version of the boot image is small enough to be loaded on I/O controllers with 4MB of Flash memory, but it supports only Ethernet, FastEthernet, Gigabit Ethernet, OC POS, and a limited number of ATM port adapters. If you are using a serial port adapter or most ATM port adapters, you will not be able to boot over the WAN interface.

This difference in boot images affects only the ability of the Cisco uBR7246VXR router to boot over the WAN interface. When the router has successfully loaded the Cisco IOS software, it has connectivity over all of the port adapters that this particular version of Cisco IOS software supports.

Table 1-3 displays the memory recommendations of the Cisco IOS feature sets for the Cisco uBR7200 series universal broadband routers for Cisco IOS Release 12.2(15)CX1. Cisco uBR7200 series routers are only available with a 48 MB or 128 MB of Flash disk memory on the I/O Controller cards. The UBR7200-NPE-G1 uses only compact Flash disk.

Flash disks, an alternative to linear Flash memory, are Flash memory-based devices that can be used as file storage media in the PCMCIA card slots of the I/O Controllers. Each I/O Controller has two PCMCIA slots and can be configured with up to 256 MB of Flash disk memory.

Table 1-3 Memory Recommendations for the Cisco uBR7200 Series Routers, Cisco Release 12.2(15)CX1 Feature Sets

Feature Set	Software Image	Recommended Flash Disk Memory	Recommended DRAM Memory	Runs From
Two-Way Data/VoIP Images				
DOCSIS Two-Way	ubr7200-p-mz	48 MB Flash	128 MB DRAM	RAM
DOCSIS Two-Way IP Plus	ubr7200-is-mz	48 MB Flash	128 MB DRAM	RAM
DOCSIS Two-Way with BPI	ubr7200-k8p-mz	48 MB Flash	128 MB DRAM	RAM
DOCSIS Two-Way IP Plus with BPI	ubr7200-ik8s-mz	48 MB Flash	128 MB DRAM	RAM
DOCSIS Two-Way 3DES	ubr7200-k9p-mz	48 MB Flash	128 MB DRAM	
DOCSIS Two-Way 3DES IP Plus	ubr7200-ik9s-mz	48 MB Flash	128 MB DRAM	

The image subset legend for Table 1-3 is as follows:

- i = IP routing, MPLS-VPN support, and non-cable interface bridging, including Network Address Translation (NAT)
- k8 = DOCSIS Baseline Privacy
- p = IP routing with Intermediate System-to-Intermediate System (IS-IS) and Border Gateway Protocol (BGP); MPLS-VPN support; no bridging and no NAT
- s = "Plus" features: NAT and Inter-Switch Link (ISL)
- k9 = 3DES level of encryption

12.1 EC Images and Requirements

The 12.1 EC train is the Cisco cable-specific early deployment release train that introduces several new feature sets, support for the Cisco uBR-MC28C cable interface line card, and several new software features.

Table 4 displays the memory recommendations of the Cisco IOS feature sets for the Cisco uBR7200 series universal broadband routers for the latest Cisco IOS Release 12.1(20)EC1. Cisco uBR7200 series routers support a 16-MB or 20-MB Type II PCMCIA Flash memory card.

Table 4 Memory Recommendations for the Cisco uBR7200 Series Routers, Cisco Release 12.1(20)EC1 Feature Sets

Feature Set	Software Image	Recommended Flash Memory	Recommended DRAM Memory	Runs From
Two-Way Data/VoIP Images				
DOCSIS Two-Way	ubr7200-p-mz	16 MB Flash	128 MB DRAM	RAM
DOCSIS Two-Way IP Plus	ubr7200-is-mz	16 MB Flash	128 MB DRAM	RAM
DOCSIS Two-Way with BPI	ubr7200-k1p-mz	16 MB Flash	128 MB DRAM	RAM
DOCSIS Two-Way IP Plus with BPI	ubr7200-ik1s-mz	16 MB Flash	128 MB DRAM	RAM
Telco-Return Images				
DOCSIS IP Plus Telco Return	ubr7200-ist-mz	16 MB Flash	128 MB DRAM	RAM
DOCSIS IP Plus Telco Return with BPI	ubr7200-ik1st-mz	16 MB Flash	128 MB DRAM	RAM
Boot Image				
UBR7200 Boot Image[1]	ubr7200-boot-mz	None	None	—

1. The 12.1 EC UBR7200 boot image is provided for the IUBR7200-I/O-2FE/E input/output controller, which must use the Cisco IOS 12.1(10)EC1 or later 12.1 EC release boot image. This image cannot be used on any other I/O controllers.

The image subset legend for Table 4 is as follows:

- i = IP routing, MPLS-VPN support, and non-cable interface bridging, including Network Address Translation (NAT)
- k1 = DOCSIS Baseline Privacy and MPLS-VPN support
- p = IP routing with Intermediate System-to-Intermediate System (IS-IS) and Border Gateway Protocol (BGP); MPLS-VPN support; no bridging and no NAT
- s = “Plus” features: NAT and Inter-Switch Link (ISL)
- t = DOCSIS telco return

Note All images support all of the hardware listed in the section “Supported Hardware on the Cisco uBR7200 Series” section on page 1-11, unless otherwise indicated.

Cisco uBR7200 Series Chassis Overview

The Cisco uBR7200 series universal broadband routers allow high-speed data services to be packaged similar to cable TV service or video fare. Cisco uBR7200 Series equipment supports data and digitized voice connectivity between Internet Protocol (IP) hosts and connected subscribers using a bidirectional cable TV and IP backbone.

Note For 6 MHz National Television Systems Committee (NTSC) cable plants not fully upgraded to two-way transmission, the equipment works with dial-up access products to support upstream traffic from Data-over-Cable Service Interface Specification (DOCSIS)-based telco-return cable interfaces.

For international cable plants that use 8-MHz Phase Alternating Line (PAL) or Systeme Electronique Couleur Avec Memoire (SECAM) channel plans, Cisco uBR7200 Series equipment supports bidirectional transfer of traffic between the Cable Modem Termination System (CMTS) and EuroDOCSIS-based CMs or set top box (STB) units with integrated EuroDOCSIS modems.

Cable companies and Internet service providers (ISPs) can allocate radio frequency (RF) channel capacity for Internet access, Virtual Private Network (VPN), or Voice over IP (VoIP) services using a hybrid fiber/coax (HFC) or all-coax cable plant. Cisco currently provides three router-based DOCSIS CMTS solutions that offer a wider feature set and better manageability than bridge-based systems.

- **Cisco uBR7246 VXR Universal Broadband Router**—Supports higher density and broad media configurations; the chassis contains up to two single-width IP backbone interfaces, up to four cable TV RF interfaces, up to two power supplies, an optional clock interface that enables the router to synchronize to an external timing reference, a faster processor, and higher bus bandwidth.
- **Cisco uBR7246 Universal Broadband Router**—Supports large cable installations; the chassis contains up to two single-width IP backbone interfaces, up to four cable TV RF interfaces, and up to two power supplies.
- **Cisco uBR7223 Universal Broadband Router**—Supports small-to-medium cable installations; the chassis contains one single-width IP backbone interface and up to two cable TV RF interfaces.

Note This guide focuses on Cisco uBR7200 Series software. For detailed descriptions of Cisco uBR7200 Series chassis and components, refer to the *Cisco uBR7200 Series Hardware Installation Guide* and appropriate field replaceable unit (FRU) documents on Cisco.com.

Cisco cable interface line cards serve as the RF cable TV interfaces, supporting downstream and upstream signal combining and splitting arrangements. The cards currently require external upconverters to connect to the cable system. Cisco port adapters connect to the IP backbone and external networks. Your cable plant, combined with your planned and installed subscriber base, service offering, and external network connections, determine the Cisco uBR7200 Series chassis, cable interface line cards, port adapters, and other components you use.

Data is modulated or demodulated using either of the following two methods:

- Downstream 6 MHz channels in the 54-to-860 MHz range with upstream ranges of 5 to 42 MHz. Cisco MC11 FPGA, MC11C, MC12C, MC14C, MC16B, MC16C, and MC16S cable interface line cards support NTSC channel operation, using standard (STD), Harmonic Related Carrier (HRC), or Incremental Related Carrier (IRC) frequency plans conforming to EIA-S542.

  NTSC uses a 6 MHz-wide modulated signal with an interlaced format of 25 frames per second and 525 lines per frame. NTSC is compatible with CCIR Standard M. PAL, used in West Germany, England, Holland, Australia, and several other countries.

Note Cisco 6 MHz products can be used in 8 MHz cable plants. The products, however, operate at a maximum downstream bandwidth of 27 Mbps, ignoring 2 MHz of available channel width, and limiting upstream channel choices to the range below 42 MHz.

- Downstream 8 MHz channels in the 85-to-860 MHz range with an upstream range of 5 to 65 MHz. The Cisco MC16E cable interface line card supports PAL and SECAM channel plans using an 8 MHz modulated signal.

  PAL uses a 625-line scan picture delivered at 25 frames per second where the color carrier phase definition changes in alternate scan lines. SECAM uses an 819 line scan picture that provides better resolution than PAL's 625-line and NTSC's 525-line.

  The MC16E uses the EuroDOCSIS J.112 (Annex A) standard, CableLabs ECR RFI-R-98036, which is similar to the Digital Audio Video Council/Digital Video Broadcast (DAVIC/DVB) ITU J.83 Annex A physical layer. Cable companies can support data, voice, and video services with DOCSIS-based CMs or set top boxes (STBs) that contain integrated EuroDOCSIS modems.

Caution The MC16E supports only Annex A operation and should not be used in production cable plants that support a 6 MHz channel plan.

Note The difference between DOCSIS and EuroDOCSIS is at the physical layer. EuroDOCSIS support requires the Cisco MC16E cable interface line card, appropriate upconverters that support an 8 MHz PAL or SECAM channel plan, appropriate diplex filters, and EuroDOCSIS-based CMs or STBs.

The DOCSIS Radio Frequency (RF) specification defines the RF communication paths between the CMTS and CMs (or CMs in STBs). The DOCSIS RF specification defines the physical, link, and network layer aspects of the communication interfaces. It includes specifications for power level, frequency, modulation, coding, multiplexing, and contention control. Cisco offers products that support all DOCSIS error correction encoding and modulation types and formats, and that support DOCSIS Annex B or EuroDOCSIS Annex A operations.

Cisco uBR7200 Series Universal Broadband Routers

The Cisco uBR7200 series universal broadband routers are based on the Data-over-Cable Service Interface Specification (DOCSIS) standards. Each is designed to be installed at a cable operator's headend facility or distribution hub and to function as the cable modem termination system (CMTS) for subscriber-end devices such as the Cisco uBR905 and Cisco uBR925 cable access routers, and other DOCSIS-compliant CMs and set-top boxes (STBs).

Cisco uBR7200 series universal broadband routers allow two-way transmission of digital data and Voice over IP (VoIP) traffic over a hybrid fiber-coaxial (HFC) network. For cable plants not fully upgraded to support two-way cable transmission, the routers support DOCSIS-compliant telco return, where the cable modem's return path to the CMTS uses a dial-up telephone line connection instead of an upstream channel over the coaxial cable. The telco-return delivery mechanism enables cable operators to accelerate deployment of high-speed data services before the cable systems are upgraded to two-way plants.

The Cisco uBR7200 series routers support IP routing with a wide variety of protocols and combinations of Ethernet, Fast Ethernet, Gigabit Ethernet, serial, High-Speed Serial Interface (HSSI), Packet over SONET (POS) OC-3 and OC-12c, and Asynchronous Transfer Mode (ATM) media.

Cisco uBR7246 VXR Universal Broadband Router

The Cisco uBR7246VXR offers an industry-proven CMTS and carrier-class router in a scalable platform with a high-performance network processing engine to support data, voice, and video services for medium to large network installations.

The Cisco uBR7246 VXR provides the following major hardware features:

- High-performance network processing engine or network services engine
- I/O controller
- Up to two network interface port adapters
- Up to four cable interface line cards
- Up to two removable power supplies providing load-sharing and redundancy capabilities
- Two Personal Computer Memory Card International Association (PCMCIA) slots that allow for software upgrades through the use of Flash memory cards

Note The Cisco uBR7246 VXR chassis does not support the MC11-FPGA cable interface line card.

Cisco uBR7246 Universal Broadband Router

The Cisco uBR7246 offers an industry-proven CMTS and carrier-class router in a scalable platform to support data, voice, and video services for medium to large network installations. The Cisco uBR7246 provides the following major hardware features:

- Network processing engine
- I/O controller
- Up to two network interface port adapters
- Up to four cable interface line cards
- Up to two removable power supplies providing load-sharing and redundancy capabilities
- Two PCMCIA slots that allow for software upgrades through the use of Flash memory cards

Cisco uBR7223 Universal Broadband Router

The Cisco uBR7223 is a cost-effective, scalable interface between subscriber CMs and the backbone data network, and is designed specifically for small to medium network installations.

The Cisco uBR7223 provides the following major hardware features:

- Network processing engine
- I/O controller
- One network interface port adapter
- Up to two cable interface line cards
- One removable power supply (The Cisco uBR7223 does not feature load-sharing and redundant power supply capability like the Cisco uBR7246 VXR and Cisco uBR7246.)
- Two PCMCIA slots that allow for software upgrades through the use of Flash memory cards

Supported Hardware on the Cisco uBR7200 Series

Table 1-5 provides a quick overview of the major hardware features of the Cisco uBR7200 series routers.

Table 1-5 Cisco uBR7200 Series Hardware Overview

Supported Hardware	Cisco uBR7246 VXR	Cisco uBR7246	Cisco uBR7223
Network Processing Engines	One of the following: • UBR7200-NPE-G1 • NPE-225 • NPE-300 • NPE-400	One of the following: • NPE-150 • NPE-200 • NPE-225	One of the following: • NPE-150 • NPE-200 • NPE-225
I/O Controllers	One of the following: • UBR7200-I/O • UBR7200-I/O-FE • UBR7200-I/O-2FE/E	One of the following: • UBR7200-I/O • UBR7200-I/O-FE	One of the following: • UBR7200-I/O • UBR7200-I/O-FE
Network Interface Port Adapters	Up to two	Up to two	One
Cable Interface Line Cards	Up to four	Up to four	Up to four
Removable Power Supplies	Up to two	Up to two	One
PCMCIA Slots	Two	Two	Two

Note Earlier release notes stated that the NPE-175 was also supported on the Cisco uBR7200 series routers. Because the NPE-175 has reached its end of life and was never made available for order on the Cisco uBR7200 series routers, it has been removed from the table.

The UBR7200-NPE-G1 does not require that an I/O controller be installed. Refer to the *Cisco uBR7200 Series Software Release Notes* on Cisco.com:

http://www.cisco.com/en/US/docs/cable/cmts/ubr7200/release/notes/12_3bc/123BCu72.html

Network Processing Engines

The Cisco uBR7246 VXR supports the following Network Processing Engines (NPEs):

- UBR7200-NPE-G1
- NPE-225
- NPE-300
- NPE-400

The Cisco uBR7223 and the Cisco uBR7246 support the following Network Processing Engines (NPE) :

- NPE-150
- NPE-200
- NPE-225

Note The NPE-300 and NPE-400 are not supported on the Cisco uBR7223 and the Cisco uBR7246. The NPE-150 and NPE-200 are not supported on the Cisco uBR7246 VXR.

For more information, refer to the following resources on Cisco.com:

- *Network Processing Engine and Network Services Engine Installation and Configuration Guide*
- *Memory Replacement Instructions for the Network Processing Engine or Network Services Engine and Input/Output Controller*

I/O Controllers

The Cisco uBR7200 series universal broadband routers support the following input/output (I/O) controllers:

- UBR7200-I/O-2FE/E input/output controller
  - Features two Fast Ethernet ports and one Ethernet port.
  - Equipped with 2 RJ-45 receptacles for 10/100 Mbps operation.
  - Supported for the Cisco uBR7246VXR router.
  - The Cisco IOS Release 12.1(10)EC boot helper image [ubr7200-boot-mz.12.1-10.EC] must be used on this controlle.r
- UBR7200-I/O-FE
  - Features one Fast Ethernet port.
  - Equipped with an MII receptacle and an RJ-45 receptacle for use at 100 Mbps full-duplex or half-duplex operation.
  - Only one receptacle can be configured for use at a time.
  - Supported for Cisco uBR7223, Cisco uBR7246, and Cisco uBR7246 VXR routers.
  - The 12.0(15)SC [ubr7200-boot-mz.12.0-15.SC] boot helper image is recommended for this controller.
- UBR7200-I/O
  - Has no Fast Ethernet port.
  - Supported for Cisco uBR7223, Cisco uBR7246, and Cisco uBR7246 VXR routers.
  - The 12.0(15)SC [ubr7200-boot-mz.12.0-15.SC] boot helper image is recommended for this controller.

Note The Single-Port Fast Ethernet I/O Controller (UBR7200-I/O-FE) reached its End of Sale (EOS) point on June 30, 2003. For details, see the Addendum to Product Bulletin, No. 1725, available at the following location on Cisco.com:

http://www.cisco.com/en/US/products/hw/cable/ps2217/prod_eol_notice09186a00800a470d.html

Note Do not use the 12.1(10)EC boot helper image with the UBR7200-I/O-FE and UBR7200-I/O controllers.

Network Interface Port Adapters

The Cisco uBR7200 series routers support multiple port adaptors with Ethernet, Gigabit Ethernet and Serial versions. Enhancements and options are available in multiple Cisco IOS Software release trains. For the latest information about supported port adaptors, refer to *Cisco uBR7200 Series Software Release Notes* on Cisco.com:

http://www.cisco.com/en/US/docs/cable/cmts/ubr7200/release/notes/12_3bc/123BCu72.html

Note Not all Cisco uBR7200 series routers support all port adapters. Some port adapters must be at certain revision levels to be used in the Cisco uBR7246 VXR router.

Note Cisco recommends using the most current release in a release train if possible.

Cable Interface Line Cards

The Cisco uBR7200 series supports the following cable interface line cards, all of which provide connection to the hybrid fiber-coaxial (HFC) network.

Table 1-6 provides a quick overview of the cable interface line cards that are supported with Cisco uBR7200 series routers.

Table 1-6 Cisco uBR7200 Series Cable Interface Line Cards

Cable Interface Line Card	Upstream Ports	Downstream Ports	Additional Features
MC11C	1	1	
MC12C	2	1	
MC14C	4	1	
MC16C	6	1	
MC16E	6	1	EuroDOCSIS (Annex A) Support
MC16S	6	1	Enhanced software- and hardware-based Spectrum Management Support
MC28C	8	2	
MC28C-BNC	8	2	BNC connectors instead of F-connectors

For the latest information about supported cable interface line cards, refer to *Cisco uBR7200 Series Software Release Notes* on Cisco.com:

http://www.cisco.com/en/US/docs/cable/cmts/ubr7200/release/notes/12_3bc/123BCu72.html

System Interoperability

This section describes guidelines about the interoperability of certain features in the Cisco uBR7200 series universal broadband routers. Additional DOCSIS interoperability is described in the "Supported Software Features for the Cisco uBR7200 Series" section on page 1-22.

Cable Modem Interoperability

The Cisco uBR7200 series interoperates with the following cable modems:

- DOCSIS-based two-way cable modems that support basic Internet access, VoIP, or Virtual Private Networks (VPNs).
- Telco-return Cable modems

  To support telco return, use a Cisco uBR7200 series software image that contains "t" in its file name. The telco-return cable modem must be DOCSIS-based or compliant and must be configured to support telco return.

  Note Some third-party telco-return CMs cannot receive traffic over the same downstream channel as CMs operating on a two-way data system. In these instances, segment your cable plant to allow more than one downstream channel.

- EuroDOCSIS cable modems or STBs with integrated EuroDOCSIS CMs using Cisco MC16E cable interface line cards and Cisco IOS Release 12.1(2)EC1 or higher.

  EuroDOCSIS operation support includes 8-MHz Phase Alternating Line (PAL) or Systeme Electronique Couleur Avec Memoire (SECAM) channel plans.

Clock Synchronization

The Cisco uBR7200 series support clock hardware and software to enable high-quality delivery of IP telephony services through synchronized data transmissions. To support the clock feature set, a Cisco uBR7246 VXR chassis must be used. The Cisco uBR7246 VXR must contain a clock card and an MC16S, MC16E, or MC28C cable interface line card. Only the MC16S, MC16E, and MC28C cable interface line cards support the external clock reference from the clock card to distribute that signal to CMs or STBs attached to the specific network segments. A chassis configured with an MC16S or MC16E cable interface line card must be running Cisco IOS Release 12.1(2)EC1 or higher. A chassis configured with an MC28C cable interface line card must be running Cisco IOS Release 12.1(3a)EC1 or higher.

Each cable modem must also support VoIP applications and the clock reference feature set to enable synchronized timing. The Cisco uBR924 cable access router, running Cisco IOS Release 12.0(7)T or later, supports the clock reference feature set automatically.

Cisco uBR7200 Series Router Configuration Overview

This section describes Cisco uBR7200 series router features that require software configuration, and summarizes these features of the Cisco uBR7200 series router:

Refer to the "Cisco uBR7200 Series Router Configuration Tools" section on page 1-31 for additional configuration utilities.

Port Adapter and Line Card Slot and Logical Interface Numbering

For Cisco uBR7200 series components, the slot number is the chassis slot in which a port adapter or a cable interface card is installed. The logical interface number is the physical location of the interface port on a port adapter. Numbers on a Cisco uBR7200 series router begin with 0. Using a Cisco uBR7246 to illustrate, slot/port positioning is as follows:

- Slot 0—I/O controller
- Slot 1-2—Cisco port adapters
- Slot 3-6—Cisco cable interface line cards; the upstream ports on the card start with port 0.

To configure the system, define the Cisco uBR7200 series interfaces, using the **interface type slot/port** commands:

- Type—Cable
- Slot—Slot number in chassis. Slot numbers begin with 0.
- Port—Port number on a cable interface line card slot. Port numbers begin with a 0.

Configuring Cisco cable interface line cards is particularly important because these components serve as the cable TV RF interfaces. Configuration involves the following tasks for each interface:

- Setting the downstream center frequency for the card to reflect the digital carrier frequency of the downstream RF carrier (the channel) for that downstream port. To do this, enter the fixed center frequency for your downstream RF carrier in Hz:

```
Router (config-int)# cable downstream frequency down-freq-hz
```

Note This command has no effect on the external upconverter, which actually sets the downstream frequency. Noting the correct value for the cable interface line card, however, provides useful information for troubleshooting.

The digital carrier frequency is specified to be the center of a 6 or 8 MHz channel based on your channel plan. To illustrate for NTSC channel plans, EIA channel 95 spans 90.00 to 96.00 MHz. The center frequency is 93.000 MHz which is the digital carrier frequency that should be configured as the downstream frequency.

Tip The digital carrier frequency is not the same as the video carrier frequency. For EIA channel 95, the video carrier frequency is 91.250 MHz which is 1.75 MHz below the center frequency.

- Activating the downstream port on the cable interface line card for data transmission over the HFC network, using the following command:

```
Router (config-int)# no shutdown
```

  The particular downstream port LED should light.

- Setting the upstream frequency of your RF output to comply with the expected input frequency of your Cisco cable interface line card.

Tip The valid range for a fixed upstream frequency is 5,000,000 Hz to 65,000,000 Hz for the MC16E cable interface line card. The valid range for all other cable interface line cards that support NTSC operations is 5,000,000 Hz to 42,000,000 Hz.

  The cable interface will not operate until you either set a fixed upstream frequency or create and configure a spectrum group. Enter the fixed center frequency for your upstream RF carrier in Hz and specify a port number from 0 to 5:

```
Router (config-int)# cable upstream port frequency up-freq-hz
```

Note Make sure that the selected upstream frequency does not interfere with the frequencies used for any other upstream applications in your cable plant.

- Entering an upstream RF carrier frequency for each upstream port on a cable modem.
- Activating the RF carrier on each upstream port to support data from CMs or set top boxes on your network to the Cisco uBR7200 series router. Enable upstream data traffic, using the following command:

```
Router (config-int)# no cable upstream port shutdown
```

  The specified upstream port LED lights.

  Repeat the above for each upstream port to activate.

- Verifying your settings using the following command:

```
Router# show running-config
```

- Saving the configuration to nonvolatile random access memory (NVRAM) so that your settings are retained after a power cycle:

```
Router# copy running start
```

- Verifying the upstream frequency, using the **show controllers cable** *slot/port* **upstream** command for the upstream port you just configured.
- Verifying the downstream center frequency, using the **show controllers cable** *slot/port* **downstream** command for the downstream port you just configured.

MAC-Layer Addressing

The Media Access Control (MAC)-layer or hardware address is a standardized data link layer address required for certain network interface types. These addresses are not used by other devices in the network; they are specific and unique to each port. The Cisco uBR7200 series uses a specific method to assign and control the MAC-layer addresses for port adapters.

All LAN interfaces (ports) require unique MAC-layer addresses, also known as hardware addresses. Typically, the MAC address of an interface is stored on a memory component that resides directly on the interface circuitry; however, the online insertion and removal (OIR) feature requires a different method. The OIR feature lets you remove a port adapter or cable interface card and replace it with another identically configured one. If the new port adapter or cable interface card matches the port adapter or cable interface card you removed, the system immediately brings it online.

To support OIR, an address allocator with a unique MAC address is stored in an EEPROM on the universal broadband router midplane. Each address is reserved for a specific port and slot in the router regardless of whether a port adapter or a cable interface card resides in that slot.

Note Port adapter and cable interface card slots maintain the same slot number regardless of whether other port adapters or cable interface cards are installed or removed. However, when you move a port adapter or cable interface card to a different slot, the logical interface number changes to reflect the new slot number.

Caution When "hot swapping" a port adapter or cable interface line card with a different type of component (for example, an MC11 FPGA with an MC11C, or an MC16B with an MC16C), you might have to reconfigure the interfaces. Refer to the *Cisco uBR7200 Series Universal Broadband Router Hardware Installation Guide* or appropriate FRU document for more specific information regarding online insertion and removal (OIR).

The MAC addresses are assigned to the slots in sequence. The first addresses are assigned to port adapter slot 0 and slot 1, and the next addresses are assigned to port adapter slot 2 through cable interface card slot 6. This address scheme allows you to remove port adapters or cable interface cards and insert them into other universal broadband routers without causing the MAC addresses to move around the network or be assigned to multiple devices.

Storing the MAC addresses for every slot in one central location means the addresses stay with the memory device on which they are stored.

Cable Interface Line Cards

As of the date of this publication, the following Cisco cable interface cards can be installed in a Cisco uBR7200 series router:

- MC11 with one downstream modulator and one upstream demodulator. Two different revisions exist for this card:
  - The FPGA version of the card supports the following defaults: Quadrature Amplitude Modulation (QAM)-64 at 27 Mbps downstream, and Quadrature Phase Shift Keying (QPSK) at 1.280 kbps upstream. The card outputs +32 dBmV and +/- 2 dBmV.
  - The C version of the card supports the following defaults: QAM-256 at 40 Mbps downstream and QAM-16 at 5 Mbps upstream. The card supports upstream channel widths of 200 kHz, 400 kHz, 800 kHz, 1.6 MHz, and 3.2 MHz. The card outputs +42 dBmV and +/- 2 dBmV.

Note All C version cards support all DOCSIS modulation and symbol rates. Refer to Table 1-7Table 1-6 for a list of DOCSIS supported data rates and modulation schemes.

Because the FPGA version of the MC11 card supports only one upstream modulation and channel width, you cannot define an upstream modulation profile for the card. The default modulation profile 1 cannot be changed when using the FPGA version of the MC11 card.

- MC12C with one downstream modulator and two upstream demodulators: The card supports the following defaults: QAM-256 at 40 Mbps downstream and QAM-16 at 5 Mbps upstream. The card supports upstream channel widths of 200 kHz, 400 kHz, 800 kHz, 1.6 MHz, and 3.2 MHz.The card outputs +42 dBmV and +/- 2 dBmV.
- MC14C with one downstream modulator and four upstream demodulators: The card supports the following defaults: QAM-256 at 40 Mbps downstream and QAM-16 at 5 Mbps upstream. The card supports upstream channel widths of 200 kHz, 400 kHz, 800 kHz, 1.6 MHz, and 3.2 MHz. The card outputs +42 dBmV and +/- 2 dBmV.
- MC16 with one downstream modulator and six upstream demodulators. Two different revisions exist for this card:
  - The B version of the card supports the following defaults: QAM-64 at 27 Mbps downstream and QPSK at 2.56 Mbps upstream. The card supports channel widths of 200 kHz, 400 kHz, 800 kHz, 1.6 MHz, and 3.2 MHz. The card outputs +32 dBmV and +/- 2 dBmV.

    Note The B version card excludes support of QAM-256 downstream and QAM-16 upstream support at two of the five DOCSIS upstream symbol rates—2.56 M and 1.28 M. Refer to Table 1-7Table 1-6 for Table 1-6a list of DOCSIS supported data rates and modulation schemes.

  - The C version of the card supports the following defaults: QAM-256 at 40 Mbps downstream and QAM-16 at 5 Mbps upstream. The card supports upstream channel widths of 200 kHz, 400 kHz, 800 kHz, 1.6 MHz, and 3.2 MHz. The card outputs +42 dBmV and +/- 2 dBmV.
- MC16S with one downstream modulator and six upstream demodulators. The card supports the following defaults: QAM-256 at 40 Mbps downstream and QAM-16 at 5 Mbps upstream. The card supports upstream channel widths of 200 kHz, 400 kHz, 800 kHz, 1.6 MHz, and 3.2 MHz. The card outputs +42 dBmV and +/- 2 dBmV.

  The MC16S includes the ability to scan portions of the upstream spectrum for clean channels of varying widths. A daughtercard on the MC16S samples the 5-to-42 MHz upstream spectrum and initiates a frequency hop if an administrator-defined threshold value for offline CMs is met. The threshold value is contained in the router's configuration file. When the threshold value is reached, the spectrum management daughtercard takes a snapshot of the available upstream spectrum and passes this information to the Cisco IOS software where it is analyzed for indications of significant ingress or impulse noise. From this analysis, the Cisco IOS software draws informed conclusions on the cleanest portion(s) of the upstream frequency spectrum to switch to and initiates a frequency hop.
- MC16E with one downstream modulator and six upstream demodulators. The card supports the following defaults: QAM-256 at 40 Mbps downstream and QAM-16 at 5 Mbps upstream. The card supports EuroDOCSIS 8 MHz PAL and SECAM channel plans, supporting downstream rates of 85-to-860 MHz range with upstream ranges of 5-to-65 MHz. The card outputs +40 dBmV and +/- 2 dB.

Note While most Cisco cable interface line cards transmit downstream signals to upconverters using a 44 MHz frequency, the MC16E transmits downstream IF signals to an upconverter using the 36.125 MHz frequency. Only the MC16E cable interface line card supports full 8 MHz operation.

The cable interface cards can be configured in a number of different upstream combinations based on the card used, your cable network, and the anticipated subscription and service levels. Table 1-7 shows the DOCSIS and EuroDOCSIS data rates.

Table 1-7 DOCSIS and EuroDOCSIS Data Rates

Upstream Channel Width	Modulation Scheme	Baud Rate Sym/sec	Raw Bit Rate Mbit/sec
3.2 MHz	QAM-16 QPSK	2.56 M	10.24 5.12
1.6 MHz	QAM-16 QPSK	1.28 M	5.12 2.56
800 kHz	QAM-16 QPSK	640 K	2.56 1.28
400 kHz	QAM-16 QPSK	320 K	1.28 0.64
200 kHz	QAM-16 QPSK	160 K	0.64 0.32

Cable Interface Line Card Slots

To display information about a specific cable interface card slot's downstream channel, use the **show interfaces cable** command with the cable modem line card's slot number and downstream port number in the following format:

show interfaces cable *slot/downstream-port* [**downstream**]

Use the slot number and downstream port number to display information about a downstream interface. You can abbreviate the command to **sh int c**. The following example illustrates the display for downstream channel port 0 in cable interface slot 3 of a Cisco uBR7246:

```
Router# sh int c 3/0

Cable3/0 is up, line protocol is up
    Hardware is CMTS, address is 0009.0ed6.ee18 (bia 0009.0ed6.ee18
    Internet address is 1.1.1.1/24
    MTU 1500 bytes, BW 27000 Kbit, DLY 1000 usec, rely 255/255, load 1/255
    Encapsulation MCNS, loopback not set, keepalive not set
    ARP type: ARPA, ARP Timeout 04:00:00
    Last input 00:00:00, output 00:00:00, output hang never
    Last clearing of "show interface" counters never
    Queueing strategy: fifo
    Output queue 0/40, 0 drops; input queue 0/75, 0 drops
    5 minute input rate 41000 bits/sec, 45 packets/sec
    5 minute output rate 43000 bits/sec, 45 packets/sec
        1616534 packets input, 184284660 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        1616534 packets output, 184284660 bytes, 0 underruns
        0 output errors, 0 collisions, 0 interface resets
        0 output buffer failures, 0 output buffers swapped out
```

To display information about a specific cable interface card slot's upstream channel, use the **show interfaces cable** command with the cable modem card's slot number, downstream port number, and upstream port number in the format of **show interfaces cable** *slot/downstream-port* [**upstream**] *upstream-port*. Use the slot number, downstream port number, and upstream port number to display information about an upstream interface. You can abbreviate the command to **sh int c**.

The following example shows the display for upstream channel port 0 in cable interface slot 3 of a Cisco uBR7246 that is turned up:

```
Router# sh int c 3/0 0

Cable6/0: Upstream 0 is up
    Received 3699 broadcasts, 0 multicasts, 28586 unicasts
    0 discards, 0 errors, 0 unknown protocol
    21817 packets error-free, 2371 corrected, 8097 uncorrectable
    0 noise, 0 microreflections
    CBR_queue_depth: [not implemented], ABR_queue_depth: [not implemented],
    UBR[1]_queue_depth: 0, UBR[2]_queue_depth: 0,
    UBR[3]_queue_depth: 0,  POLLS_queue_depth:  [not implemented]
    ADMIN_queue_depth: [not implemented]
    Last Minislot Stamp (current_time_base):190026    FLAG:1
    Last Minislot Stamp (scheduler_time_base):200706  FLAG:1
```

Interfaces and Physical Ports

Table 1-8 maps the cable interface card's interfaces and physical ports. The cards can be configured in a number of different upstream combinations.

Table 1-8 Interface to Port Mapping

Cable Interface Line Card	Interface	Physical Ports
MC11	Cable N/0	DS, US0
MC12	Cable N/0	DS, US0, US1
MC14	Cable N/0	DS, US0, US1, US2, US3
MC16	Cable N/0	DS, US0, US1, US2, US3, US4, US5

Port Adapter Slots

You can display information on a specific port adapter or all port adapters in the Cisco uBR7200 series. To display information about all port adapter slots, use the **show interfaces** command. To display information about a specific port adapter slot, use the **show interfaces** command with the port adapter type and slot number in the format of **show interfaces** [*type slot/port*].

Tip If you abbreviate the command (**sh int**) and do not specify the port adapter type and slot number (or arguments), the system interprets the command as **show interfaces.** The system displays the status of all port adapters, all cable interface cards, and all ports.

The follow example illustrates the **show interfaces** command with status information (including the physical port adapter number) for each port adapter and cable interface card in the Cisco uBR7246 router:

```
Router# sh int

FastEthernet0/0 is administratively up, line protocol is up
Hardware is DEC21140, address is 0000.0000.0000 (bia 0000.0000.0000)
Internet address is 1.1.1.3
MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec, rely 255/255, load 1/255
(display text omitted)
Hssi1/0 is administratively down, line protocol is down
Hardware is MIF68840_MM, address is 0000.0000.0000 (bia 0000.0000.0000)
Internet address is 1.1.1.0
MTU 4470 bytes, BW 100000 Kbit, DLY 100 usec, rely 255/255, load 1/255
(display text omitted)
Ethernet2/0 is administratively up, line protocol is up
Hardware is AmdP2, address is 0000.0000.0000 (bia 0000.0000.0000)
Internet address is 1.1.1.7
MTU 1500 bytes, BW 100000 Kbit, DLY 1000 usec, rely 255/255, load 1/255
(display text omitted)
Cable3/0 is up, line protocol is up
Hardware is CMTS, address is 0009.0ed6.ee18 (bia 0009.0ed6.ee18)
Internet address is 1.1.1.1/24
MTU 1500 bytes, BW 27000 Kbit, DLY 1000 usec, rely 255/255, load 1/255
(display text omitted)
```

You can also use arguments such as the interface type (Ethernet, Fast Ethernet, ATM, serial, HSSI, Packet-over-SONET, and so forth) and the port address (slot/port) to display information about a specific port adapter interface only. The following example shows such a display:

```
Router# sh int f1/0
FastEthernet1/0 is up, line protocol is up
  Hardware is AmdFE, address is 0030.7bfa.a81c (bia 0030.7bfa.a81c)
  Internet address is 111.0.1.18/30
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, 100BaseTX/FX
  ARP type:ARPA, ARP Timeout 04:00:00
  Last input 00:00:01, output 00:00:02, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy:fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets put, 230925 bytes
     Received 146107 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog
     0 input packets with dribble condition detected
     0 packets put, 284529 bytes, 0 underruns
     0 output errors, 0 collisions, 10 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
```

Supported Software Features for the Cisco uBR7200 Series

This section summarizes Cisco uBR7200 series router software features for all supported Cisco IOS Release trains, and directs you to additional configuration information for each feature.

Cisco uBR7200 Series Router Features and Cisco IOS Releases

Table 1-9 summarizes the software-related features and related Cisco IOS releases that support the Cisco uBR7200 series router. Cisco IOS features indicate the first release in which the feature was introduced. Unless otherwise noted, feature support continues in later releases of the same or related Cisco IOS release train

Many additional features were introduced in release trains prior to those listed above, such as 12.0 T, 12.0 SC, 12.1 XF and other earlier releases that may no longer be supported on the Cisco uBR7200 Series. Refer to the release notes for your respective Cisco IOS release for additional feature support and image information.

Table 1-9 Cisco uBR7200 Series Routers Features by Cisco IOS Release

Feature	Supporting Cisco IOS Releases
Cisco uBR7200 Series Router Configuration Tools	
Autoinstall	12.0 T, 12.0 XR, 12.0 SC, 12.1 EC, 12.1 CX, 12.2 BC and 12.3 BC releases
Cable Interface Setup Facility	12.1 EC, 12.1 CX, 12.2 BC and 12.3 BC releases
Cable Interface Extended Setup Facility	12.1(3a)EC1 and all later Cisco IOS releases supporting the Cisco uBR7200 Series CMTS
Cisco Network Registrar	12.1 EC, 12.2 BC, 12.3 BC
Interface Range Specification	12.0 T, 12.0 XR, 12.0 SC, 12.1 EC, 12.1 CX, 12.2 BC and 12.3 BC releases
Internal Modem Configuration File Editor	12.2(1)XF1 and later 12.2 XF, 12.2 BC and 12.3 BC releases
Manual Configuration Mode for the Cisco uBR7200 Series CMTS	All Cisco IOS releases supporting the Cisco uBR7200 Series CMTS
Virtual Interface Support and Frequency Stacking Support	12.3(9a)BC and later 12.3 BC releases
Bandwidth Management Features	
Load Balancing Support	12.3(9a)BC and later 12.3 BC releases
Cisco IOS Command-Line Enhancements	
exec prompt timestamp Command	12.1(12c)EC, 12.2(8)BC2 and later 12.1 EC, 12.2 BC and 12.3 BC releases
show Command Enhancements	Multiple Cisco IOS software releases. Enhancements include: • show cable qos • show int cx/y sid • show cable modem • show cable modulation-profile • show cable modem summary

Table 1-9 Cisco uBR7200 Series Routers Features by Cisco IOS Release (continued)

Feature	Supporting Cisco IOS Releases
Cisco IOS Release 12.3(9a)BC Command-Line Interface (CLI) Enhancements	12.3(9a) enhancements to or introductions of the following commands: • cable logging layer2events • cable source-verify • show cable tech-support • show controllers cable • show tech-support
Cisco Quality of Service Features	
Cisco Network-Based Application Recognition (NBAR)	12.1(10)EC, 12.2 BC and later releases
RTP Header Compression	11.3(11)NA, 12.0 T and later releases
DHCP Servers and Feature Support	
Configurable Leasequery Server	12.3(17a)BC and later 12.3 BC releases
DHCP MAC Address Exclusion List for cable-source verify dhcp Command	12.3(13a)BC and later 12.3 BC releases See the "DOCSIS 1.1 Feature Support" section on page 1-57 for additional DHCP features.
DOCSIS 1.0 Feature Support	
DOCSIS 1.0 Baseline Privacy	12.0(6)SC, 12.1 EC and later releases
DOCSIS 1.0 Baseline Privacy Interface Encryption and Encrypted Key Exchange	12.0 SC and later releases in multiple release trains
DOCSIS 1.0 Concatenation Override Featurette	12.3(13a)BC and later 12.3 BC releases
DOCSIS 1.0 Extensions	12.0(16)SC3, 12.1 EC, 12.2 CX, 12.2 BC, and 12.3 BC
DOCSIS 1.0 Quality of Service	12.1 EC, 12.2 CX, 12.2 BC, and 12.3 BC Several additional DOCSIS 1.0 QoS enhancements for the Cisco uBR7200 Series are described in release notes for earlier releases.
DOCSIS Quality of Service Enhancements Prior to DOCSIS 1.1	DOCSIS quality of service (QoS) enhancements added to Cisco IOS Release 12.1(1a)T1 and continue with later releases in multiple trains.
DOCSIS 1.0 ToS Overwrite	12.3(17a)BC2 and later 12.3 BC releases.
DOCSIS Customer Premises Equipment Configurator	DOCSIS CPE Configurator V2.0.4 and V 3.2 supported in multiple Cisco IOS releases.
Enhanced Rate Bandwidth Allocation (ERBA) Support for DOCSIS 1.0 Cable Modems	12.3(13a)BC and later 12.3 BC releases

Table 1-9 Cisco uBR7200 Series Routers Features by Cisco IOS Release (continued)

Feature	Supporting Cisco IOS Releases
DOCSIS 1.0+ Feature Support	
Concatenation for DOCSIS 1.0+	12.1(1)T and later releases in multiple trains support DOCSIS 1.0+ on the Cisco uBR7200 Series.
Dynamic MAC messages	
Multiple SIDs per Cable Modem	
Separate Downstream Rates	
Unsolicited Grant Service (CBR-scheduling) on the Upstream	
DOCSIS 1.1 Feature Support	
Baseline Privacy Interface Plus (BPI+)	12.2(4)BC1 and later 12.2 BC and 12.3 BC releases
Burst Profile Configuration	12.2(4)BC1 and later 12.2 BC and 12.3 BC releases
Cable Modulation Profile Default Templates	12.1(3a)EC1 and later 12.1 EC releases
DHCP Cable Modem Host ID	12.0(4)T, with additional enhancements and support in 12.0 (6) SC, 12.1(2) EC1, 12.1(3a)EC, 12.2(15)BC2 and later releases
DHCP Client ID/Remote ID Options	12.0(16)SC3 and later releases in multiple release trains
DHCP, Time of Day (ToD) and TFTP Servers	Multiple releases in multiple release trains beginning with 12.0 early deployment releases
DOCSIS 1.1 Quality of Service Features	12.2 BC and 12.3 BC release trains, with additional DOCSIS 1.1 features supported in certain earlier Cisco IOS 12.1 EC and 12.0 SC release trains. Includes: • Concatenation for DOCSIS 1.1 • DOCSIS 1.0 and 1.0+ Cable Modem Support • DOCSIS 1.1 Service Flow Model • Downstream QoS Handling Supported • Dynamic MAC Messages • Dynamic Map-Advance • Dynamic SID Support • Fragmentation (Layer 2) • Multiple SID Support • Payload Header Suppression (PHS) • QoS Configuration • QoS Profile Enforcement • Time-of-Day Server • Trivial File Transfer Protocol Server • Type/Length/Value Parser and Encoder • UpstreamAddress Verification • Upstream QoS Improvements • Upstream QoS Models Supported

Table 1-9 Cisco uBR7200 Series Routers Features by Cisco IOS Release (continued)

Feature	Supporting Cisco IOS Releases
DOCSIS 1.1 Two-way Transmission (Cisco uBR7246VXR Router)	12.2 BC, 12.3 BC
Downstream Channel ID	12.0(4)T and later releases in multiple trains
Downstream Frequency Override	12.0(6)SC, 12.1 EC and later releases supporting the Cisco uBR7200 series
Downstream Packet Classifier	12.2 BC and 12.3 BC release trains
Downstream Packet Scheduler	12.2 BC and 12.3 BC release trains
Downstream Rate Shaping with IP Type of Service Bits	11.3NA, 12.0(5)T and later releases in multiple release trains.
Downstream Traffic Shaping	11.3(6) NA, with additional enhancements and support in 12.0(4)XI, 12.0(5)T1, 12.1(1)EC1, 12.2(4)BC1 and later releases.
Optional Upstream Scheduler Modes	12.3(13a)BC and later 12.3 BC releases
DOCSIS 2.0 Feature Support	
DOCSIS 2.0 A-TDMA Support	12.2(15)CX and continues with later 12.2 CX, 12.2 BC and 12.3 BC releases
High Availability Features	
Cisco DDC (Dual DOCSIS Channel)	12.3(9a)BC and later 12.3 BC releases
DSX Messages and Synchronized PHS Information	12.3(17a)BC and later 12.3 BC releases
HCCP Support for the Cisco uBR-MC16S Cable Interface Line Card	12.1(7)EC and later releases in multiple release trains
HCCP N+1 Redundancy	12.1(10)EC, with additional enhancements and support in 12.2(4)XF1, 12.2(4)BC1, 12.2(8)BC2, 12.2(11)BC1, 12.2(15)BC1, 12.2(15)BC2a and later releases in multiple trains
High Availability Features in Cisco IOS Release 12.3(13a)BC	12.3(13a)BC and later 12.3 BC releases
Hot-Standby 1+1 Redundancy	12.1(3a)EC and later releases in multiple release trains
IF Muting for HCCP N+1 Redundancy	12.2(15)BC2a and later 12.2 BC and 12.3 BC releases
Intercept Features	
Access Control List Support for COPS Intercept	12.3(13a)BC and later 12.3 BC releases
Cable Monitor Enhancements	12.3(17a)BC and later 12.3 BC releases
COPS TCP Support for the Cisco Cable Modem Termination System	12.3(13a)BC and later 12.3 BC releases
Service Independent Intercept (SII) Support on the Cisco uBR7200 Series	12.3(13a)BC and later 12.3 BC releases

Table 1-9 Cisco uBR7200 Series Routers Features by Cisco IOS Release (continued)

Feature	Supporting Cisco IOS Releases
IP Broadcast and Multicast Features	
Multicast QoS Support on the Cisco uBR7246VXR CMTS	12.3(13a)BC and later 12.3 BC releases
IP Routing Features	
Cable ARP Filter Enhancement	12.2(15)BC2b and later 12.2 BC and 12.3 BC releases
Cable Interface Bundling and Cable Subinterfaces	12.0 SC, 12.1 EC, 12.2 BC and later BC releases
Configurable Alternate Termination System Information Messages	12.1(2)EC and later releases in this and additional release trains
Easy IP (Phase 1)	12.0 XC and later releases in this and additional release trains
Fast-Switched Policy Routing	12.0 XC and later releases in this and additional release trains
HSRP over ISL in Virtual LAN Configurations	12.0 XC and later releases in this and additional release trains
IP Enhanced IGRP Route Authentication	12.0 XC and later releases in this and additional release trains
IP Network Address Translation/Port Address Translation	12.0 XC and later releases in this and additional release trains
NAT—Support for NetMeeting Directory (Internet Locator Service—ILS)	12.0 XC and later releases in this and additional release trains
Router-Port Group Management Protocol	12.1 T and later releases in this and additional release trains
Supported Protocols on the Cisco uBR7200 Series	Multiple protocols are supported in all release trains that support the Cisco uBR7200 Series.
Management Features	
Admission Control for the Cisco CMTS	12.3(13a)BC and later 12.3 BC releases
Cable ARP and Proxy ARP (cable arp and cable proxy arp commands)	12.1T , 12.0(6)SC , 12.1(2) EC1, 12.2(8)BC1, and later releases in respective release trains
cable map-advance Command Enhancements	12.1 EC and later releases in multiple release trains
cable monitor Command	12.0(6)EC with additional enhancements and support in later releases in multiple release trains
cable intercept Command	12.0(5)T1, 12.0(6)SC, 12.1(2)EC, 12.2(4)BC1 and later releases in respective release trains
DOCSIS 2.0 SAMIS ECR Data Set	12.3(17a)BC and later 12.3 BC releases
Downstream Load Balancing Distribution with Upstream Load Balancing	12.3(17b)BC and later 12.3 BC releases
Dynamic Channel Change (DCC) for Loadbalancing	12.3(17a)BC and later 12.3 BC releases

Table 1-9 Cisco uBR7200 Series Routers Features by Cisco IOS Release (continued)

Feature	Supporting Cisco IOS Releases
Dynamic Ranging Support	12.1 EC and later releases in this and multiple release trains
Load Balancing for the Cisco CMTS	12.2(15)BC1 and later releases in the 12.2 BC and 12.3 BC release trains
Management Information Base (MIB) Changes and Enhancements	12.3(17a)BC and later 12.3 BC releases
MAX-CPE Override for Cable Modems	12.1(2)EC1 and later releases or release trains
Per-Modem Error Counter Enhancements	12.1(4)CX, 12.2(1)XF, and 12.2(4)BC1 and later releases in these release trains
Pre-equalization Control for Cable Modems	12.3(17a)BC and later 12.3 BC releases
Subscriber Traffic Management (STM) Version 1.1	12.3(9a)BC and later 12.3 BC releases
Usage Based Billing (SAMIS)	12.3(9a)BC and later 12.3 BC releases
Multicast Features	
Bidirectional PIM	12.1 EC, 12.2 BC
DOCSIS Set-top Gateway (DSG) 1.0	12.3(9a)BC and later 12.3 BC releases
Advanced-mode DOCSIS Set-Top Gateway Issue 1.1	12.3(13a)BC and later 12.3 BC releases
Advanced-mode DOCSIS Set-Top Gateway Issue 1.2	12.3(17a)BC2 and later 12.3 BC releases
IGMP Version 3	12.1(3)T and later releases in multiple release trains
IP Multicast Load Splitting across Equal-Cost Paths	12.0 XC and later releases in this and additional release trains
IP Multicast over ATM Point-to-Multipoint Virtual Circuits	12.0 XC and later releases in this and additional release trains
IP Multicast over Token Ring LANs	12.0 XC and later releases in this and additional release trains
Source Specific Multicast	12.0 XC and later releases in this and additional release trains
Stub IP Multicast Routing	12.0 XC and later releases in this and additional release trains
PacketCable and Voice Support Features	
PacketCable 1.0 With CALEA	12.3(13a)BC and later 12.3 BC releases
Security Features	
Access Control Lists	12.2(4)XF1 and later XF and BC releases 12.2(10)EC and later EC releases
Automated Double Authentication	12.0 XC and later releases in this and additional release trains
Cable Modem and Multicast Authentication Using RADIUS	12.0 XC and later releases in this and additional release trains
Cable Source Verification (cable source-verify Command)	11.3 XA with additional support and enhancements in later releases in additional release trains

Table 1-9 Cisco uBR7200 Series Routers Features by Cisco IOS Release (continued)

Feature	Supporting Cisco IOS Releases
Cisco IOS Firewall Feature Set	12.0(1)T and later releases in this and additional release trains
Cisco IOS Firewall Feature Enhancements	12.1 XM and later releases in this and additional release trains
Dynamic Mobile Hosts	12.1 CX, 12.2(4)XF and later releases in this and additional release trains
Dynamic Shared Secret for DOCSIS	12.2(15)BC1 and later releases in the 12.2 BC and 12.3 BC release trains
Dynamic Shared Secret (DMIC) with OUI Exclusion for DOCSIS	12.3(9a)BC and later 12.3 BC releases
HTTP Security	12.2(4)BC1 and later releases in this and additional release trains
Named Method Lists for AAA Authorization & Accounting	12.0 T, 12.0 CX, and later releases in these and additional release trains
Per-Modem Filters (Per-Modem and Per-Host Access Lists)	12.0(5)T1, 12.0(6)SC, and later releases in these and additional release trains
Per-User Configuration	12.0 T and later releases in this and additional release trains
Redirect-Number Support for RADIUS and TACACS+ Servers	12.0(4)XI with additional support and enhancements in later releases in additional release trains
Reflexive Access Lists	12.0 XC and later releases in this and additional release trains
Secure Shell (SSH) Supported in "k1" Images for Cisco uBR7200	12.1(1)T, 12.2(2)XA, 12.2 CX and later releases in this and additional release trains
Turbo Access Control Lists	12.1 EC, 12.2 CX, 12.2(4)XF1 and later releases in these and additional release trains
Vendor-Proprietary RADIUS Attributes	11.3(11)NA, 12.0 T and later releases in these and additional release trains
SNMP Features and Enhancements	
Individual SNMP Trap Support	12.1(3)T and later releases in this and additional release trains
LinkUp/Down Traps Support (RFC 2233)	12.1 EC and later releases in this and additional release trains
SNMPv2C	12.0 XC and later releases in this and additional release trains
SNMPv3	12.0 T and later releases in this and additional release trains
SNMP Cable Modem Remote Query	12.1 EC and later releases in this and additional release trains
SNMP Management Information Base (MIB) Enhancements	Multiple Cisco IOS releases and release trains
SNMP MIBs Changes and Updates in Cisco IOS Release 12.3(9a)BC	12.3(9a)BC and later 12.3 BC releases
SNMP Warm Start Trap	12.1 CX, 12.1 EC and later releases in these and additional release trains
Spectrum Management and Advanced Spectrum Management Features	
Advanced Spectrum Management	12.1 CX and later releases in this and additional release trains

Table 1-9 Cisco uBR7200 Series Routers Features by Cisco IOS Release (continued)

Feature	Supporting Cisco IOS Releases
Cable Modulation Profile Default Templates	12.1 EC and later releases in this and additional release trains
Downstream Traffic Shaping	12.0(7)XR2, 12.2(2)XF1 and later releases in these and additional release trains
Dynamic Upstream Modulation	12.1(3)EC and later releases in this and additional release trains
Guided and Scheduled Spectrum Management	Refer to the following features: • Traffic Shaping (Downstream or Upstream) • Frequency Hopping Capabilities • Dynamic Upstream Modulation (SNR-based) • Input Power Levels
Input Power Levels	11.3 NA, with additional enhancements in 12.0(7)XR2, 12.0(13)SC, 12.1(4)EC, 12.2(4)BC1 and later releases in these release trains
Spectrum Management Enhancements in Cisco IOS Release 12.3(9a)BC	12.3(9a)BC and later 12.3 BC releases
Upstream Traffic Shaping	11.3(9)NA and later releases in this and additional release trains
Testing, Troubleshooting and Diagnostic Features	
Cable Downstream Frequency Override	12.0 SC, 12.1 EC, 12.1T and 12.2BC release trains
Cable Flap List	11.3 NA, 12.0(4)XA, 12.0(7)XR, 12.1(2)EC, 12.1(5)EC, 12.1(7)CX, 12.2(4)BC1 and later releases in these and additional release trains
Cisco Broadband Troubleshooter (CBT) 3.2	12.3(9a)BC and later 12.3 BC releases
Cisco CMTS Static CPE Override	12.3(9a)BC and later 12.3 BC releases
Fast Fault Detection	12.2(15)BC1 and later 12.2 BC and 12.3 BC releases
Virtual Interfaces	
Virtual Interface Bundling on the Cisco uBR-MC28/U BPE	
VPN and Layer 2 Tunneling Features	
Dynamic SID/VRF Mapping Support	12.3(13a)BC and later 12.3 BC releases
NAT—Support for NetMeeting Directory (Internet Locator Service—ILS)	12.0 XC and later releases in this and additional release trains
IPv6 over L2VPN	12.3(17a)BC and later 12.3 BC releases
Mapping Service Flows to MPLS-VPN	12.2(11)BC2 and later 12.2 BC and 12.3 BC releases
MPLS VPN Support for Subinterfaces and Cable Interface Bundles	12.1 CX, 12.1 EC and later releases in these and additional release trains

Table 1-9 Cisco uBR7200 Series Routers Features by Cisco IOS Release (continued)

Feature	Supporting Cisco IOS Releases
Overlapping Subinterface IP Addresses	12.1(3)EC and later releases in this and additional release trains
Transparent LAN Services (TLS) and L2 Tunneling ATM/SIDs	12.3(9a)BC and later 12.3 BC releases
Transparent LAN Services (TLS) and L2 Virtual Private Networks	12.3(13a)BC and later 12.3 BC releases
VLAN Features	
HSRP over ISL in Virtual LAN Configurations	12.0 XC and later releases in this and additional release trains
WAN Optimization and Services Features	
Bandwidth Allocation Control Protocol (BACP)	12.0 XC and later releases in this and additional release trains
Closed User Group Selection Facility Suppress Option	12.1 T, 12.1 XM and later releases in these and additional release trains
Enhanced Local Management Interface (ELMI)	11.3(11)T, 12.0 XC and later releases in these and additional release trains
Frame Relay Enhancements	12.2(4)BC1 and later 12.2 BC and 12.3 BC releases
Frame Relay MIB Extensions	12.0 XC and later releases in this and additional release trains
Frame Relay Router ForeSight	12.0 XC and later releases in this and additional release trains
ISDN Advice of Charge	12.0 XC and later releases in this and additional release trains
ISDN Caller ID Callback	12.0 XC and later releases in this and additional release trains
ISDN Multiple Switch Types	12.0 XC and later releases in this and additional release trains
ISDN NFAS	12.0 XC and later releases in this and additional release trains
Microsoft Point-to-Point Compression (MPPC)	12.0 XC and later releases in this and additional release trains
MLPPP Support	12.3(13a)BC and later 12.3 BC releases
National ISDN Switch Types for BRI and PRI	12.0 XC and later releases in this and additional release trains
PAD Subaddressing	12.0 XC and later releases in this and additional release trains
PPPoE Termination Support on Cable Interfaces	12.1(5)T and later releases in this and additional release trains
Transparent LAN Services (TLS) and L2 Tunneling ATM/SIDs	12.3(9a)BC and later 12.3 BC releases
VPDN MIB and Syslog Facility	12.0 XC and later releases in this and additional release trains
X.25 Enhancements	11.3(11)NA and later releases in additional release trains
X.25 Switching Between PVCs and SVCs	11.3(11)NA and later releases in additional release trains

For feature comparisons between multiple releases, refer to the corresponding release notes, or to the *Cisco IOS Feature Navigator* on Cisco.com (registration required).

Cisco uBR7200 Series Router Configuration Tools

The Cisco uBR7200 series router provides you with the following configuration tools, allowing you flexibility in choosing your configuration method:

Autoinstall

The AutoInstall Using DHCP for LAN Interfaces feature replaces the use of the Bootstrap Protocol (BOOTP) with the use of the Dynamic Host Configuration Protocol (DHCP) for Cisco IOS AutoInstall over LAN interfaces. AutoInstall is a Cisco IOS software feature that provides for the configuration of a new routing device automatically when the device is initialized. DHCP (defined in RFC 2131) is based on the Bootstrap Protocol, which provides the framework for passing configuration information to hosts on a TCP/IP network. DHCP adds the capability of automatic allocation of reusable network addresses and additional configuration options.

In Cisco IOS Release 12.1(5)T, the IP address procurement phase of the AutoInstall process is now accomplished using DHCP for Ethernet, Token Ring, and FDDI interfaces. Before this release, IP addresses for LAN interfaces were obtained using BOOTP during the AutoInstall process. The AutoInstall Using DHCP for LAN Interfaces feature also allows the routing device to recognize IP address allocation messages coming from regular BOOTP servers, providing a seamless transition for those devices already using BOOTP servers for AutoInstall. Additionally, this feature allows for the uploading of configuration files using unicast Trivial File Transfer Protocol (TFTP).

Use the Autoinstall facility to configure the Cisco uBR7200 series router automatically *after* connection to your WAN. For further details, refer to these sections or documents:

- "Configuring the Cisco uBR7200 Series Using AutoInstall" section on page 2-10
- *Autoinstall Using DHCP for LAN Interfaces on Cisco.com*

  http://www.cisco.com/en/US/docs/ios/12_1t/12_1t5/feature/guide/dt_dhcpa.html

Cable Interface Setup Facility

Use the Setup facility *prior to* completing a WAN or LAN connection to your router. The Setup facility supports a number of functions so that cable interfaces and cable interface line cards are fully operational after initial setup. Refer to the "Configuring the Cisco uBR7200 Series Using the Setup Facility" section on page 2-17.

Cable Interface Extended Setup Facility

The Extended Setup facility enhances the Setup Facility by prompting you to configure each interface on the system as you progress through the CMTS configuration. The Configuration mode allows you to configure the Cisco uBR7200 series router manually if you prefer not to use Autoinstall or the Setup Facility. Refer to the "Configuring the Cable Interface with the Extended Setup Facility" section on page 2-25.

Cisco Network Registrar

The Cisco Network Registrar (CNR) is a configuration tool that automates dynamic IP address allocation to cable interfaces, PCs, and other devices on the broadband network. CNR allows you to track serial numbers and MAC addresses for each cable interface on your network, and reduces customer service involvement when tracking subscriber CPE equipment.

Cisco provides the CNR with each Cisco uBR7200 series router. CNR dramatically improves the reliability of naming and addressing services for enterprise and service provider networks. CNR provides scalable Domain Name System (DNS) and Dynamic Host Configuration Protocol (DHCP) services and forms the basis of a DOCSIS cable modem provisioning system.

For additional information about configuring or using CNR, refer to the document titled *Cisco Network Registrar for the Cisco uBR7200 Series Routers*:

http://www.cisco.com/en/US/docs/cable/cmts/ubr7200/feature/guide/6126inst.html

Interface Range Specification

The Interface Range Specification feature allows specification of a range of interfaces to which subsequent commands are applied and supports definition of macros that contain an interface range.

Implement the Interface Range Specification feature with the **range** keyword, which is used with the **interface** command. In the interface configuration mode with the range keyword, all entered commands are applied to all interfaces within the range until you exit interface configuration mode.

For additional command information, refer to the *Interface Range Specification* feature module on Cisco.com:

http://www.cisco.com/en/US/docs/ios/12_1t/12_1t4/feature/guide/range.html

Internal Modem Configuration File Editor

This feature adds support for internal DOCSIS cable modem configuration file storage and generation. The cable modem configuration file is generated and stored as part of the Cisco IOS configuration file. The DOCSIS configuration files are not stored in Flash memory but are automatically generated when requested for TFTP downloads to cable modems.

For the latest additional information about DOCSIS configuration files, refer to the document titled *Internal DOCSIS Configurator File Generator for the Cisco Cable Modem Termination System* on Cisco.com:

http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/ufgCFile.html

Manual Configuration Mode for the Cisco uBR7200 Series CMTS

The Configuration mode allows you to configure the Cisco uBR7200 series router manually if you prefer not to use Autoinstall or the Setup Facility. Refer to the "Configuring the Cisco uBR7200 Series Manually Using Configuration Mode" section on page 2-27.

Virtual Interface Support and Frequency Stacking Support

Cisco IOS Release 12.3(9a)BC supports virtual interfaces and frequency stacking on the Cisco uBR7246VXR router. Virtual interfaces allows a DS interface to be configured with up to eight upstream channels. Frequency stacking allows two frequencies to be configured on one physical connector.

For additional information about frequency stacking and virtual interfaces on the Cisco uBR7246VXR router, refer to the following document on Cisco.com:

- *Virtual Interfaces and Frequency Stacking Configuration on MC5x20S and MC28U Linecards*

  http://www.cisco.com/en/US/tech/tk86/tk804/technologies_white_paper09186a0080232b49.shtml

Bandwidth Management Features

This section describes the following bandwidth management feature available on the Cisco uBR7200 Series:

Load Balancing Support

Cisco IOS Release 12.3(9a)BC introduces support for Load Balancing on the Cisco uBR7246VXR router. The Load Balancing feature allows system operators to distribute cable modems across radio frequency (RF) downstreams and upstreams, to maximize bandwidth and usage of the cable plant.

The Load Balancing feature allows service providers to optimally use both downstream and upstream bandwidth, enabling the deployment of new, high-speed services such as voice and video services. This feature also can help reduce network congestion due to the uneven distribution of cable modems across the cable network and due to different usage patterns of individual customers.

By default, the Cisco CMTS platforms use a form of load balancing that attempts to equally distribute the cable modems to different upstreams when the cable modems register. You can refine this form of load balancing by imposing a limit on the number of cable modems that can register on any particular upstream, using the **cable upstream admission-control** command.

However, this default form of load balancing affects the cable modems only when they initially register with the Cisco CMTS. It does not dynamically rebalance the cable modems at later times, such as when they might change upstream channels in response to RF noise problems, or when bandwidth conditions change rapidly because of real-time traffic such as Voice over IP (VoIP) and video services. It also does not affect how the cable modems are distributed among downstream channels.

For additional information about configuring Load Balancing on the Cisco CMTS, refer to the following document on Cisco.com:

- *Configuring Load Balancing for the Cisco CMTS*

  http://www.cisco.com/en/US/docs/cable/cmts/troubleshooting_batch9/cmtslbg.html

Cisco IOS Command-Line Enhancements

In addition to new or enhanced commands that tie to a specific feature, this section describes general enhancements to Cisco IOS Software commands that support the Cisco uBR7200 series.

In some cases, additional feature descriptions that relate to these commands are available elsewhere in this chapter.

exec prompt timestamp Command

Cisco IOS Release 12.1(12c)EC and 12.2(8)BC2 add a new command, **exec prompt timestamp**. This command adds load information and a timestamp to all **show** commands. This can be useful for troubleshooting and system analysis.

The **exec prompt timestamp** command has the following syntax in line configuration mode:

```
Router(config-line)# [no] exec prompt timestamp
```

The command has the following syntax in User EXEC mode, so that users who do not know the **enable** password can also timestamp their **show** commands:

```
Router> terminal [no] exec prompt timestamp
```

The following example illustrates how to enable and disable the timestamp for the console connection:

```
Router# config t
Router(config)# line console 0
Router(config-line)# exec prompt timestamp
Router(config-line)# no exec prompt timestamp
```

The following example illustrates how to enable and disable the timestamp for the first five telnet connections:

```
Router(config)# line vty 0 4

Router(config-line)# exec prompt timestamp

Router(config-line)# no exec prompt timestamp
```

The following example illustrates how to enable and disable the timestamp when logged into User EXEC mode:

```
Router> terminal exec prompt timestamp

Router> terminal no exec prompt timestamp
```

parser cache Command

A new global configuration command, [**no**] **parser cache**, allows you to enable or disable the parser cache feature on the Cisco uBR7200 series.The parser cache feature is enabled by default on all platforms using Cisco IOS Release 12.1(5)T or later.

The parser cache feature optimizes the parsing (translation) of Cisco IOS software configuration command lines by remembering how to parse recently encountered command lines. This feature improves the scalability of the Cisco IOS software command-line interface (CLI) parser when processing large configuration files.

This improvement is especially useful for those cases in which thousands of virtual circuits must be configured for interfaces, or hundreds of access control lists (ACLs) are required. The parser chain cache can rapidly recognize and translate configuration lines that differ slightly from previously used configuration lines (for example, pvc 0/100, pvc 0/101, and so on).

Note Testing indicates an improvement to load time of between 30% and 36% for large configuration files when using the parser cache.

For additional information, refer to the *Parser Cache* feature module on Cisco.com:

http://www.cisco.com/en/US/docs/ios/12_1t/12_1t5/feature/guide/dt5parse.html

show Command Enhancements

The Cisco uBR7200 series universal broadband routers contain the following additional or changed **show** commands.

show cable qos

The **show cable qos** command is changed to **show cable qos profile** *n* command, where the optional argument *n* can be used to display a specific profile.

Note The release notes up to and including Cisco IOS Release 12.0(12)SC stated that the show cable qos command was changed to **show cable qos-profile** *n* command, with a hyphen between "qos" and "profile". This was incorrect.

show int cx/y sid

The **show int cx/y sid** command displays more complete Service ID (SID) status information.

show cable modem

The **show cable modem** command displays a list of options for a single modem to be specified by entering either the cable modem's IP address or MAC address.

show cable modulation-profile

The **show cable burst-profile** command has been removed. Its functions have been incorporated into the **show cable modulation-profile** command, which includes an added option number that displays the modulation profile number.

show cable modem summary

Commencing with Cisco IOS Release 12.1(6) EC, the **show cable modem summary** command is enhanced with the following options to display per-card and per-port totals:

- **show cable modem summary total**—Displays a summary and a total for all modems on the chassis.
- **show cable modem summary** *cable x/0* **total**—Displays a summary of modems on a specified card.
- **show cable modem summary** *cable x/0* **upstream** *port1 port2* **total**—Displays a summary of modems on the specified card and specified range of ports.
- **show cable modem summary cable** *x/0 cable y/0* **total**—Displays a summary of modems on the specified range of cards.
- **show cable modem summary cable** *x/0 cable y/0* **upstream** *port1 port2* **total**—Displays a summary of modems on the specified range of ports on the specified range of cards.

For additional command information, refer to the *Cisco IOS CMTS Cable Command Reference Guide* on Cisco.com:

http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html

Cisco IOS Release 12.3(9a)BC Command-Line Interface (CLI) Enhancements

Cisco IOS Release 12.3(9a)BC supports the following new or enhanced command-line interface:

For additional information about these command changes, refer to this document on Cisco.com:

- *CiscoIOS CMTS Cable Command Reference Guide*

  http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html

cable logging layer2events

To save DOCSIS events that are specified in Cable Device MIB to the cable logging buffer (instead of to the general logging buffer), use the **cable logging layer2events** command in global configuration mode. To disable the logging of DOCSIS events to the cable logging buffer, use the **no** form of this command.

cable logging layer2events

no cable logging layer2events

Syntax Description

This command has no additional arguments or keywords.

Defaults

DOCSIS events are saved to the general logging buffer on the Cisco CMTS by default.

Command Modes

Global configuration mode

Command History

Release	Modification
12.3(9a)BC	This command was introduced on the Cisco uBR10012 and Cisco uBR7246VXR universal broadband routers.

Usage Guidelines

Use the **show cable logging** command to check whether the logging feature is enabled and the status of the logging buffer.

Examples

The following example shows how to clear the log buffer that contains a bad IP source address error messages:

```
Router# show cable logging summary

Cable logging: BADIPSOURCE Enabled
Total buffer size (bytes): 1000000
```

```
Used buffer size (bytes) : 36968
Logged messages : 231

Router# clear cable logging badipsource

Router# show cable logging summary

Cable logging: BADIPSOURCE Enabled
Total buffer size (bytes): 1000000
Used buffer size (bytes) : 0
Logged messages : 0
```

Related Commands

Command	Description
cable logging badipsource	Logs error messages about bad IP source addresses on the cable interfaces to a separate log buffer,
show cable logging	Indicates whether the logging feature is enabled and the status of the logging buffer.

For additional information about logging events on the Cisco CMTS, refer to the following document on Cisco.com:

- *Cisco IOS CMTS Cable Command Reference Guide*

  http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html

cable source-verify

To enable verification of IP addresses or service IDs (SIDs) for CMs and CPE devices on the upstream, use the **cable source-verify** command in global configuration, cable interface configuration or subinterface configuration modes. To disable verification, use the **no** form of this command.

Cable Interface and Subinterface Configuration Modes

cable source-verify [**dhcp** | **leasetimer** *value* | **leasequery-filter upstream** *query-num interval*]

no cable source-verify

Global Configuration Mode

cable source-verify leasequery-filter downstream *query-num interval*

no cable source-verify

Syntax Description

dhcp	(Optional) Specifies that queries will be sent to verify unknown source IP addresses in upstream data packets. **Note** Do not enable the local DHCP server on the Cisco CMTS and configure local DHCP address pools, using the **ip dhcp pool** command, when using this option, because this prevents DHCP address validation.
leasetimer *value*	(Optional) Specifies the time, in minutes, for how often the router should check its internal CPE database for IP addresses whose lease times have expired. The valid range for value is 1 to 240 minutes, with a default of 60 minutes. **Note** The **leasetimer** option takes effect only when the **dhcp** option is also used on an interface. Also, this option is supported only on the master interface and cannot be configured on subinterfaces. Configuring it for a master interface automatically applies it to all subinterfaces.
leasequery-filter upstream *query-num interval*	(Optional) Enables upstream lease queries to be defined on a per-SID basis to reduce the chance of Denial of Service attacks. • *query-num*— Number of leased queries per SID. • *interval*—Size of timer window in seconds.
leasequery-filter downstream *query-num interval*	(Optional) Enables downstream lease queries to be defined on a per-SID basis to reduce the chance of Denial of Service attacks. • *query-num*— Number of leased queries for an unknown SID. • *interval*—Size of timer window in seconds.

Defaults

Disabled. When the **dhcp** option is specified, the **leasetimer** option is set by default to 60 minutes.

Command Modes

Global configuration, Cable interface configuration or subinterface configuration

Note Configuring the **cable source-verify** command on the master interface of a bundle will configure it for all of the slave interfaces in the bundle as well.

Command History

Release	Modification
11.3 XA	This command was introduced.
12.0(7)T	The **dhcp** keyword was added.
12.0(10)SC, 12.1(2)EC	Support was added for these trains.
12.1(3a)EC	Subinterface support was added.
12.1(13)EC, 12.2(11)BC1	The **leasetimer** keyword was added.
12.2(15)BC1	The verification of CPE devices was changed when using the **dhcp** keyword.

Release	Modification
12.2(15)BC2	Support for verifying CMs and CPE devices that are on a different subnet than the cable interface was enhanced to use Reverse Path Forwarding (RFP).
12.3(9a)BC	In order to protect the Cisco CMTS from denial of service attacks, Cisco IOS Release 12.3(9a)BC adds the option of using a per SID basis for deriving lease queries from CPE devices. This release also introduces a global rate limit for lease queries initiated by downstream traffic. These enhancements reduce the CPU utilization of DHCP Receive and ISR processes when the Cisco CMTS is configured with the **cable source-verify dhcp** and **no cable arp** commands.

For additional information about this and other commands, refer to the following document on Cisco.com:

- *Cisco IOS CMTS Cable Command Reference Guide*

  http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html

cable submgmt default

To enable the Cisco CMTS Static CPE Override feature on the Cisco CMTS, use the **cable submgmt default** command in global configuration mode. This command enables field technicians to add a temporary CPE device behind the subscriber's cable modem. The temporary CPE device shares the same SID settings as the original CPE device, even though the temporary CPE device has a different MAC address. The original CPE device automatically changes from *dhcp cpe* to *static cpe* in the CMTS host routing tables, and the CPE device continues to receive service with the same SID. To disable Cisco CMTS Static CPE Override on the Cisco CMTS, use the **no** form of this command. This automatically updates the routing tables and enables the MAC address from the technician's laptop for a future field service connection at a different location.

cable submgmt default {**active** | **filter-group** {**cm** | **cpe**} | **learnable** | **max-cpe**}

no cable submgmt default

Syntax Description

active	Keyword enables Cisco CMTS Static CPE Override, granting local CPE control for subscriber management filtering (as defined by existing SID settings).
filter-group {**cm** | **cpe**}	Keyword enables one ore more temporary CPE devices to inherit the characteristics of an existing filter group, either on the downstream or the upstream of the cable modem (**cm**) or the CPE device (**cpe**). • **filter-group cm {downstream | upstream}**—This keyword combination enables one or more temporary CPE devices to inherit and filter by the default downstream cable modem group, or by the default upstream cable modem group. • **filter-group cpe {downstream | upstream}**—This keyword combination enables one or more temporary CPE devices to inherit and filter by the default downstream CPE group, or by the default upstream CPE group.

learnable	Keyword automatically enables one or more temporary CPE devices to learn and to operate within the CPE IP address(es) in the Cisco CMTS routing table.
max-cpe	Keyword sets the maximum number of IP addresses to be permitted behind a cable modem while the Cisco CMTS Static CPE Override feature is enabled. This keyword enables multiple temporary CPE devices in the range of 0 to 1024.

Defaults

This command is disabled by default.

Command Modes

Global configuration mode

Command History

Release	Modification
12.3(9a)BC	This feature was introduced on Cisco uBR10012 and Cisco uBR7200 series universal broadband routers.

Usage Guidelines

Prior to using this command, the first (existing) DHCP CPE device maintains its DHCP dynamic MAC address behind the cable modem. The SID is assigned to this IP address.

However, by enabling Static CPE override, you gain the following states and options on two CPE devices behind the cable modem.

- The SID definition on the first CPE device is assigned a different static IP address. This enables you to change the existing (dynamic) DHCP IP address to a static IP address without first clearing the DHCP CPE host entries from the Cisco CMTS. The CPE IP state changes from **dhcp** to **static** cpe.
- This static override allows a second CPE device with a second MAC address behind the same cable modem with SID1 to be assigned same IP address as the first CPE device.

Note The second CPE device changes from **dhcp cpe** to **static CPE** in the CMTS host tables.

Examples

The following example enables Cisco CMTS Static CPE Override in the field, enabling more or more additional CPE devices to be added behind a subscriber's cable modem:

```
Router(config)# cable submgmt default active
```

The following example configures the Cisco CMTS to accept a temporary CPE device, which inherits and filters by the subscriber's default downstream cable modem group:

```
Router(config)# cable submgmt default filter-group cm downstream
```

The following example configures the Cisco CMTS to accept a temporary CPE device, and to update the temporary CPE device with the current routing table from the Cisco CMTS:

```
Router(config)# cable submgmt default learnable
```

The following example configures the Cisco CMTS to accept a maximum of five temporary CPE devices behind a subscriber's cable modem:

```
Router(config)# cable submgmt default max-cpe 5
```

Related Commands

Command	Description
show cable host	Displays the CPE devices (hosts) residing behind a specified cable modem (MAC address).

show cable tech-support

Cisco IOS Release 12.3(9a)BC introduces changes to the output of the **show cable tech-support** command. This change allows users with large numbers of online cable modems to collect the necessary information without consuming the console session for a long period of time.

To display general information about the router when reporting a problem, use the **show cable tech-support** command in privileged EXEC mode.

show cable tech-support

Syntax Description

This command has no additional arguments or keywords.

Defaults

This command has no default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.2	This command was introduced.
12.1(1a)T1	This command was modified to include information about the cable clock card.
12.2(15)BC2	This command added several **show pxf** commands to the display on the Cisco uBR10012 router.
12.3(9a)BC	The output of the command was significantly shortened by moving a number of **show** commands (the ones that display information about individual cable modems) to the **show tech-support** command. This release also adds support for an option to display information about only one specific cable interface.

Examples

The following example illustrates the cable modem and interface information from a Cisco uBR7246VXR router on which Cisco IOS Release 12.3(9a)BC is installed.

```
Router# show cable tech-support
```

For additional information about this and other commands, refer to the following document on Cisco.com:

- *Cisco IOS CMTS Cable Command Reference Guide*

  http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html

show controllers cable

Cisco IOS Release 12.3(9a)BC removes the **tech-support** keyword from the **show controllers cable** command. This change allows users with large numbers of online cable modems to collect the necessary information without consuming the console session for a long period of time.

Additional and related improvements are also available for the **show tech-support** command.

To display information about the interface controllers for a cable interface on the Cisco CMTS router, use the **show controllers cable** command in user EXEC or privileged EXEC mode.

show controllers cable {*slot/port* | *slot*/*subslot*/*port*} [**downstream** | **upstream** [*port*] | [**mem-stat**] [**memory**] [**proc-cpu**]] [**tech-support**]

Syntax Description

slot/port	Identifies the cable interface and downstream port on the Cisco uBR7100 series and Cisco uBR7200 series routers. On the Cisco uBR7100 series router, the only valid value is **1/0**. On the Cisco uBR7200 series router, *slot* can range from 3 to 6, and *port* can be 0 or 1, depending on the cable interface.
slot/port	Identifies the cable interface on the Cisco uBR7246VXR router. Th syntax for the Cisco uBR10012 router is slot/subslot/port, where the following are the valid values: • *slot* = 5 to 8 • *subslot* = 0 or 1 • *port* = 0 to 4 (depending on the cable interface)
downstream	(Optional) Displays downstream interface status.
upstream	(Optional) Displays upstream interface status.
port	(Optional) Specifies the desired upstream port. Valid values start with 0 for the first upstream port on the cable interface line card.
mem-stat	(Optional) Displays the output from the **show memory statistics** command to display a summary of memory statistics for a Broadband Processing Engine (BPE) cable interface line card.
memory	(Optional) Displays the output from the **show memory** command to display a summary of memory statistics, including the memory as it is allocated per process, for a Broadband Processing Engine (BPE) cable interface line card.
proc-cpu	(Optional) Displays the output from the **show processes cpu** command to display the processor status for a Broadband Processing Engine (BPE) cable interface line card.
tech-support	(Optional) Displays information from a number of different show commands for technical support purposes. The exact output depends on the platform, configuration, and type of protocols being used

Command Modes User EXEC, Privileged EXEC

Command History

Release	Modification
11.3 NA	This command was introduced.
12.0(2)XC	This command was modified to show a number of additional fields.
12.1(5)EC1	Support was added for the Cisco uBR7100 series router, including information about the Cisco uBR7100 series integrated upconverter.
12.2(1)XF1	Support was added for the Cisco uBR10012 router.
12.0(16)SC2, 12.1(10)EC1, 12.2(4)BC1b	The algorithm for calculating the SNR value was enhanced for a more accurate value.
12.2(15)CX	Support was added for the Cisco uBR-MC28U/X cable interface line card, including the display of the number of packets dropped because they were for a Service Flow ID (SFID) of 0.
12.2(15)BC2b	The **mem-stat**, **memory**, and **proc-cpu** options were added to obtain processor information from the onboard processor on Broadband Processing Engine (BPE) cable interface line cards, such as the Cisco uBR-MC16U/X, Cisco uBR-MC28U/X, and Cisco uBR-MC5X20S/U cards.
12.3(9a)BC	Adds the **tech-support** option to improve information required during technical support.

Usage Guidelines The **mem-stat**, **memory**, and **proc-cpu** keywords execute the related command on the processor that runs on added to obtain the relevant information from the onboard processor on Broadband Processing Engine (BPE) cable interface line cards, such as the Cisco uBR-MC16U/X, Cisco uBR-MC28U/X, and Cisco uBR-MC5X20S/U cards. This allows you to obtain information that is specific for that particular cable interface card, as opposed to having to run these commands on the entire router.

Note The **mem-stat**, **memory**, and **proc-cpu** options are not available for cable interface line cards that do not contain an onboard processor (for example, the Cisco uBR-MC16C card).

Examples The following is sample output for the downstream connection for slot 3 on port 0 on Cisco CMTS router from the **show controllers cable downstream** command:

```
CMTS01# show controllers cable 3/0 downstream

Cable 3/0 Downstream is up
Frequency not set, Channel Width 6 MHz, 64-QAM, Symbol Rate 5.056941 Msps
FEC ITU-T J.83 Annex A, R/S Interleave I=12, J=17
```

Table 10 describes the fields displayed by the **show controllers cable downstream** command.

Table 10 show controllers cable downstream Field Descriptions

Field	Description
Cable	Slot number/port number indicating the location of the Cisco cable interface line card.
Downstream is up	Indicates that the RF downstream interface is enabled.
Frequency	Transmission frequency of the RF downstream. (This information may not match the current transmission frequency, which is external on CMTS platforms that use an external upconverter.)
Channel Width	Indicates the width of the RF downstream channel.
QAM	Indicates the modulation scheme.
Symbol Rate	Indicates the transmission rate (in number of symbols per second).
FEC ITU-T	Indicates the Motion Picture Experts Group (MPEG) framing standard.
R/S Interleave I/J	Indicates Reed Solomon framing based on ITU S.83-B.

The following example illustrates the information from the **show controllers cable** command on a Cisco uBR7246VXR router on which Cisco IOS Release 12.3(9a)BC is installed.

```
Router# show controllers cable x/y
```

For additional information about this and other commands, refer to the following document on Cisco.com:

- *Cisco IOS CMTS Cable Command Reference Guide*

  http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html

show tech-support

Cisco IOS Release 12.3(9a)BC shortens the output of the **show tech-support** command on the Cisco uBR10012 and the Cisco uBR7246VXR routers. This change allows users with large numbers of online cable modems to collect information without consuming the console session for a long period of time.

To display general information about the Cisco CMTS router when reporting a problem to Cisco technical support, use the **show tech-suppor**t command in privileged EXEC mode.

show tech-support [**page**] [**password**] [**cef** | **ipc** | **ipmulticast** | **isis** | **mpls** | ospf | **rsvp**]

Note The **show tech-support** command automatically displays the output of a number of different **show** commands. The exact output depends on the platform, configuration, and type of protocols being used.

Note The **show tech-support** includes most of the information shown in the **show cable tech-support** command.

Syntax Description

page	(Optional) Causes the output to display a page of information at a time. Use the Return key to display the next line of output or use the space bar to display the next page of information. If not used, the output scrolls (that is, does not stop for page breaks).
password	(Optional) Leaves passwords and other security information in the output. If not used, passwords and other security-sensitive information in the output are replaced with the label "<removed>" (this is the default).
cef	(Optional) Displays information about the Cisco Express Forwarding (CEF) protocol configuration and status.
ipc	(Optional) Displays information about interprocess communications on the Cisco router.
ipmulticast	(Optional) Displays information about the IP multicast configuration and status.
isis	(Optional) Displays information about the Connectionless Network Service (CLNS) and Intermediate System-to-Intermediate System (IS-IS) routing protocol configuration and status. **Note** IS-IS support is provided only on CMTS platforms running Cisco IOS images that have a “-p-” as part of the image name.
mpls	(Optional) Displays information about Multiprotocol Label Switching (MPLS) on the Cisco router, which instructs the routers and the switches in the network on where to forward the packets based on preestablished IP routing information.
ospf	(Optional) Displays information about the Open Shortest Path First (OSPF) routing algorithm and status on the Cisco router.
rsvp	(Optional) Displays information about the IP Resource Reservation Protocol (RSVP) configuration and status.

For additional information about this and other commands, refer to the following document on Cisco.com (updated through Cisco IOS Release 12.3(9a)BC):

- *Cisco IOS CMTS Cable Command Reference Guide*

  http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html

Cisco Quality of Service Features

Networks must provide secure, predictable, measurable, and sometimes guaranteed services. Achieving the required Quality of Service (QoS) by managing delay, delay variation (jitter), bandwidth, and packet loss parameters on a network becomes the secret to a successful end-to-end business solution. Cisco QoS is the set of techniques to manage network resources. The Cisco uBR7200 series CMTS offers the following Cisco QoS features, in addition to supporting additional DOCSIS QoS features.

- Cisco Network-Based Application Recognition (NBAR), page 1-46
- RTP Header Compression, page 1-46

For additional information, refer to the *Cisco IOS Quality of Service* Web page on Cisco.com:

http://www.cisco.com/en/US/technologies/tk389/tk813/technologies_white_paper0900aecd802b68b1_ps6558_Products_White_Paper.html

Cisco Network-Based Application Recognition (NBAR)

Cisco IOS Release 12.1(10)EC added support for Cisco IOS Network-Based Application Recognition (NBAR). The NBAR feature is a new classification engine that can recognize a wide variety of network applications, including Web-based applications, client/server applications, and other difficult-to-classify protocols that dynamically assign TCP or UDP port numbers.

NBAR enhances existing methods of application-recognition by adding several new classification features:

- Classification of applications that use statically assigned TCP/UDP port numbers, that use dynamically assigned TCP/UDP port numbers, or that use protocols other than TCP and UDP
- Classification of HTTP traffic by URL, host, or MIME type
- Classification of Citrix ICA traffic by application name
- Classification of application traffic using subport information

NBAR can also classify static port protocols. Although access control lists (ACLs) can also be used for this purpose, NBAR is easier to configure and can provide other options and classification statistics that are not available when using ACLs.

After NBAR recognizes an application, the Cisco uBR7200 series router can invoke specific services appropriate for that application. These services can provide QoS features such as:

- Guaranteed bandwidth
- Bandwidth limits
- Traffic shaping
- Packet coloring

The Cisco IOS NBAR feature can also be used to detect and respond to denial-of-service and other types of network attacks. Cisco IOS NBAR uses a protocol description language module (PDLM) to define the rules by which the NBAR processes recognize an application. New PDLM definitions can usually be loaded without the need for a Cisco IOS software upgrade or a router reboot, allowing for a rapid response to discovered attacks.

Note For basic information on configuring and using the Cisco IOS NBAR feature, see the *Network-Based Application Recognition* feature module.

For information on configuring NBAR for Quality of Service (QoS) control, see the "Configuring Network-Based Application Recognition" chapter of theCisco IOS Release 12.2 Quality of Service Solutions Configuration Guide.

These documents are available on Cisco.com and the Customer Documentation CD-ROM.

Tip Cisco.com also contains a technical note, *Using Network-Based Application Recognition and Access Control Lists for Blocking the Code Red Worm*, that provides information on using NBAR to block denial-of-service attacks. Registration and login is required to view this document.

RTP Header Compression

Real-Time Transport Protocol (RTP) is the Internet Standard (RFC 1889) protocol for the transport of real-time data. It is intended to provide end-to-end network transport functions for applications that support audio, video, or simulation data over multicast or unicast network services.

RTP provides support for real-time conferencing of groups of any size within the Internet. This support includes source identification and support for gateways such as audio and video bridges as well as multicast-to-unicast translators. RTP offers QoS feedback from receivers to the multicast group, and support for the synchronization of different media streams.

RTP includes a data portion and a header portion. The data portion of RTP is a thin protocol that provides support for the real-time properties of applications, such as continuous media, including timing reconstruction, loss detection, and content identification.

The header portion of RTP is considerably large. As shown in Figure 16, the minimal 12 bytes of the RTP header, combined with 20 bytes of IP header (IPH) and 8 bytes of UDP header, create a 40-byte IP/UDP/RTP header. For compressed-payload audio applications, the RTP packet typically has a 20-byte to 160-byte payload. Given the size of the IP/UDP/RTP header combinations, it is inefficient to send the IP/UDP/RTP header without compressing it.

To avoid the unnecessary consumption of available bandwidth, the RTP header compression feature—referred to as CRTP—is used on a link-by-link basis.

For configuration information and additional explanation, refer to the Link Efficiency Mechanisms" chapters of the *Cisco IOS Quality of Service Solutions Configuration Guide*, Release 12.2 on Cisco.com.

DHCP Servers and Feature Support

Cisco IOS software supports multiple DHCP features and server functions on the network for the Cisco uBR7200 series.

- Configurable Leasequery Server, page 1-47
- DHCP MAC Address Exclusion List for cable-source verify dhcp Command, page 1-48
- See the "DOCSIS 1.1 Feature Support" section on page 1-57 for additional DHCP features.

Configurable Leasequery Server

Previously, lease query requests could only be sent to the DHCP server. Beginning with Cisco IOS Release 12.3(17a)BC, an alternate server may be configured to receive the requests.

There are a few restrictions:

- Lease queries are sent to the DHCP server unless an alternate server is configured.
- Only one alternate server may be configured.
- Users are responsible for the synchronization of the DHCP server and configured alternate server.
- If the configured alternate server fails, lease query requests will not be diverted back to the DHCP server.

Regardless of which server is configured (DHCP or alternate), unknown IP addresses that are found in packets for customer premises equipment (CPE) devices that use the cable modems on the cable interface are verified. The DHCP server or configured alternate server returns a DHCP ACK message with the MAC address of the CPE device that has been assigned this IP address, if any.

To configure the Cisco CMTS router to send DHCP LEASEQUERY requests to an alternate server, use the **cable source-verify dhcp server** *ipaddress* and **no cable arp** commands. (To configure the DHCP server instead, use the **cable source-verify dhcp** and **no cable arp** commands.)

For additional information about this feature, refer to the following documents on Cisco.com:

- *Filtering Cable DHCP Lease Queries on Cisco CMTS Routers*

  URL: http://www.cisco.com/en/US/docs/cable/cmts/feature/cblsrcvy.html

DHCP MAC Address Exclusion List for cable-source verify dhcp Command

Cisco IOS Release 12.3(13a)BC introduces the ability to exclude trusted MAC addresses from standard DHCP source verification checks, as supported in previous Cisco IOS releases for the Cisco CMTS. This feature enables packets from trusted MAC addresses to pass when otherwise packets would be rejected with standard DHCP source verification. This feature overrides the **cable source-verify** command on the Cisco CMTS for the specified MAC address, yet maintains overall support for standard and enabled DHCP source verification processes. This feature is supported on Performance Routing Engine 1 (PRE1) and PRE2 modules on the Cisco uBR10012 router chassis.

To enable packets from trusted source MAC addresses in DHCP, use the **cable trust** command in global configuration mode. To remove a trusted MAC address from the MAC exclusion list, use the **no** form of this command. Removing a MAC address from the exclusion list subjects all packets from that source to standard DHCP source verification.

cable trust *mac-address*

no cable trust *mac-address*

Syntax Description

mac-address	The MAC address of a trusted DHCP source, and from which packets will not be subject to standard DHCP source verification.

Usage Guidelines

This command and capability are only supported in circumstances in which the Cable Source Verify feature is first enabled on the Cisco CMTS.

When this feature is enabled in addition to cable source verify, a packet's source must belong to the MAC Exclude list on the Cisco CMTS. If the packet succeeds this exclusionary check, then the source IP address is verified against Address Resolution Protocol (ARP) tables as per normal and previously supported source verification checks. The service ID (SID) and the source IP address of the packet must match those in the ARP host database on the Cisco CMTS. If the packet check succeeds, the packet is allowed to pass. Rejected packets are discarded in either of these two checks.

Any trusted source MAC address in the optional exclusion list may be removed at any time. Removal of a MAC address returns previously trusted packets to non-trusted status, and subjects all packets to standard source verification checks on the Cisco CMTS.

Note When the **cable source-verify dhcp** feature is enabled, and a statically-defined IP address has been added to the CMTS for a CM using the **cable trust** command to override the **cable source-verify dhcp** checks for this device, packets from this CM will continue to be dropped until an entry for this CM is added to the ARP database of the CMTS. To achieve this, disable the **cable source-verify dhcp** feature, ping the CMTS from the CM to add an entry to the ARP database, and re-enable the c**able source-verify dhcp** feature.

For additional information about the enhanced Cable Source Verify DHCP feature, and general guidelines for its use, refer to the following documents on Cisco.com:

- *IP Address Verification for the Cisco uBR7200 Series Cable Router*
  http://www.cisco.com/en/US/docs/ios/12_0t/12_0t7/feature/guide/sourcver.html
- *Filtering Cable DHCP Lease Queries*
  http://www.cisco.com/en/US/docs/cable/cmts/feature/cblsrcvy.html
- *Cisco IOS CTMS Cable Command Reference Guide*
  http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html

- CABLE SECURITY, *Cable Source-Verify and IP Address Security*, White Paper
  http://www.cisco.com/en/US/tech/tk86/tk803/technologies_tech_note09186a00800a7828.shtml

DOCSIS 1.0 Feature Support

The Cisco uBR7200 series and associated Cisco IOS software support multiple DOCSIS 1.0 enhancements, extensions, and features.

DOCSIS 1.0 Baseline Privacy

DOCSIS baseline privacy interface (BPI) gives subscribers data privacy across the RF network, encrypting traffic flows between the CMTS and cable modem. BPI ensures that a cable modem, uniquely identified by its Media Access Control (MAC) address, can obtain keying material for services only it is authorized to access.

To enable BPI, choose software at both the CMTS and cable modem that support the mode of operation. For the Cisco uBR7200 series software, choose an image with “k1” in its file name or BPI in the feature set description.

The cable modem must also support BPI. CMs must have factory-installed RSA private/public key pairs to support internal algorithms to generate key pairs prior to first BPI establishment. BPI must be enabled using the DOCSIS configuration file.

Note RSA stands for Rivest, Shamir, and Adelman, inventors of a public-key cryptographic system.

DOCSIS 1.0 Baseline Privacy Interface Encryption and Encrypted Key Exchange

The Cisco uBR7200 series supports full DOCSIS 1.0 BPI specifications. The BPI for DOCSIS 1.0 protects user data privacy across the shared-medium cable network and prevents unauthorized access to DOCSIS-based data transport services across the cable network. BPI encrypts traffic across the RF interface between the cable modem and CMTS, and includes authentication, authorization, and accounting (AAA) features.

The level of data privacy is roughly equivalent to that provided by dedicated line network access services such as analog modems or digital subscriber lines (DSL). BPI provides basic protection of service, ensuring that a cable modem, uniquely identified by its MAC address, can obtain keying material for services only when it is authorized to access.

Note Encryption and decryption are subject to export licensing controls.

BPI supports access control lists (ACLs), tunnels, filtering, protection against spoofing, and commands to configure source IP filtering on RF subnets to prevent subscribers from using source IP addresses that are not valid.

Baseline privacy extensions permit the encryption of data transferred between the cable modem and the Cisco uBR7200 series universal broadband router. The key management protocol defined by baseline privacy allows Cisco uBR7200 series universal broadband routers to provide two types of keys to cable modems. The Key Exchange Key (KEK) decrypts the Traffic Exchange Keys (TEK). The TEK is the key used to encrypt and decrypt data packets.

DOCSIS 1.0 Concatenation Override Featurette

Cisco IOS release 12.3(13a)BC introduces support for the DOCSIS 1.0 concatenation override feature on the Cisco uBR10012 router. This feature provides the ability to disable concatenation on DOCSIS 1.0 cable modems, even in circumstances where concatenation is otherwise supported for the upstream channel.

DOCSIS 1.0 concatenation allows the cable modem to make a single-time slice request for multiple packets, and to send all packets in a single large burst on the upstream. Concatenation was introduced in the upstream receive driver in the previous Cisco IOS releases that supported DOCSIS 1.0 +. Per-SID counters were later added in Cisco IOS release 12.1(4)CX for debugging concatenation activity.

In some circumstances, overriding concatenation on DOCSIS 1.0 cable modems may be preferable, and Cisco IOS release 12.3(13a)BC supports either option.

Note Even when DOCSIS 1.0 concatenation is disabled with this feature, concatenation remains enabled for cable modems that are compliant with DOCSIS 1.1 or DOCSIS 2.0.

To enable DOCSIS 1.0 concatenation override with Cisco IOS release 12.3(13a)BC and later releases, use the new **docsis10** keyword with the previously supported **cable upstream** <*n*> **concatenation** command in privileged EXEC mode:

cable upstream <*n*> **concatenation docsis10**

Syntax Description

n	Specifies the upstream port number. Valid values start with 0 for the first upstream port on the cable interface line card.

Examples

The following example illustrates DOCSIS 1.0 concatenation override on the Cisco uBR7246VXR router:

```
Router# no cable upstream 0 concatenation docsis10
```

In this example, DOCSIS 1.0 cable modems are updated with REG-RSP so that they are not permitted to use concatenation.

For additional information about this command, refer to the *Cisco IOS CMTS Cable Command Reference Guide* on Cisco.com:

http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html

DOCSIS 1.0 Extensions

The Cisco uBR7200 series supports the following DOCSIS 1.0 Quality of Service (QoS) extensions:

- Multi-Service ID (SID) support, allowing the definition of multiple SIDs on the upstream—Voice traffic can be designated on a higher QoS committed information rate (CIR) secondary SID, while data traffic can be forwarded on a best-effort basis on a primary SID. Secondary SIDs are higher QoS CIR-type classes that have a nonzero minimum reserved rate (CIR-type service). These SIDs receive preferential treatment at the CMTS for grants over any tiered best-effort type data SID of that upstream. Reliable operation with voice requires multiple SIDs—at least two per cable modem to separate voice from data. In DOCSIS 1.0, SIDs are set up statically. When supporting DOCSIS 1.0 extensions, SIDs can be set up statically or dynamically. Both the CMTS and cable modem must support this capability.
- Cable modem-initiated dynamic MAC messages—Dynamic Service Addition (DSA) and Dynamic Service Deletion (DSD). These messages allow dynamic SIDs to be created and deleted at run-time on a per-VoIP call basis.
- Unsolicited grant service (constant bit rate [CBR] scheduling) on the upstream—This helps provide a higher-quality channel for upstream VoIP packets from an Integrated Telephony Cable Modem (ITCM) such as the Cisco uBR924 cable access router.
- Ability to provide separate downstream rates for any given ITCM, based on the IP-precedence value in the packet—This helps separate voice signaling and data traffic that goes to the same ITCM to address rate-shaping purposes.
  - **Concatenation**—To increase the per- cable modem upstream throughput in certain releases of software, Cisco uBR7200 series software supports a concatenated burst of multiple MAC frames from a cable modem that supports concatenation.

Note All DOCSIS 1.0 extensions are activated only when a cable modem or Cisco uBR924 that supports these extensions solicits services using dynamic MAC messages or the feature set. If the CMs in your network are pure DOCSIS 1.0-based, they receive regular DOCSIS 1.0 treatment from the CMTS.

DOCSIS 1.0 Quality of Service

The Cisco uBR7200 series universal broadband routers support quality of service (QoS) as defined by the DOCSIS 1.0 specification. Service class profiles can be configured through the command-line interface to support the QoS profile number, traffic priority, maximum upstream bandwidth, guaranteed upstream bandwidth, maximum downstream bandwidth, maximum transmit burst length, baseline privacy enable/disable, and type of service (ToS) overwrite byte.

QoS Profile Enforcement allows cable modem termination system (CMTS) operators to control the QoS to eliminate any interference from improper local-rate limiting implemented on the cable modem. The CMTS provisions a registering cable modem with a default DOCSIS 1.0 service class assigned by the operator, overriding any service class that previously existed on the modem. This service class has no upstream or downstream rate limits, so that the CMTS can do traffic shaping based on the QoS profile enforced by the operator.

The following commands are available on Cisco uBR7200 series universal broadband routers to update the QoS table:

- **create-snmp**—Permits creation of QoS table entries by SNMP.
- **modems**—Permits creation of QoS table entries by modem registration requests.
- **update-snmp**—Permits dynamic update of QoS table entries by SNMP.

DOCSIS Quality of Service Enhancements Prior to DOCSIS 1.1

A number of DOCSIS quality of service (QoS) enhancements were added to Cisco IOS Release 12.1(1a)T1 and continue with later releases; these features paralleled some of those that were expected in the DOCSIS 1.1 specification prior to finalization.

For supported DOCSIS 1.1 QoS features, refer to the "DOCSIS 1.1 Quality of Service Features" section on page 1-60.

Note These QoS enhancements are in addition to the currently existing QoS traffic shaping and tiered best effort features.

Concatenation Support Prior to DOCSIS 1.1

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 needs to make only one bandwidth request for a concatenated packet, as opposed to making a different bandwidth request for each individual packet; this technique is especially effective for burst-intensive real-time traffic, such as voice calls.

Concatenation is enabled by default for current cable modem cards (see the "Cable Modem Cards" section), but can be disabled with the Cisco IOS command **no cable upstream number concatenation interface**. The **show controller** command displays whether concatenation is enabled on an interface.

Note Concatenation is supported only with cable modems that support DOCSIS concatenation.

Embedded Client Signaling (dynamic SIDs)

Supports the dynamic creation, configuration, and deletion of Service Identifiers (SIDs) to accommodate different classes of service. This allows cable modems to request high-priority or high-bandwidth data streams as needed, such as when a VoIP call is made.

Note Dynamic SIDs can be used only with cable modems that also support this feature. Otherwise, cable modems must use the static SIDs supported in previous releases.

IP Precedence-Based Rate Limiting

In addition to the currently supported traffic shaping techniques, Cisco IOS Release 12.1(1a)T1 supports a new configuration field that associates a maximum bandwidth (in kbps) with a particular setting of the IP type of service (ToS) bits. This can be used to ensure that certain traffic, such as data, does not exceed a preset rate limit and thereby interfere with higher-priority real-time traffic, such as VoIP calls.

Support for Unsolicited Grants

New fields in the DOCSIS configuration file can be used so that when a cable modem requests a voice or fax SID, the MAC scheduler on the Cisco uBR7200 series router schedules fixed periodic slots on the upstream for that traffic flow. The cable modem does not have to contend for these slots, and because the Cisco uBR7200 series router controls the timing of the slots, it has a very precise control over potential delay and jitter. This provides a Constant Bit Rate (CBR) traffic flow for real-time traffic such as voice and fax calls.

In addition, the Cisco uBR7200 series router can create QoS profiles for G.711 fax traffic and G.729 voice traffic. These profiles can be customized with the scheduling parameters required for the G.711 and G.729 CODECs being used at the subscriber's site.

DOCSIS 1.0 ToS Overwrite

Cisco IOS release 12.3(17a)BC2 introduces support for the DOCSIS 1.0 Type of Service (ToS) Overwrite feature. Currently, ToS overwrite requires the creation of static cable QoS profiles, which are then assigned to the ToS fields. This implementation works well if only a few different service types are offered. However, scalability issues arise when large numbers of service types are presented; each requiring a static QoS profile in order to perform ToS overwrite.

The Default DOCSIS 1.0 ToS Overwrite feature eliminates the need to create multiple QoS profiles in order to perform type-of-service (ToS) overwrite by automatically bounding all DOCSIS 1.0 Cable Modem (CM) created profiles to a default ToS overwrite.

DOCSIS Customer Premises Equipment Configurator

DOCSIS CPE Configurator V2.0.4

The DOCSIS specification requires that a DOCSIS-compliant modem download a DOCSIS configuration file during its power-on or reset sequence. This file must be in the format described in the DOCSIS Radio Frequency Specification (SP-RFI-IOS-991105).

The DOCSIS Customer Premises Equipment (CPE) Configurator V2.0.4 provides you with a Web-based graphical user interface (GUI) that allows you to collect information needed to generate and download configuration files for DOCSIS or EuroDOCSIS CMs and STBs.

There are two versions of the Cisco DOCSIS CPE Configurator V2.0.4:

- Cisco Connection Online (CCO) version (HTML-based). This Web-based, free-of-charge version needs no installation at the customer site, and is viewable at http://www.cisco.com/en/US/products/sw/netmgtsw/ps819/products_user_guide_list.html.
- Desktop (Java-based) version. This stand-alone, desktop version gives operators flexibility in supporting NOC and remote subscriber site usage, and is viewable at this online location:

  http://www.cisco.com/cgi-bin/tablebuild.pl/cpe-conf.

Refer to the following document for additional information about CPE Configurator V2.0.4:

- *CMTS Configuration FAQ*, Document ID: 12180

  http://www.cisco.com/en/US/tech/tk86/tk804/technologies_q_and_a_item09186a00800a4ae5.shtml

DOCSIS CPE Configurator V3.2

Cisco has developed the DOCSIS CPE Configurator tool Version 3.2 that allows to configure DOCSIS 1.1 specific features like upstream and downstream service flows, upstream and downstream Packet Classification, and Payload Header Suppression.

If you are a registered user and are logged in to Cisco.com, you can download the stand-alone DOCSIS CPE Configurator tool Version 3.2 at this online location:

http://www.cisco.com/cgi-bin/tablebuild.pl/cpe-conf.

Refer to the following document for additional information about the DOCSIS CPE Configurator V3.2, which is available to registered, logged in users only.

- *Building DOCSIS 1.0 Configuration Files Using Cisco DOCSIS Configurator*, Document ID: 16480

  http://www.cisco.com/en/US/customer/tech/tk86/tk168/technologies_tech_note09186a0080094d00.shtml

Enhanced Rate Bandwidth Allocation (ERBA) Support for DOCSIS 1.0 Cable Modems

Cisco IOS release 12.3(13a)BC introduces Enhanced Rate Bandwidth Allocation (ERBA) support for DOCSIS 1.0 cable modems and the Cisco uBR7200 series router. ERBA allows DOCSIS1.0 modems to burst their temporary transmission rate up to the full line rate for short durations of time. This capability provides higher bandwidth for instantaneous bandwidth requests, such as those in Internet downloads, without having to make changes to existing service levels in the QoS Profile.

This feature enables MSOs to set the DOCSIS 1.0 cable modems burst transmissions, with mapping to overriding DOCSIS 1.1 QoS profile parameters on the Cisco CMTS. DOCSIS 1.0 cable modems require DOCSIS 1.0 parameters when registering to a matching QoS profile. This feature enables maximum downstream line rates, and the ERBA setting applies to all cable modems that register to the corresponding QoS profile.

Note QoS definitions must previously exist on the Cisco CMTS headend to support this feature.

ERBA for DOCSIS 1.0 cable modems is supported with these new or enhanced commands or keywords in Cisco IOS release 12.3(13a)BC:

- **cable qos pro max-ds-burst** *burst-size*
- **show cable qos profile** *n* **[verbose]**

To define ERBA on the downstream for DOCSIS 1.0 cable modems, use the **cable qos promax-ds-burst** command in global configuration mode. To remove this ERBA setting from the QoS profile, use the **no** form of this command.

cable qos pro max-ds-burst *burst-size*

no cable qos pro max-ds-burst

Syntax Description

burst-size	The QoS profile's downstream burst size in bytes.

To display ERBA settings as applied to DOCSIS 1.0 cable modems and QoS profiles on the Cisco CMTS, use the **show cable qos profile** command in Privileged EXEC mode.

The following example of the **cable qos profile** command in global configuration mode illustrates changes to the **cable qos profile** command. Fields relating to the ERBA feature are shown in bold for illustration:

```
Router(config)# cable qos pro 10 ?
  grant-interval       Grant interval
  grant-size           Grant size
  guaranteed-upstream  Guaranteed Upstream
  max-burst            Max Upstream Tx Burst
  max-ds-burst        Max Downstream Tx burst (cisco specific)
  max-downstream       Max Downstream
  max-upstream         Max Upstream
  name                 QoS Profile name string (cisco specific)
  priority             Priority
  privacy              Cable Baseline Privacy Enable
tos-overwrite        Overwrite TOS byte by setting mask bits to value
```

The following example of the **show cable qos profile** command illustrates that the maximum downstream burst has been defined, and is a management-created QoS profile:

```
Router# show cable qos pro
ID  Prio Max       Guarantee Max         Max   TOS  TOS   Create  B     IP prec.
         upstream  upstream  downstream  tx    mask value by      priv  rate
         bandwidth bandwidth bandwidth   burst                    enab  enab
1   0    0         0         0           0     0xFF 0x0   cmts(r) no    no
2   0    64000     0         1000000     0     0xFF 0x0   cmts(r) no    no
3   7    31200     31200     0           0     0xFF 0x0   cmts    yes   no
4   7    87200     87200     0           0     0xFF 0x0   cmts    yes   no
6   1    90000     0         90000       1522  0xFF 0x0   mgmt    yes   no
10  1    90000     0         90000       1522  0x1  0xA0  mgmt    no    no
50  0    0         0         96000       0     0xFF 0x0   mgmt    no    no
51  0    0         0         97000       0     0xFF 0x0   mgmt    no    no
```

The following example illustrates the maximum downstream burst size in sample QoS profile 10 with the **show cable qos prof verbose** command in privileged EXEC mode:

```
Router# show cable qos pro 10 ver
Profile Index                           10
Name
Upstream Traffic Priority               1
Upstream Maximum Rate (bps)             90000
Upstream Guaranteed Rate (bps)          0
Unsolicited Grant Size (bytes)          0
Unsolicited Grant Interval (usecs)      0
Upstream Maximum Transmit Burst (bytes) 1522
Downstreamam Maximum Transmit Burst (bytes) 100000
IP Type of Service Overwrite Mask       0x1
IP Type of Service Overwrite Value      0xA0
Downstream Maximum Rate (bps)           90000
Created By                              mgmt
Baseline Privacy Enabled                no
```

Usage Guidelines

If a cable modem registers with a QoS profile that matches one of the existing QoS profiles on the Cisco CMTS, then the maximum downstream burst size, as defined for that profile, is used instead of the default DOCSIS QoS profile of 1522.

For example, a DOCSIS 1.0 configuration that matches QoS profile 10 in the previous examples would be as follows:

```
03 (Net Access Control)         = 1

04 (Class of Service Encodings Block)
   S01 (Class ID)               = 1
   S02 (Maximum DS rate)        = 90000
   S03 (Maximum US rate)        = 90000
   S06 (US burst)               = 1522
   S04 (US Channel Priority)    = 1
   S07 (Privacy Enable)         = 0
```

The maximum downstream burst size (as well as the ToS overwrite values) are not explicitly defined in the QoS configuration file because they are not defined in DOCSIS. However, because all other parameters are a perfect match to profile 10 in this example, then any cable modem that registers with these QoS parameters has a maximum downstream burst of 100000 bytes applied to it.

For further illustration, consider a scenario in which packets are set in lengths of 1000 bytes at 100 packets per second (pps). Therefore, the total rate is a multiplied total of 1000, 100, and 8, or 800kbps.

To change these settings, two or more traffic profiles are defined, with differing downstream QoS settings as desired. Table 11 provides two examples of such QoS profiles for illustration:

Table 11 Sample QoS Profiles with Differing ERBA (Maximum Downstream) Settings

QoS Profile Setting	QoS Profile 101	QoS Profile 102
Maximum Downstream Transmit Burst (bytes)	max-burst 4000	max-burst 4000
Maximum Downstream Burst (bps)	max-ds-burst 20000	max-ds-burst 5000
Maximum Downstream Bandwidth	max-downstream 100	max-downstream 100

In this scenario, both QoS profiles are identical except for the max-ds-burst size, which is set to 5000 in QoS profile 101 and 5000 in QoS profile 102.

Optimal Settings for DOCSIS 1.0 Downstream Powerburst

DOCSIS allows the setting different token bucket parameters for each service flow, including the token bucket burst size. When burst sizes are closer to 0, QoS is enforced in a stricter manner, allowing a more predictable sharing of network resources, and as a result easier network planning.

When burst sizes are larger, individual flows can transmit information faster (lower latency), although the latency variance can be larger as well.

For individual flows, a larger burst size is likely to be better. As long as the system is not congested, a large burst size reduces the chances of two flows transmitting at the same time, because each burst is likely to take less time to transmit. However, as channel bandwidth consumption increases, it is probably that large burst traffic would exceed the thresholds of buffer depths, and latency is longer than with well shaped traffic.

For additional information about the **cable qos profile** command and configuring QoS profiles, refer to the following documents on Cisco.com:

- *Cisco IOS CMTS Cable Command Reference Guide*

  http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html
- *DOCSIS 1.1 for the Cisco CMTS*

  http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/ufg_docs.html

DOCSIS 1.0+ Feature Support

In response to the limitations of DOCSIS 1.0 in handling real-time traffic, such as voice calls, Cisco created the DOCSIS 1.0+ extensions to provide the more important QoS enhancements that were expected in DOCSIS 1.1. The main enhancements provide basic Voice-over IP (VoIP) service over the DOCSIS link, support for dynamic creation and teardown of flows during voice calls, support for one new unsolicited grant service (UGS) slot scheduling mechanism for voice slots, and per IP-precedence rate shaping on the downstream. In particular, the Cisco DOCSIS 1.0+ extensions include the DOCSIS 1.1 features described in this section:

- Concatenation for DOCSIS 1.0+, page 1-57
- Dynamic MAC messages, page 1-57
- Multiple SIDs per Cable Modem, page 1-57
- Separate Downstream Rates, page 1-57
- Unsolicited Grant Service (CBR-scheduling) on the Upstream, page 1-57

Refer to the following online document for additional information about DOCSIS 1.0+ support on the Cisco uBR7200 Series:

- *Frequently Asked Questions on DOCSIS 1.0+*

http://www.cisco.com/en/US/tech/tk86/tk168/technologies_q_and_a_item09186a0080094eb2.shtml

Concatenation for DOCSIS 1.0+

Concatenation allows a cable modem to send several packets in one large burst, instead of having to make a separate grant request for each.

Caution All DOCSIS 1.0 extensions are available only when using a cable modem (such as the Cisco uBR924 cable access router) and CMTS (such as the Cisco uBR7200 series router) that support these extensions. The cable modem activates the use of the extensions by sending a dynamic MAC message. DOCSIS 1.0 CMs continue to receive DOCSIS 1.0 treatment from the CMTS.

Dynamic MAC messages

The Dynamic Service Addition (DSA) and Dynamic Service Deletion (DSD) messages allow dynamic SIDs to be created and deleted on demand so that the bandwidth required for a voice call can be allocated at the time a call is placed and then freed up for other uses when the call is over.

Multiple SIDs per Cable Modem

This feature creates separate service flows for voice and data traffic. This allows the CMTS and cable modem to give higher priority for voice traffic, preventing the data traffic from affecting the quality of the voice calls.

Separate Downstream Rates

This feature provides an ability to provide separate downstream rates for any given cable modem, based on the IP-precedence value in the packet—This helps separate voice signaling and data traffic that goes to the same ITCM to address rate shaping purposes.

Unsolicited Grant Service (CBR-scheduling) on the Upstream

This feature helps provide a higher-quality channel for upstream VoIP packets from an Integrated Telephony Cable Modem (ITCM) such as the Cisco uBR924 cable access router.

DOCSIS 1.1 Feature Support

DOCSIS 1.1 is the first major revision of the initial DOCSIS 1.0 standard for cable networks. Although the initial standard provided quality data traffic over the coaxial cable network, the demands of real-time traffic such as voice and video required many changes to the DOCSIS specification.

This section describes the major enhancements supported on the Cisco uBR7200 series:

Baseline Privacy Interface Plus (BPI+)

Baseline Privacy Interface Plus (BPI+) is available and supported on the Cisco uBR7200 series with Cisco IOS Release 12.2(4)BC1 and subsequent BC1 releases.

DOCSIS 1.1 enhances these security features with Baseline Privacy Interface Plus (BPI+), which includes the following enhancements:

- Digital certificates provide secure user identification and authentication.
- Key encryption uses 168-bit Triple DES (3DES) encryption that is suitable for the most sensitive applications.
- 1024-bit public key with Pkcs#1 Version 2.0 encryption.
- Multicast support.
- Secure software download allows a service provider to upgrade a cable modem's software remotely, without the threat of interception, interference, or alteration.

Additional feature information and configuration guidelines are provided in *Configuring DOCSIS Baseline Privacy Interface on the Cisco uBR7200 Series*, available on Cisco.com:

http://www.cisco.com/en/US/docs/cable/cmts/ubr7200/configuration/guide/u72_bpi.html

Burst Profile Configuration

For each modulation/burst profile configuration, Cisco uBR7200 series universal broadband routers support burst profile number, burst profile interval usage code, burst type, preamble length and unique word length, differential encoding enable/disable, forward error correction (FEC) correctable bytes value, FEC code word length, scrambler seed value, maximum burst size, guard time size, last code word shortened/lengthened, and scrambler enable/disable.

Note Multiple burst profiles are supported on the MC11C, MC12C, MC14C, MC16B, and MC16C cable modem cards. Only one profile is supported on the original MC11-FPGA card.

Cable Modulation Profile Default Templates

Commencing with Release 12.1(3a)EC1 and later releases, the **cable modulation-profile** global configuration command has been enhanced with three new options that enable you to quickly create basic modulation profiles using the default values for each burst type.

To define the modulation profile, use the **cable modulation-profile** command in global configuration mode. Use the **no** form of this command to remove the entire modulation profile or to reset a particular burst to its default values.

cable modulation-profile *profile* {**mix** | **qam-16** | **qpsk**}

no cable modulation-profile *profile* {**mix** | **qam-16** | **qpsk**}

Syntax Description The syntax for the new options is as follows:

profile	Specifies the modulation profile number (1-8).
mix	Creates a default QPSK/16-QAM mix modulation profile where short and long grant bursts are sent using 16-QAM, while request, request data, initial ranging, and station maintenance bursts are sent using QPSK). The burst parameters are set to their default values for each burst type.
qam-16	Creates a default 16-QAM modulation profile, where all bursts are sent using 16-QAM. The burst parameters are set to their default values for each burst type.
qpsk	Creates a default QPSK modulation profile, where all bursts are sent using QPSK. The burst parameters are set to their default values for each burst type.

DHCP Cable Modem Host ID

This feature—also known as Cable Modem and Host Subnet Addressing—allows the Cisco uBR7200 series universal broadband router to set the GIADDR field of DHCPDISCOVER and DHCPREQUEST packets with a Relay IP address to help automate the provisioning of cable modems on systems that use multiple IP subnets.

To modify the GIADDR field of DHCPDISCOVER and DHCPREQUEST packets with a Relay IP address before they are forwarded to the DHCP server, use the **cable dhcp-giaddr** command in cable interface or subinterface configuration mode. To set the GIADDR field to its default, use the **no** form of this command.

cable dhcp-giaddr [**policy** | **primary**]

no cable dhcp-giaddr

Syntax Description

policy	(Optional) Selects the control policy, so the primary address is used for CMs and the secondary addresses are used for hosts.
primary	(Optional) Always selects the primary address to be used for the GIADDR field. Primarily used for the MC16E card and Cisco uBR7100E series routers, for support of EuroDOCSIS.

For additional command information, refer to the *Cisco IOS CMTS Cable Command Reference Guide* on Cisco.com.

DHCP Client ID/Remote ID Options

This feature—also known as the Customer Premises Equipment (CPE) Limitation—allows Cisco uBR7200 series universal broadband routers to report and limit the number of CPEs that can use the cable modem to access the cable network.

Note This feature is separate from the cable modem's ability to support multiple CPE devices. For example, depending on the Cisco IOS software release being used, Cisco uBR900 series cable access routers can support a maximum of either 3 or 254 CPE devices. Also, by default, a DOCSIS-based cable modem supports one CPE device, but this can be changed by modifying the MAX CPE parameter in the modem's DOCSIS configuration file.

DHCP, Time of Day (ToD) and TFTP Servers

The Cisco uBR7200 series routers support onboard Dynamic Host Configuration Protocol (DHCP) servers, Time of Day (ToD) and TFTP servers. This allows the Cisco uBR7200 series routers to provide cable modems with IP address information, to supply an RFC 868-compliant time-of-day timestamp, and to download a DOCSIS configuration file, without requiring separate and external servers.

A DOCSIS-compliant cable modem requires access to three types of servers in order to successfully come online:

- The first is a DHCP server, which provides the cable modem with an IP address, a subnet mask and other IP related parameters.
- The second is an RFC868 compliant Time-of-Day Server which lets the modem know what the current time is. A cable modem needs to know the time in order to be able to properly add accurate timestamps to its event log.
- The third is a Trivial File Transfer Protocol (TFTP) server from which a cable modem is able to download a DOCSIS configuration file containing cable modem specific operational parameters.

The Dynamic Host Configuration Protocol (DHCP) is a network management features that simplifies CMTS provisioning. DHCP provides configuration parameters to Internet hosts. DHCP consists of two components:

- a protocol for delivering host-specific configuration parameters from a DHCP server to a host
- a mechanism for allocating network addresses to hosts

DHCP is built on a client/server model, where designated DHCP server hosts allocate network addresses and deliver configuration parameters to dynamically configured hosts. DHCP supports three mechanisms for IP address allocation:

- Automatic allocation—DHCP assigns a permanent IP address to a client.
- Dynamic allocation—DHCP assigns an IP address to a client for a limited period of time (or until the client explicitly relinquishes the address).
- Manual allocation—The network administrator assigns an IP address to a client and DHCP is used simply to convey the assigned address to the client.

The Cisco IOS DHCP server feature is a full DHCP server implementation that assigns and manages IP addresses from specified address pools within the router to DHCP clients. If the Cisco IOS DHCP server cannot satisfy a DHCP request from its own database, it can forward the request to one or more secondary DHCP servers defined by the network administrator.

You can configure a DHCP server in the following ways:

- You can configure the DHCP server when using the Cable Interface Setup facility. For additional information, refer to the "Configuring the Cisco uBR7200 Series Using the Setup Facility" section on page 2-17.
- You can configure DHCP services alone, or when configuring ToD and TFTP services. For additional information, refer to the chapter titled "Configuring DHCP, ToD, and TFTP Services" in the *Cisco Cable Modem Termination System Feature Guide* on Cisco.com.

DOCSIS 1.1 Quality of Service Features

DOCSIS 1.1 modifies the DOCSIS 1.0 specification to provide better performance, in particular for real-time traffic such as voice calls. The DOCSIS 1.1 specification provides several functional enhancements over DOCSIS 1.0 coaxial cable networks.

DOCSIS 1.1 features are supported in the Cisco IOS 12.2 BC release train, with additional DOCSIS 1.1 features being supported in certain earlier Cisco IOS 12.1 EC and 12.0 SC release trains.

Concatenation for DOCSIS 1.1

Concatenation allows a cable modem to send multiple MAC frames in the same time slot, as opposed to making an individual grant request for each frame. This avoids wasting upstream bandwidth when sending a number of very small packets, such as TCP acknowledgement packets.

You can turn concatenation on or off. For information about configuring concatenation, refer to *Configuring Concatenation on the Cisco uBR7200 Series Cable Router* on Cisco.com.

DOCSIS 1.0 and 1.0+ Cable Modem Support

DOCSIS 1.1 cable modems can coexist with DOCSIS 1.0 and 1.0+ cable modems in the same network—the Cisco uBR7200 series provides the levels of service that are appropriate for each cable modem.

DOCSIS 1.1 Service Flow Model

DOCSIS 1.1 offers enhanced Quality of Service (QoS) features that give priority for real-time traffic such as voice and video:

- The DOCSIS 1.0 QoS model (a Service IDs (SID) associated with a QoS profile) has been replaced with a service flow model that allows greater flexibility in assigning QoS parameters to different types of traffic and in responding to changing bandwidth conditions
- Multiple service flows per cable modem in either direction due to packet classifiers
- Support for multiple service flows per cable modem allowing a single cable modem to support a combination of data, voice, and video traffic.
- Greater granularity in QoS per cable modem in either direction, using unidirectional service flows
- Dynamic MAC messages that can create, modify, and tear-down QoS service flows dynamically when requested by a DOCSIS 1.1 cable modem

Downstream QoS Handling Supported

Downstream QoS handling is compliant with Multimedia Cable Network System (MCNS) requirements. For additional downstream QoS feature configuration, refer to the *DOCSIS 1.1 for the Cisco uBR7200 Series Universal Broadband Routers* feature module on Cisco.com:

http://www.cisco.com/en/US/docs/cable/cmts/feature/DOCSIS11.html

Dynamic MAC Messages

Dynamic Service MAC messages allow dynamic signaling of QoS between the cable modem and the CMTS. These messages are DOCSIS link layer equivalents of the higher layer messages that create, tear down, and modify a service flow. These messages are collectively known as DSX messages.

The DSX state machine module on the CMTS manages the several concurrent dynamic service transactions between cable modems and the CMTS. It include state machine support for all three DOCSIS1.1 DSX MAC messages:

- Dynamic Service Add (DSA)—This message is used to create a new service flow.
- Dynamic Service Change (DSC)—This message is used to change the attributes of an existing service flow.
- Dynamic Service Deletion (DSD)—This message is used to delete an existing service flow.

For additional information, refer to the *DOCSIS 1.1 for the Cisco uBR7200 Series Universal Broadband Routers* feature module on Cisco.com:

http://www.cisco.com/en/US/docs/cable/cmts/feature/DOCSIS11.html

Dynamic Map-Advance

A CMTS administrator can enhance the upstream throughput from a cable modem connected to the Cisco Cisco uBR7200 series CMTS. The system employs a new algorithm that automatically tunes the lookahead time in MAPs, based on several input parameters for the corresponding upstream channel. The use of dynamic and optimal lookahead time in MAPs significantly improves the per-modem upstream throughput.

For configuration information, refer to "Configuring the Dynamic Map Advance Algorithm" section on page 5-7.

Dynamic SID Support

For additional feature information, refer to the document titled *Cisco uBR7200 - QoS/MAC Enhancements for Voice and Fax Calls: DOCSIS 1.0+* on Cisco.com.

Fragmentation (Layer 2)

Layer 2 fragmentation on the upstream prevents large data packets from affecting real-time traffic, such as voice and video. Large data packets are fragmented and then transmitted in the time slots that are available between the time slots used for the real-time traffic.

Multiple SID Support

This feature consists of changes made to various **show** commands to expand service identifier (SID) information.

- The **show cable modem** command has been changed to indicate that the SID shown is the primary SID for each cable modem.
- The **show interface cable** command has been updated to include the secondary SIDs for each cable modem.

For additional information, refer to *Multiple Service ID Support for the Cisco uBR7200 Series Cable Router* on Cisco.com:

http://www.cisco.com/en/US/docs/ios/12_0t/12_0t5/feature/guide/multisid.html

Payload Header Suppression (PHS)

Payload Header Suppression (PHS) conserves link-layer bandwidth by suppressing unnecessary packet headers on both upstream and downstream traffic flows.

To configure PHS, refer to the "Configuring Payload Header Suppression and Restoration" section on page 3-33. For additional information about configuring these and other DOCSIS features, refer to the *DOCSIS 1.1 for the Cisco uBR7200 Series Universal Broadband Routers* feature module on Cisco.com:

http://www.cisco.com/en/US/docs/cable/cmts/feature/DOCSIS11.html

QoS Configuration

QoS configuration information is now included in the Cable Modem Database Manager, which is described further in the document titled *DOCSIS 1.1 for the Cisco uBR7200 Series Universal Broadband Routers* feature module on Cisco.com:

http://www.cisco.com/en/US/docs/cable/cmts/feature/DOCSIS11.html

QoS Profile Enforcement

This feature allows CMTS operators to override the provisioned service class of a cable modem at the time of registration with a CMTS local-static quality of service (QoS) profile. CMTS operators can control the QoS from the CMTS and eliminate any interference from improper local-rate limiting

implemented on the cable modem. The CMTS provisions a registering cable modem with a default Data-over-Cable Service Interface Specifications (DOCSIS) 1.0 service class that is assigned by the operator. This service class has no upstream or downstream rate limits.

When the modem sends data upstream, it makes bandwidth requests without throttling or dropping packets because of its own rate-policing algorithm. The CMTS does traffic shaping based on the QoS profile enforced by the operator.

For configuration information, refer to the document titled *QoS Profile Enforcement for the Cisco uBR7200 Series Router* on Cisco.com:

http://www.cisco.com/en/US/docs/ios/12_0t/12_0t4/feature/guide/qospr124.html

Time-of-Day Server

The Time-of-Day (ToD) server enables the Cisco Cable Modem Termination System (CMTS) to provide a ToD server to the CMs and other customer premises equipment (CPE) devices connected to its cable interfaces. The cable modem uses the ToD server to get the current date and time to accurately time-stamp its Simple Network Management Protocol (SNMP) messages and error log entries.

The Data-over-Cable System Interface Specifications (DOCSIS) 1.0 and 1.1 specifications require that a DOCSIS cable modem or other CPE device must specify the following time-related fields in the Dynamic Host Configuration Protocol (DHCP) request it sends during its initial power-on provisioning:

- Time Offset (option 2)—Specifies the time zone for the cable modem or CPE device, as the number of seconds that the device's time stamp is offset from Greenwich Mean Time (GMT)
- Time Server Option (option 4)—Specifies one or more IP addresses for a ToD server.
- During initial provisioning, a DOCSIS cable modem or CPE device attempts to contact the ToD server. If successful, the cable device updates its onboard clock with the time offset and timestamp received from the ToD server. If a ToD server cannot be reached or if it does not respond, the cable device eventually times out and continues on with the initialization process.

For configuration information, refer to the chapter titled Time of Day Server" in the *Cisco Cable Modem Termination System Feature Guide* on Cisco.com.

Trivial File Transfer Protocol Server

A DOCSIS-compliant cable modem requires access to three types of servers in order to successfully come online:

- A DHCP, Time of Day (ToD) and TFTP Servers provides the cable modem with an IP address, a subnet mask and other IP related parameters.
- A Time-of-Day Server which lets the modem know what the current time is. A cable modem needs to know the time in order to be able to properly add accurate timestamps to its event log.
- A Trivial File Transfer Protocol (TFTP) server from which a cable modem is able to download a DOCSIS configuration file containing cable modem specific operational parameters. After a cable modem has attempted to contact a ToD server, it contacts a TFTP server to download a DOCSIS configuration file. If a binary DOCSIS configuration file can be copied to a Flash device on a Cisco CMTS, then the router can act as a TFTP server for that file.

Type/Length/Value Parser and Encoder

The Type/Length/Value (TLV) parser and encoder is a new module that handles parsing and encoding TLVs on the CMTS. All old DOCSIS1.0/1.0+ TLVs are supported. In addition, many new TLVs have been added in DOCSIS1.1, such as service flow encodings, classifier encodings, and support for PHS rules. The new TLV parser features are used by different MAC message modules.

To display the Type/Length/Value (TLV) encodings parsed by the DOCSIS 1.1 TLV parser/encoder, use the **debug cable tlvs** command in privileged EXEC mode. The **no** form of this command disables debugging output.

debug cable tlvs

no debug cable tlvs

Refer to the following documents on Cisco.com for additional information about the TLV parser/encoder:

- *Cisco IOS CMTS Cable Command Reference Guide*
  http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html
- *DOCSIS 1.1 for the Cisco uBR7200 Series Universal Broadband Routers*
  http://www.cisco.com/en/US/docs/cable/cmts/feature/DOCSIS11.html
- *Cable DOCSIS 1.1 FAQs*
  http://www.cisco.com/warp/public/109/cable_faq_docsis11.shtml

UpstreamAddress Verification

This feature prevents the spoofing of IP addresses. Using the CLI, administrators can determine the IP and MAC address of a given cable interface, and the SID number that shows the IP and MAC addresses of all devices learned in the cable interface's MAC table.

The CMTS verifies the source IP address against the MAC address for the cable modem. Cable modem and PC IP addresses are verified to ensure that SID and MAC addresses are consistent. A PC behind a cable interface is assigned an IP address from the DHCP server. If a user on a second PC or cable interface statically assigns the same IP address to a PC, the Cisco uBR7200 series CMTS reports this. Using customer databases, administrators can cross-reference the spoofing cable modem and PC to prevent further usage.

The **cable source-verify** [**dhcp**] command (for cable interfaces) specifies that DHCP lease query requests are sent to verify any unknown source IP address found in upstream data packets. Upstream Address Verification requires a DHCP server that supports the new LEASEQUERY message type. Cisco Network Registrar supports the LEASEQUERY message type in Cisco IOS Release 3.01(T) and later releases.

For configuration information, refer to Chapter 5, "Managing Cable Modems on the Hybrid Fiber-Coaxial Network".

Upstream QoS Improvements

Supported QoS models for the upstream are:

- Best-effort—Data traffic sent on a non-guaranteed best-effort basis.
- Committed information rate (CIR)—Guaranteed minimum bandwidth for data traffic.
- Unsolicited grants (UGS)—Constant bit rate (CBR) traffic, such as voice, that is characterized by fixed size packets at fixed intervals.
- Unsolicited grants with activity detection (USG-AD)—Combination of UGS and RTPS, to accommodate real time traffic that might have periods of inactivity (such as voice using silence suppression). The service flow uses UGS fixed grants while active, but switches to RTPS polling during periods of inactivity to avoid wasting unused bandwidth.

For detailed information about QoS, refer to the *DOCSIS 1.1 for the Cisco uBR7200 Series Universal Broadband Routers* feature module on Cisco.com:

http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/cmtsfg.html

Upstream QoS Models Supported

Supported QoS models for the upstream are as follows:

- Best effort-Data traffic sent on a non-guaranteed best-effort basis
- Committed Information Rate (CIR)—Guaranteed minimum bandwidth for data traffic
- Unsolicited Grants (UGS)—Constant bit rate (CBR) traffic, such as voice, that is characterized by fixed size packets at fixed intervals
- Real Time Polling (rtPS)—Real Time service flows, such as video, that produce unicast, variable size packets at fixed intervals
- Unsolicited Grants with Activity Detection (USG-AD)—Combination of UGS and RTPS, to accommodate real time traffic that might have periods of inactivity (such as voice using silence suppression). The service flow uses UGS fixed grants while active, but switches to RTPS polling during periods of inactivity to avoid wasting unused bandwidth.
- Enhanced time-slot scheduling mechanisms to support guaranteed delay/jitter sensitive traffic on the shared multiple access upstream link

DOCSIS 1.1 Two-way Transmission (Cisco uBR7246VXR Router)

The Cisco uBR7200 series routers allow DOCSIS 1.1 two-way transmission of digital data and Voice over IP (VoIP) traffic over a hybrid fiber-coaxial (HFC) network. The Cisco uBR7200 series support IP routing with a wide variety of protocols and combinations of Ethernet, Fast Ethernet, Gigabit Ethernet, serial, High-Speed Serial Interface (HSSI), Packet over SONET (POS) OC-3 and OC-12c, and Asynchronous Transfer Mode (ATM) media.

Downstream Channel ID

This feature allows all cable modems in an HFC network to identify themselves via unique downstream channel IDs instead of their downstream frequencies.

To configure the downstream channel ID, use the **cable downstream channel-id** configuration command. Use the **no** form of this command to set the downstream channel ID to its default value.

cable downstream channel-id *id*

no cable downstream channel-id

Syntax DescriptionS

id	Specifies a downstream channel ID. Valid values are from 1 to 255.

For additional information, refer to the following documents on Cisco.com:

- *Configuring Downstream Channel IDs*

  http://www.cisco.com/en/US/docs/ios/12_0t/12_0t4/feature/guide/downchan.html
- *Cisco IOS CMTS Cable Command Reference Guide*

  http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html

Downstream Frequency Override

Downstream frequency override allows the CMTS administrator to change the downstream frequency assigned to a cable modem, overriding the frequency set in the cable modem DOCSIS configuration file.

To enable cable downstream frequency override, use the **cable downstream override** command in cable interface configuration mode. To disable the override feature, use the **no** form of this command.

cable downstream override

no cable downstream override

For additional command information, refer to the following document on Cisco.com:

- *Cisco IOS CMTS Cable Command Reference Guide*

  http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html

Downstream Packet Classifier

This feature helps to map packets into DOCSIS service flows. The Cisco CMTS supports downstream IP packet classifiers.

Downstream Packet Scheduler

This module controls all output packet queuing service on the downstream link of each cable interface.

Downstream Rate Shaping with IP Type of Service Bits

Cisco uBR7200 series routers support downstream data rate shaping on a per-modem basis. The Type of Service (ToS) bits in the IP packet header can be set to specify that packet's class of service, allowing packets for certain traffic flows (such as VoIP) to be given precedence over packets for other flows (such as data).

Downstream rate shaping with ToS bits allows you to configure multiple data rates for a given modem. Also, by specifying a maximum data rate for a particular ToS, you can override the common maximum downstream data rate. Packets that contain ToS bytes that have not been configured for downstream data rates continue to use the common data rate limits.

Prior releases set the ToS bits to zero; however, with the advent of virtual private network (VPN) and QoS applications, it is desirable to copy the ToS bits when the router encapsulates the packets using generic routing encapsulation (GRE). Thus, intermediate routers between tunnel endpoints can also take advantage of QoS features such as weighted fair queuing (WFQ) and weighted random early detection (WRED).

For additional information, refer to the following document on Cisco.com:

- *Downstream Rate Shaping with TOS Bits for the Cisco uBR7200 Series Cable Router*

  http://www.cisco.com/en/US/docs/ios/12_0t/12_0t5/feature/guide/tosbit.html

Optional Upstream Scheduler Modes

With this feature, the user is able to select either Unsolicited Grant Services (UGS) or Real Time Polling Service (rtPS) scheduling types, as well as packet-based or TDM-based scheduling. Low latency queueing (LLQ) emulates a packet-mode-like operation over the Time Division Multiplex (TDM) infrastructure of DOCSIS. As such, the feature provides the typical trade-off between packets and TDM: with LLQ, the user has more flexibility in defining service parameters for UGS or rtPS, but with no guarantee (other than statistical distribution) regarding parameters such as delay and jitter.

Restrictions

- To ensure proper operation, Call Admission Control (CAC) must be enabled. When the Low Latency Queueing (LLQ) option is enabled, it is possible for the upstream path to be filled with so many calls that it becomes unusable, making voice quality unacceptable. CAC must be used to limit the number of calls to ensure acceptable voice quality, as well as to ensure traffic other than voice traffic.
- Even if CAC is not enabled, the default (DOCSIS) scheduling mode blocks traffic after a certain number of calls.
- Unsolicited Grant Services with Activity Detection (UGS-AD) and Non Real Time Polling Service (nrtPS) are not supported.

cable upstream *n* scheduling type

Use this new command to turn the various scheduling modes on or off, where *n* specifies the upstream port.

```
Router(config-if)# [no] cable upstream n scheduling type [ugs | rtps] mode [llq | docsis]
```

For additional information about scheduler enhancements on the Cisco CMTS, refer to the following documents on Cisco.com:

- *Cisco CMTS Feature Guide — Configuring Upstream Scheduler Modes on the Cisco CMTS*
  http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/ufg_schd.html
- *DOCSIS 1.1 for the Cisco CMTS*
  http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/ufg_docs.html

DOCSIS 2.0 Feature Support

This section describes DOCSIS 2.0 enhancements supported on the Cisco uBR7200 series:

- DOCSIS 2.0 A-TDMA Support, page 1-67

DOCSIS 2.0 A-TDMA Support

Support for DOCSIS 2.0 A-TDMA on the Cisco uBR7200 series commences with Cisco IOS Release 12.2(15)CX and continues with later releases in the 12.2 CX, 12.2 BC and 12.3 BC release trains.

The Cisco uBR-MC16U/X and Cisco uBR-MC28U/X cards improve the maximum upstream bandwidth on existing DOCSIS 1.0 and DOCSIS 1.1 cable networks by providing a number of advanced PHY capabilities that have been specified by the new DOCSIS 2.0 specifications.

The DOCSIS 2.0 A-TDMA Support feature incorporates the following advantages and improvements of DOCSIS 2.0 networks:

- Builds on existing DOCSIS cable networks by providing full compatibility with existing DOCSIS 1.0 and DOCSIS 1.1 cable modems. (The registration response (REG-RSP) message contains the DOCSIS version number to identify each cable modem's capabilities.)
- Upstreams can be configured for three different modes to support different mixes of cable modems:
  - An upstream can be configured for TDMA mode to support only DOCSIS 1.0 and DOCSIS 1.1 cable modems.
  - An upstream can be configured for A-TDMA mode to support only DOCSIS 2.0 cable modems.
  - An upstream can be configured for a mixed, TDMA/A-TDMA mode, to support both DOCSIS 1.0/DOCSIS 1.1 and DOCSIS 2.0 cable modems on the same upstream.

Note DOCSIS 2.0 A-TDMA cable modems will not register on a TDMA upstream if an A-TDMA or mixed upstream exists in the same MAC domain, unless the CMTS explicitly switches the cable modem to another upstream using an Upstream Channel Change (UCC) message. DOCSIS 1.0 and DOCSIS 1.1 cable modems cannot register on an A-TDMA only upstream.

- A-TDMA mode defines new interval usage codes (IUC) of A-TDMA short data grants, long data grants, and Unsolicited Grant Service (UGS) grants (IUC 9, 10, and 11) to supplement the existing DOCSIS 1.1 IUC types
- Increases the maximum channel capacity for A-TDMA upstreams to 30 Mbps per 6 MHz channel.
- A-TDMA and mixed modes of operation provide higher bandwidth on the upstream using new 32-QAM and 64-QAM modulation profiles. In addition, an 8-QAM modulation profile is supported.

- Supports a minislot size of 1 tick for A-TDMA operations.
- Increases channel widths to 6.4 MHz (5.12 Msymbol rate).

For additional information on DOCSIS 2.0 A-TDMA Support on the Cisco uBR-MC16U/X card, refer to the section, "DOCSIS 2.0 A-TDMA Support" in *Configuring the Cisco uBR-MC16U/MC16X Cable Interface Line Card* on Cisco.com:

http://www.cisco.com/en/US/docs/interfaces_modules/cable/line_cards/ubr16u_x/configuration/guide/mc16uxfm.html#wp1153687

For additional information on DOCSIS 2.0 A-TDMA Support on the Cisco uBR-MC28U/X card, refer to the section, "DOCSIS 2.0 A-TDMA Support" in *Configuring the Cisco uBR-MC28U/MC28X Cable Interface Line Card* on Cisco.com:

http://www.cisco.com/en/US/docs/interfaces_modules/cable/line_cards/ubr28u_x/configuration/guide/mc28uxfm.html#wp1153687

High Availability Features

Several powerful High Availability features are supported on the Cisco uBR7200 series:

Cisco DDC (Dual DOCSIS Channel)

The Cisco Dual DOCSIS Channel (DDC) feature provides redundancy to cable voice and data customers by using two or three CMTSs with connected RF upstreams and downstreams. Redundancy is provided by controlling each CMTS on which the cable modems register, and by allowing movement of the cable modems between the Cisco CMTS systems.

Cisco DDC provides redundancy during planned downtime, especially during software upgrades, with minimal configuration or control external to the Cisco CMTS.

For information about configuring, maintaining and troubleshooting DDC on the Cisco uBR7246VXR router, refer to the section “Configuring Dual DOCSIS Channel on the Cisco uBR7246VXR Universal Broadband Router” in the following document on Cisco.com:

- *Cisco Dual DOCSIS Channel (DDC) on the Cisco uBR7246VXR Universal Broadband Router*

  http://www.cisco.com/en/US/docs/cable/cmts/feature/docs_DDC.html

DRP Server Agent

The Director Response Protocol (DRP) is a simple User Datagram Protocol (UDP)-based application developed by Cisco Systems. It enables Cisco's DistributedDirector product to query routers (DRP Server Agents) in the field for Border Gateway Protocol (BGP) and Interior Gateway Protocol (IGP) routing table metrics between distributed servers and clients. DistributedDirector, a separate standalone product, uses DRP to transparently redirect end-user service requests to the topologically closest responsive server. DRP enables DistributedDirector to provide dynamic, scalable, and "network intelligent" Internet traffic load distribution between multiple geographically dispersed servers.

DRP Server Agents are border routers (or peers to border routers) that support the geographically distributed servers for which DistributedDirector service distribution is desired. Note that, because DistributedDirector makes decisions based on BGP and IGP information, all DRP Server Agents must have access to full BGP and IGP routing tables. For configuration information, refer to the section titled "Configuring a DRP Server Agent" in the *Cisco IOS IP Configuration Guide*, Release 12.2.

DSX Messages and Synchronized PHS Information

Cisco IOS Release 12.3(17a)BC introduces support for PHS rules in a High Availability environment. In this release, and later releases, PHS rules synchronize and are supported during a switchover event of these types:

- Route Processor Redundancy Plus (RPR+), with Active and Standby Performance Routing Engines (PREs)
- HCCP N+1 Redundancy, with Working and Protect cable interface line cards

For additional information about these enhancements, and related High Availability features, refer to the following documents on Cisco.com:

- *N+1 Redundancy for the Cisco Cable Modem Termination System*

  http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/uFGnpls1.html
- *Route Processor Redundancy Plus for the Cisco uBR10012 Router*

  http://www.cisco.com/en/US/products/hw/cable/ps2209/products_feature_guide09186a00801a24e0.html

Globally Configured HCCP 4+1 Redundancy on the Cisco uBR7246VXR Router

Cisco IOS Release 12.3(17a)BC introduces support for HCCP 4+1 Redundancy on the Cisco uBR7246VXR router. Global configuration makes this High Availability feature quick to implement in the HCCP redundancy scheme.

In this High Availability configuration, four Working router chassis are supported with one Protect router chassis. These five routers are further cabled and configured with two Cisco RF Switches in the same rack using the Cisco Hot Standby Connection to Connection (HCCP) protocol.

HCCP 4+1 Redundancy is a global configuration for all the Cisco uBR7246VXR routers in the scheme. HCCP 4+1 Redundancy supports the Cisco uBR-MC28U broadband processing engine (BPE), configured in inter-chassis protection, where the Working and Protect cable interface line cards or BPEs are operating in different router chassis. A switchover event applies to an entire cable interface line card.

Note 4+1 Redundancy on the Cisco uBR7246VXR router requires that all BPEs in the router be the same.

For additional information about HCCP 4+1 Redundancy, refer to the following document on Cisco.com:

- *N+1 Redundancy for the Cisco CMTS*

  http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/uFGnpls1.html

HCCP Support for the Cisco uBR-MC16S Cable Interface Line Card

Cisco IOS Release 12.1(7)EC adds support for the Cisco uBR-MC16S cable interface line card when used in an HCCP 1+1 redundant configuration. Previously, the Cisco uBR-MC16S card could be used in a redundant configuration only by first disabling its intelligent spectrum management features.

In Cisco IOS Release 12.1(7)EC and later releases, the Cisco uBR-MC16S card can be used as the protect cable interface or working cable interface, with either another Cisco uBR-MC16S card or a Cisco uBR-MC16C card. Table 9 shows how a switchover in each of these configurations affects the intelligent spectrum management features of the Cisco uBR-MC16S card.

Table 1-12 Switchover Operation for a Cisco uBR-MC16C/Cisco uBR-MC16S Configuration

Working Cable Interface	Protect Cable Interface	Operation After Switchover
Cisco uBR-MC16C	Cisco uBR-MC16S	The protect card (Cisco uBR-MC16S) uses the same upstream frequency as the working card, but after the system stabilizes, the protect card begins using the intelligent spectrum management features of the Cisco uBR-MC16S card, as configured on the protect CMTS.
Cisco uBR-MC16S	Cisco uBR-MC16C	The protect card (Cisco uBR-MC16C) uses the same upstream frequency as the working card. If the upstream becomes unstable, the Cisco uBR-MC16C performs only blind frequency hopping.
Cisco uBR-MC16S	Cisco uBR-MC16S	The protect card initially uses the same upstream frequency as the working card, but after the system stabilizes, the protect card continues using the intelligent spectrum management features of the Cisco uBR-MC16S card.

For additional information, refer to *Advanced Spectrum Management Features for the Cisco uBR-MC16S Spectrum Management Card* on Cisco.com.

Note HCCP support for the Cisco uBR-MC16S card exists only in Cisco IOS Release 12.1(7)EC or later, so you cannot use the advanced spectrum management features in Cisco IOS Release 12.1(7)CX with HCCP 1+1 redundant configuration.

HCCP N+1 Redundancy

HCCP N+1 Redundancy is made possible with the addition of the Cisco RF Switch to your cable headend network. Together with the Cisco uBR10012 and/or the Cisco uBR7246VXR routers, the Cisco RF Switch provides a fully redundant system that enables cable operators to achieve PacketCable system availability, minimize service disruptions, and simplify operations.

HCCP N+1 Redundancy is an important step toward high availability on CMTS and telecommunications networks that use broadband media. HCCP N+1 Redundancy can help limit Customer Premises Equipment (CPE) downtime by enabling robust automatic switchover and recovery in the event that there is a localized system failure.

Beginning with Cisco IOS Release 12.2(15)BC2, HCCP N+1 Redundancy adds synchronization between HCCP Working interface configurations and those inherited upon switchover to HCCP Protect interfaces. This makes the configuration of both easier and switchover times faster.

For additional configuration information about HCCP N+1 Redundancy, refer to *HCCP N+1 Redundancy for the Cisco Cable Modem Termination System* on Cisco.com:

http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/uFGnpls1.html

High Availability Features in Cisco IOS Release 12.3(13a)BC

Cisco IOS Release 12.3(13a)BC removes support for HCCP N+1 Redundancy on the Cisco uBR7200 series routers. Associated configuration, show, and debug commands are not supported in this release.

Note The latest release to support HCCP N+1 Redundancy for the Cisco uBR7200 Series is Cisco IOS release 12.3(9a)BC. When upgrading from this or earlier supporting Cisco IOS releases to Cisco IOS release 12.3(13a)BC, the HCCP configurations are discarded and not retained.

HCCP N+1 Redundancy for the Cisco CMTS is described for earlier releases in this and additional documents on Cisco.com:

- *N+1 Redundancy for the Cisco Cable Modem Termination System*

  http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/uFGnpls1.html

High Availability Support for Encrypted IP Multicast

Cisco IOS Release 12.3(17a)BC introduces support for IP Multicast streams during switchover events in a High Availability environment. This feature is supported for Route Processor Redundancy Plus (RPR+), N+1 Redundancy, and encrypted BPI+ streams.

For additional information about IP Multicast and High Availability, refer to these documents on Cisco.com:

- *Cisco CMTS Universal Broadband Router MIB Specifications Guide*

  http://www.cisco.com/en/US/docs/cable/cmts/mib/reference/guide/ubrmibv5.html
- *Dynamic Shared Secret for the Cisco CMTS*

  http://www.cisco.com/en/US/docs/cable/cmts/feature/ubrdmic.html
- *IP Multicast in Cable Networks,* White Paper

  http://www.cisco.com/en/US/tech/tk828/technologies_case_study0900aecd802e2ce2.shtml
- *N+1 Redundancy for the Cisco Cable Modem Termination System*

  http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/uFGnpls1.html

Hot-Standby 1+1 Redundancy

The Hot-Standby 1+1 Redundancy feature offers the ability to provide high system availability when configuring a Cisco uBR7200 series universal broadband router to wait in hot-standby mode to protect another Cisco uBR7200 series router in case of system failure.

The 1+1 redundancy feature is essential in a residential Voice over IP (VoIP) cable network, since it provides a three- to five-second automatic system recovery time, thus helping to eliminate “call drops” in the VoIP cable network. System failure in a non-redundancy (unprotected) deployment results in loss of all voice calls in progress as well as all voice calls in “setup” phase, because the CMTS requires human intervention to reconfigure and bring the CMTS back online.

Configuration for 1+1 redundancy takes place at the cable interface line card interface level. That is, rather than assigning an entire Cisco uBR7200 series router to support another Cisco uBR7200 series router, individual interfaces on one Cisco uBR7200 series router are configured to protect individual interfaces installed in a different Cisco uBR7200 series router.

Note 1+1 redundancy protection takes place only on an inter chassis basis. That is, you cannot protect cable interfaces on a particular CMTS with cable interfaces installed in the same chassis.

You can configure the system to switch over automatically when the interface state of a cable interface line card interface moves from "up" to "down." Alternatively, you can manually force a switch over.

Note Ensure that the same channel ID is configured for both the active and the standby cable router.

For more information on the 1+1 redundancy feature, including information on configuration tasks and command reference, refer to the document on Cisco.com:

- *Hot-Standby 1+1 Redundancy*

  http://www.cisco.com/en/US/docs/cable/cmts/feature/HCCPfeat.html

IF Muting for HCCP N+1 Redundancy

Beginning with Cisco IOS Release 12.2(15)BC2a, Cisco supports IF Muting with both SNMP and non-SNMP-capable upconverters in HCCP N+1 Redundancy. IF Muting offers the following benefits:

- IF Muting for either type of upconverter significantly increases the N+1 protection schemes that are available for Cisco CMTS headends.
- IF Muting offers the additional benefit of being faster than RF Muting.
- IF Muting is enabled by default. The Cisco CMTS automatically enjoys the benefits and availability of IF Muting.

For additional information about IF Muting and configuring HCCP N+1 Redundancy, refer to the following document on Cisco.com:

- *HCCP N+1 Redundancy for the Cisco Cable Modem Termination System*

  http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/uFGnpls1.html#wp1049303

Intercept Features

The Cisco uBR7200 Series supports several intercept features through multiple Cisco IOS release trains:

- Access Control List Support for COPS Intercept, page 1-72
- Cable Monitor Enhancements, page 1-73
- COPS TCP Support for the Cisco Cable Modem Termination System, page 1-74
- Service Independent Intercept (SII) Support on the Cisco uBR7200 Series, page 1-78

Access Control List Support for COPS Intercept

Cisco IOS Release 12.3(13a)BC introduces enhanced support for Access Control Lists (ACLs) and associated commands for the Common Open Policy Service (COPS) feature.

To configure access control lists (ACLs) for inbound connections to all COPS listener applications on the Cisco CMTS, user the **cops listeners access-list** command in global configuration mode. To remove this setting from the Cisco CMTS, us the **no** form of this command.

cops listeners access-list {*acl-num* | *acl-name*}

no cops listeners access-list {*acl-num* | *acl-name*}

Syntax Description

acl-num	Alphanumeric identifier of up to 30 characters, beginning with a letter that identifies the ACL to apply to the current interface.
acl-name	Numeric identifier that identifies the access list to apply to the current interface. For standard access lists, the valid range is 1 to 99; for extended access lists, the valid range is 100 to 199.

Additional Information

Refer also the Service Independent Intercept (SII) feature in this document. For additional information, refer to the following documents on Cisco.com:

- *Configuring COPS for RSVP, Cisco IOS Versions 12.2 and 12.3*

  http://www.cisco.com/en/US/docs/ios/12_2/qos/configuration/guide/qcfcops_ps1835_TSD_Products_Configuration_Guide_Chapter.html
- *Cable Monitor and Intercept Features for the Cisco CMTS*

  http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/ufg_cmon.html
- *PacketCable and PacketCable Multimedia on the Cisco CMTS*

  http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/ufg_pkcb.html
- *Cisco PacketCable Primer White Paper*

  http://www.cisco.com/en/US/netsol/ns341/ns121/ns342/ns343/networking_solutions_white_paper09186a0080179138.shtml

Cable Monitor Enhancements

Cisco IOS Release 12.3(17a)BC introduces the following enhancements to the cable monitor feature:

- Access Control Lists are now supported on the Cisco uBR-MC5X20U/D and Cisco uBR-MC28U cable interface line cards
- Unconditional downstream sniffing now enables downstream packets to be monitored, either for MAC or data packets. This enhancement supports both DOCSIS and Ethernet packet encapsulation.

For additional information about this enhancements to the cable monitor feature, refer to the following documents on Cisco.com:

- *Cable Monitor and Intercept Features on the Cisco CMTS*

  http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/ufg_cmon.html

COPS TCP Support for the Cisco Cable Modem Termination System

Cisco IOS Release 12.3(13a)BC introduces optimized support for the Common Open Policy Service (COPS) feature for the Cisco uBR7200 series routers. This feature supports two new configuration commands for enabling and setting COPS processes. The COPS feature in Cisco 12.3(13a)BC enables the following COPS functions:

COPS DSCP Marking for the Cisco CMTS

This feature allows you to change the DSCP marking for COPS messages that are transmitted or received by the Cisco router. Differentiated Services Code Point (DSCP) values are used in Quality of Service (QoS) configurations on a Cisco router. DSCP summarizes the relationship between DSCP and IP precedence.

Cisco IOS Release 12.3(13a)BC supports this function with the **cops ip dscp** command in global configuration mode.

COPS TCP Window Size for the Cisco CMTS

This feature allows you to override the default TCP receive window size that is used by COPS processes. This setting can be used to prevent the COPS server from sending too much data at one time.

Cisco IOS Release 12.3(13a)BC supports this function with the **cops tcp window-size** command in global configuration mode.

Note These two commands affect all TCP connections with all COPS servers.

cops ip dscp

To specify the marking for COPS messages that are transmitted by the Cisco router, use the **cops ip dscp** command in global configuration mode. To remove this configuration, use the **no** form of this command.

cops ip dscp *x*

no cops ip dscp

Syntax Description

x	This value specifies the markings with which COPS messages are transmitted. The following values are supported: • 0-63—DSCP value ranging from 0-63. • af11—Use AF11 dscp (001010) • af12—Use AF12 dscp (001100) • af13—Use AF13 dscp (001110) • af21—Use AF21 dscp (010010) • af22—Use AF22 dscp (010100) • af23—Use AF23 dscp (010110) • af31—Use AF31 dscp (011010) • af32—Use AF32 dscp (011100) • af33—Use AF33 dscp (011110) • af41—Use AF41 dscp (100010) • af42—Use AF42 dscp (100100) • af43—Use AF43 dscp (100110) • cs1—Use CS1 dscp (001000) [precedence 1] • cs2—Use CS2 dscp (010000) [precedence 2] • cs3—Use CS3 dscp (011000) [precedence 3] • cs4—Use CS4 dscp (100000) [precedence 4] • cs5—Use CS5 dscp (101000) [precedence 5] • cs6—Use CS6 dscp (110000) [precedence 6] • cs7—Use CS7 dscp (111000) [precedence 7] • default—Use default dscp (000000) • ef—Use EF dscp (101110)

Defaults

- For messages transmitted by the Cisco router, the default DSCP value is 0.
- For incoming connections to the Cisco router, by default, the COPS engine takes the DSCP value used by the COPS server that initiates the TCP connection.

Usage Guidelines

- The **cops ip dscp** command allows the Cisco router to re-mark the COPS packets for either incoming or outbound connections.
- This command affects all TCP connections with all COPS servers.
- This command does not affect existing connections to COPS servers. Once you issue this command, this function is supported only for new connections after that point in time.

Examples

The following example illustrates the cops ip dscp command with supported command variations:

```
Router(config)# cops ip dscp ?
 <0-63>   DSCP value
 af11     Use AF11 dscp (001010)
 af12     Use AF12 dscp (001100)
 af13     Use AF13 dscp (001110)
 af21     Use AF21 dscp (010010)
 af22     Use AF22 dscp (010100)
 af23     Use AF23 dscp (010110)
 af31     Use AF31 dscp (011010)
 af32     Use AF32 dscp (011100)
 af33     Use AF33 dscp (011110)
 af41     Use AF41 dscp (100010)
 af42     Use AF42 dscp (100100)
 af43     Use AF43 dscp (100110)
 cs1      Use CS1  dscp (001000) [precedence 1]
 cs2      Use CS2  dscp (010000) [precedence 2]
 cs3      Use CS3  dscp (011000) [precedence 3]
 cs4      Use CS4  dscp (100000) [precedence 4]
 cs5      Use CS5  dscp (101000) [precedence 5]
 cs6      Use CS6  dscp (110000) [precedence 6]
 cs7      Use CS7  dscp (111000) [precedence 7]
 default  Use default dscp (000000)
 ef       Use EF   dscp (101110)
```

Additional COPS Information

Cisco 12.3(13a)BC also supports Access Control Lists (ACLs) for use with COPS. Refer to the "Access Control List Support for COPS Intercept" section on page 1-72.

For additional information about configuring COPS on the Cisco CMTS, refer to the following documents on Cisco.com:

- *Cable Monitor and Intercept Features for the Cisco CMTS*

  http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/ufg_cmon.html

- *Configuring COPS for RSVP*

  http://www.cisco.com/en/US/docs/ios/12_2/qos/configuration/guide/qcfcops_ps1835_TSD_Products_Configuration_Guide_Chapter.html

- *COPS for RSVP*

  http://www.cisco.com/en/US/docs/ios/12_1t/12_1t1/feature/guide/CopsRSVP.html

cops tcp window-size

To override the default TCP receive window size on the Cisco CMTS, use the **cops tcp window-size** command in global configuration mode. This setting allows you to prevent the COPS server from sending too much data at one time. To return the TCP window size to a default setting of 4K, use the **no** form of this command.

cops tcp window-size *bytes*

no cops tcp window-size

Syntax Description

bytes	This is the TCP window size setting in bytes. This value can range from 516 to 65535 bytes.

Defaults

The default COPS TCP window size is 4000 bytes.

Usage Guidelines

This command does not affect existing connections to COPS servers. Once you issue this command, this function is supported only for new connections after that point in time.

Examples

The following example configures the TCP window size to be 64000 bytes.

```
Router(config)# cops tcp window-size 64000
```

The following example illustrates online help for this command:

```
Router(config)# cops tcp window-size ?
 <516-65535>  Size in bytes
```

Additional COPS Information

Cisco 12.3(13a)BC also supports Access Control Lists (ACLs) for use with COPS. Refer to the "Access Control List Support for COPS Intercept" section on page 1-72.

For additional information about configuring COPS on the Cisco CMTS, refer to the following documents on Cisco.com:

- *Cable Monitor and Intercept Features for the Cisco CMTS*

  http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/ufg_cmon.html

- *Configuring COPS for RSVP*

  http://www.cisco.com/en/US/docs/ios/12_2/qos/configuration/guide/qcfcops_ps1835_TSD_Products_Configuration_Guide_Chapter.html

- *COPS for RSVP*

  http://www.cisco.com/en/US/docs/ios/12_1t/12_1t1/feature/guide/CopsRSVP.html

Service Independent Intercept (SII) Support on the Cisco uBR7200 Series

The Cisco CMTS supports the Communications Assistance for Law Enforcement Act (CALEA) for voice and data. Cisco IOS Release 12.3(13a)BC introduces support for Service Independent Intercept (SII) on the Cisco uBR7200 CMTS. Cisco SII provides a more robust level of the lawful intercept (LI) options offered in the Packet Intercept feature. Cisco SII is the next level of support for judicially authorized electronic intercept, to include dial access, mobile wireless, tunneled traffic, and Resilient Transport Protocol (RTP) for voice and data traffic on the Cisco CMTS.

SII on the Cisco CMTS in Cisco IOS release 12.3(13a)BC includes these functions:

- Packet intercept on specified or unspecified interfaces or ports, including port lists
- Packet intercept on virtual interface bundles
- Corresponding SNMP MIB enhancements for each of these functions, as intercept requests are initiated a mediation device (MD) using SNMPv3

Note No new CLI commands are provided for this feature in Cisco IOS release 12.3(13a)BC.

Cisco IOS Release 12.3(13a)BC enables full Multiple Service Operator (MSO) compliance with SII and LI regulations. Service providers worldwide are legally required to allow government agencies to conduct surveillance on the service provider's traditional telephony equipment. The objective of the SII feature is to enable service providers with New World networks that legally allow government agencies to conduct electronic network surveillance.

Lawful Intercept (LI) describes the process and judicial authority by which law enforcement agencies conduct electronic surveillance of circuit and packet-mode communications. LI is authorized by judicial or administrative order and implemented for either voice or data traffic on the Cisco CMTS. Table 13 lists the differences between packet intercept and SII features

Table 13 Differences Between Packet Intercept and SII Features

Feature	Packet Intercept	Service Independent Intercept
Interface Type	Cable	Any
IP Masks	255.255.255.255 or 0.0.0.0	Any
L4 Ports	Any single port or 0-65535	Any port range
Protocol	UDP	Any
TOS/DSCP	Not supported	Supported

Additional Information

For additional information, refer to the following documents:

- *Configuring COPS for RSVP, Cisco IOS Versions 12.2 and 12.3*

  http://www.cisco.com/en/US/docs/ios/12_2/qos/configuration/guide/qcfcops_ps1835_TSD_Products_Configuration_Guide_Chapter.html
- *Cable Monitor and Intercept Features for the Cisco CMTS*

  http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/ufg_cmon.html
- *PacketCable and PacketCable Multimedia on the Cisco CMTS*

  http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/ufg_pkcb.html
- *Cisco PacketCable Primer White Paper*

  http://www.cisco.com/en/US/netsol/ns341/ns121/ns342/ns343/networking_solutions_white_paper09186a0080179138.shtml

IP Broadcast and Multicast Features

The Cisco uBR7200 Series supports the following IP broadcast and Multicast feature:

- Multicast QoS Support on the Cisco uBR7246VXR CMTS, page 1-79

Multicast QoS Support on the Cisco uBR7246VXR CMTS

Cisco IOS Release 12.3(13a)BC introduces support for Multicast downstream QoS feature. This feature t provides the ability to assign static mapping to a multicast group. The Multicast downstream QoS feature uses the existing infrastructure (DOCSIS 1.1 service flow) to assign a multicast service identifier (SID) to a multicast group used in the Baseline Privacy Interface (BPI) encryption feature.

When disabled, the Multicast downstream QoS feature does not impact any other features. The multicast packets to downstream cable interfaces are sent to the default service flow.

This feature is being implemented in response to CSCeg22989 which states, multicast traffic is not classified to any service flow, and therefore ends up queued on the default service flow. The default service flow has no specific QoS guarantees assigned to it. So once the interface approaches congestion level, multicast packets may be dropped.

Restrictions

- The multicast definitions are per-bundle, not per interface. This means that all downstreams in a bundle share the same multicast to QoS association. The downstreams will create their own service flows according to the same QoS parameters.
- Multicast to QoS definitions can not be assigned per sub-interface
- Multicast SIDs are not deleted when a group becomes idle (no response to IGMP reports).
- The QoS assignments for a multicast group can not be changed dynamically. If the user wishes to change them then a new “cable match” command must be configured.
- Multicast QoS is not supported on Multicast Echo on Cisco uBR10012 router.

New and Changed Commands

cable match address

Use the existing "cable match" command to assign QoS to a multicast group, with BPI either enabled or disabled.

```
router# cable match address <number>|<name> [service-class <name> [bpi-enable]]
router# no cable match address [<number>|<name> [service-class <name> [bpi-enable]]]
```

debug cable mcast-qos

Use this command to turn on CMTS Multicast Qos debugging.

```
router# debug cable mcast-qos
```

IP Routing Features

The Cisco uBR7200 series router offers you several features to assist with IP routing configuration and performance.

Cable ARP Filter Enhancement

The **cable arp filter** command, introduced with Cisco IOS Release 12.2(15)BC2b, enables service providers to filter ARP request and reply packets. This prevents a large volume of such packets from interfering with the other traffic on the cable network.

Cisco IOS Release 12.3(9a)BC introduces enhanced command option syntax for the **cable arp filter** command, where *number* and *window-size* values are optional for **reply-accept** and **request-send** settings.

To control the number of Address Resolution Protocol (ARP) packets that are allowable for each Service ID (SID) on a cable interface, use the **cable arp** command in cable interface configuration mode. To stop the filtering of ARP broadcasts for CMs, use the **no** form of this command.

cable arp filter {**reply-accept** *number window-size* | **request-send** *number window-size*}

no cable arp filter {**reply-accept** | **request-send**}

default cable arp filter {**reply-accept** | **request-send**}

Syntax Description

reply-accept *number window-size*	Configures the cable interface to accept only the specified *number* of ARP reply packets every *window-size* seconds for each active Service ID (SID) on that interface. The cable interface drops ARP reply packets for a SID that would exceed this number. • *number* = (Optional) Number of ARP reply packets that is allowed for each SID within the window time period. The allowable range is 0 to 20 packets, with a default of 4 packets. If *number* is 0, the cable interface drops all ARP reply packets. If not specified, this value uses default. • *window-size* = (Optional) Size of the window time period, in seconds, in which to monitor ARP replies. The valid range is 1 to 5 seconds, with a default of 2 seconds.
request-send *number window-size*	Configures the cable interface to send only the specified *number* of ARP request packets every *window-size* seconds for each active SID on that interface. The cable interface drops ARP requests for a SID that would exceed this number. • *number* = (Optional) Number of ARP request packets that is allowed for each SID within the window time period. The allowable range is 0 to 20 packets, with a default of 4 packets. If *number* is 0, the cable interface does not send any ARP request packets. • *window-size* = (Optional) Size of the window time period, in seconds, in which to monitor ARP requests. The valid range is 1 to 5 seconds, with a default of 2 seconds.

Cisco IOS Release 12.3(9a)BC also removes a prior caveat with HCCP Protect interfaces. Previously, in the event of a revert-back HCCP N+1 switchover, manual removal of **cable arp filter reply** and **cable arp filter request** configurations may have been required afterward on Protect interfaces.

For more information about ARP Filtering, refer to the following document on Cisco.com:

- *Cable ARP Filtering*

  http://www.cisco.com/en/US/docs/cable/cmts/feature/cblarpfl.html

cable intercept Command

Use the **cable intercept** command in cable interface configuration mode to allow the CMTS to forward all traffic to and from a particular cable modem to a data collector located at particular User Datagram Protocol (UDP) port. To deactivate this function, use the **no** form of this command.

cable intercept *mac-address ip-address udp-port*

no cable intercept *mac-address*

The **cable intercept** command can be used to comply with the United States Federal Communications Assistance for Law Enforcement Act (CALEA) and other law enforcement wiretap requirements for voice communications.

Syntax Description

mac-address	Specifies the MAC address to be intercepted.
ip-address	Specifies the IP address for the destination data collector.
udp-port	Specifies the destination UDP port number for the intercept stream at the data collector. Valid range is 0 to 65535.

For additional command information, refer to the *Cisco IOS CMTS Cable Command Reference Guide*.

Cable Interface Bundling and Cable Subinterfaces

Support for cable interface bundling on the Cisco uBR7200 series commences with Cisco IOS Release 12.2(4)XF1 and continues with later Cisco 12.2 BC releases.

To reduce the number of subnets consumed per Cisco CMTS, cable interface bundling is used. Multiple cable interfaces can share a single IP subnet. An IP subnet is required for each bundle. You can bundle all cable interfaces on a Cisco CMTS into a single bundle.

Note Cable interface bundling is applicable only in two-way cable configurations. It is not supported in telco-return configurations.

Using the CLI, first configure a master interface for a cable interface bundle. The master interface has an IP address assigned and is visible for IP routing functionality. After you configure the master interface, add additional cable interfaces to the same interface bundle. Those interfaces must not have an IP address assigned. You can also configure multiple bundle interfaces.

Use the following commands to configure and view cable interface bundles:

[**no**] **cable bundle** *n* **master**

show cable bundle

Up to four interface bundles can be configured. In each bundle, specify exactly one interface as the master interface, using the "master" keyword. In the case of a subinterface over a cable bundle, `x' is the interface number of the bundle master [1]. The subinterface number starts from 1.

Caution Configure an IP address on the master interface only. An attempt to add an interface to a bundle will be rejected if an IP address is configured and the interface is not specified as a master interface.

When bundling cable interfaces, only the interface configured to be the bundle master is allowed to have subinterfaces. An interface that has subinterface(s) defined over it will not be allowed to be part of a bundle. MIB objects on cable interface bundles are not supported as of the date of this publication.

For more information on cable bundling, refer to these documents on Cisco.com:

- *Cable Interface Bundling for the Cisco uBR7200 Series Cable Router* feature module:

  http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/ufg_bund.html

- *Bundling Cable Interfaces Sample Configuration and Verification*, TAC Document ID 44122

  http://www.cisco.com/en/US/products/hw/cable/ps2217/products_configuration_example09186a00801ae255.shtml

Configurable Alternate Termination System Information Messages

The registration IP address that is included in Termination System Information messages is now configurable for telco return. Previously, the downstream channel IP address of the uBR7200 was used as the registration IP address.

To select a different IP address for the telco-return cable modem to send its registration requests, use the **cable telco-return registration-ip** command in cable interface configuration mode. To restore the default value, use the **no** form of this command.

cable telco-return registration-ip *ip-address*

no cable telco-return registration-ip

Syntax Description

ip-address	Registration IP address that is sent in Termination System Information (TSI) messages. Value is any of the cable interface's IP addresses.

For additional information about telco return and the **cable telco-return registration-ip** command, refer to these documents on Cisco.com:

- "Telephone Return for the Cisco uBR7200 Series Cable Router" chapter in the Cisco Cable Modem Termination System Feature Guide:

  http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/cmtsfg.html

- *cable telco-return registration-ip Command in the Cisco IOS CMTS Cable Command Reference Guide*

  http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_09_cable_t.html#wp1014477

Easy IP (Phase 1)

The Easy IP (Phase 1) feature combines Network Address Translation (NAT) and point-to-point protocol (PPP)/Internet Protocol Control Protocol (IPCP). This feature enables a Cisco router to negotiate automatically its own registered WAN interface IP address from a central server and to enable all remote hosts to access the Internet using this single registered IP address. The ability of multiple LAN devices to use the same globally unique IP address is known as overloading. Because Easy IP (Phase 1) uses existing port-level multiplexed NAT functionality within the Cisco IOS software, IP addresses on the remote LAN are invisible to the Internet.

With PPP/IPCP, the Cisco uBR7200 routers automatically negotiate a globally unique (registered) IP address for the dialer interface from the ISP router. For additional information, refer to the following document on Cisco.comk:

- *Configuring Easy IP*

  www.cisco.com/en/US/docs/ios/12_0/dial/configuration/guide/dcezip.html

Fast-Switched Policy Routing

IP policy routing can now be fast switched. Prior to this feature, policy routing could only be process switched, meaning that on most platforms, the switching rate was approximately 1000 to 10,000 packets per second. Such rates were not fast enough for many applications. Users that need policy routing to occur at faster speeds can now implement policy routing without slowing down the router.

Fast-switched policy routing supports all of the **match** commands and most of the **set** commands with a few restrictions. Refer to the chapter titled "Configuring IP Routing Protocol-Independent Features" in the *Cisco IOS IP Configuration Guide*, Release 12.2 on Cisco.com.

IP Enhanced IGRP Route Authentication

The latest Interior Gateway Routing Protocol (IGRP) is an enhanced version of the IGRP developed by Cisco. Enhanced IGRP uses the same distance vector algorithm and distance information as IGRP. However, the convergence properties and the operating efficiency of Enhanced IGRP have improved significantly over IGRP.

The convergence technology is based on research conducted at SRI International and employs an algorithm referred to as the Diffusing Update Algorithm (DUAL). This algorithm guarantees loop-free operation at every instant throughout a route computation and allows all devices involved in a topology change to synchronize at the same time. Routers that are not affected by topology changes are not involved in recomputations. The convergence time with DUAL rivals that of any other existing routing protocol.

For configuration information, refer to the following document on Cisco.com:

- "Configuring IP Enhanced IGRP" chapter in the *Cisco IOS IP Routing Configuration Guide*, Release 12.2

  http://www.cisco.com/en/US/docs/ios/12_2/ip/configuration/guide/1cfeigrp.html

IP Network Address Translation/Port Address Translation

Network Address Translation (NAT) is a mechanism for conserving registered IP addresses in large networks and simplifying IP addressing management tasks. As its name implies, Cisco IOS NAT translates IP addresses within private "internal" networks to "legal" IP addresses for transport over public "external" networks (such as the Internet). Incoming traffic is translated back for delivery within the inside network.

Thus, Cisco IOS NAT allows an organization with unregistered "private" addresses to connect to the Internet by translating those addresses into globally registered IP addresses. Cisco IOS NAT also increases network privacy by hiding internal IP addresses from external networks.

You can configure several internal addresses with NAT to only one or a few external addresses by using a feature called Port Address Translation (PAT) which is also referred to as "overload," a subset of NAT functionality.

PAT uses unique source port numbers on the Inside Global IP address to distinguish between translations. Because the port number is encoded in 16 bits, the total number could theoretically be as high as 65,536 per IP address. PAT will attempt to preserve the original source port, if this source port is already allocated PAT will attempt to find the first available port number starting from the beginning of the appropriate port group 0-511, 512-1023, or 1024-65535. If there is still no port available from the appropriate group and more than one IP address is configured, PAT will move to the next IP address and try to allocate the original source port again. This continues until it runs out of available ports and IP addresses.

For the first steps in configuring Network Address Translation, refer to the following document on Cisco.com:

- *"Configuring Network Address Translation: Getting Started*

  http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a0080094e77.shtml

For additional information about IP NAT and PAT, refer to the following document on Cisco.com:

- *"Product Bulletin No. 1195, Cisco IOS Network Address Translation (NAT)*

  http://www.cisco.com/en/US/products/ps6640/index.html

NAT—Support for NetMeeting Directory (Internet Locator Service—ILS)

The Cisco IOS Network Address Translation (NAT) supports the Microsoft NetMeeting directory. Microsoft NetMeeting is a Windows-based application that enables multi user interaction and collaboration from a user's PC over the Internet or an intranet. Support for the NetMeeting Directory (ILS) allows connections by name from the directory built into the NetMeeting application. Destination IP addresses do not need to be known in order for a connection to be made.

For additional information, refer to the following document on Cisco.com:

- *NAT—Support for NetMeeting Directory (Internet Locator Service—ILS)*

  http://www.cisco.com/en/US/docs/ios/12_1t/12_1t5/feature/guide/dtnatils.html

Router-Port Group Management Protocol

The Router-Port Group Management Protocol (RGMP) feature introduces a Cisco protocol that restricts IP multicast traffic in switched networks. RGMP is a Layer 2 protocol that enables a router to communicate to a switch (or a networking device that is functioning as a Layer 2 switch) the multicast group for which the router would like to receive or forward traffic. For additional information, refer to the following document on Cisco.com:

- *Router-Port Group Management Protocol*

  http://www.cisco.com/en/US/docs/ios/12_1t/12_1t5/feature/guide/dtrgmp.html

Supported Protocols on the Cisco uBR7200 Series

The Cisco uBR7200 Series supports multiple protocols of multiple classes, including but not limited to, the following:

- Address Resolution Protocol (ARP)
- Cisco Discovery Protocol (CDP)
- Domain Name System (DNS)
- Internet Protocol (IP) v4/v5
- Simple Network Management Protocol (SNMP) v2 and SNMPv3 Integrated Dynamic Host Configuration Protocol (DHCP) server
- Trivial File Transfer Protocol (TFTP) client
- User Datagram Protocol (UDP)

Note Be aware that when configuring a routing protocol, the Cisco IOS software must reset the interfaces to enable the change. This normally does not significantly affect operations on the interface, except that when this is done on a cable interface, it causes all cable modems on that particular downstream to reinitialize, potentially interfering with data transmission on that downstream. Therefore, you should use routing global configuration commands, such as router rip, on a cable interface only when a minimum of subscribers would be affected.

For additional information about configuring IP routing protocols, refer to the following document on Cisco.com:

- "IP Routing Protocols" chapter in the *Cisco IOS IP Configuration Guide*, Release 12.2

  http://www.cisco.com/en/US/docs/ios/12_2/ip/configuration/guide/1cfodr.html

Management Features

The Cisco uBR7200 series routers provide you with the following features that make CMTS headend configuration, management, and DOCSIS support more powerful and efficient:

Admission Control for the Cisco CMTS

Admission Control for the Cisco Cable Modem Termination System (CMTS) is a multifaceted feature that implements a Quality of Service (QoS) policy on the CMTS Headend. Admission Control establishes efficient resource and bandwidth utilization in a way that was not possible in prior Cisco IOS releases.

Admission Control monitors multiple system-level resources on the Cisco CMTS, and performs automatic resource allocation on a service-request basis. Admission Control maintains optimal system-level operation by preventing resource consumption that would otherwise degrade the performance for the entire Cisco CMTS. Furthermore, Admission Control can allocate upstream or downstream bandwidth resources to specific DOCSIS traffic types, and maintain such prioritization amidst very dynamic traffic conditions.

Admission Control uses two event types for resource monitoring and management—cable modem registration and dynamic service (voice call) requests. When either of these two events occurs on the Cisco CMTS, Admission Control verifies that the associated resources conform to the configured limits prior to admitting and supporting the service call request.

Admission Control is not a mechanism to apply QOS to the traffic flows. Scheduling and queuing are some of the mechanisms used for implementing the QOS. The QOS is applied on per packet basis. Admission Control checks are performed before the flow is committed.

Admission Control in Cisco IOS Release 12.3(13)BC monitors the following resources on the Cisco CMTS.

- *CPU utilization*—Admission Control monitors CPU utilization on the Cisco CMTS, and preserves QoS for existing service flows when new traffic would otherwise compromise CPU resources on the Cisco CMTS.
- *Memory resource utilization (I/O, Processor, and combined total)*—Admission Control monitors one or both memory resources and their consumption, and preserves QoS in the same way as CPU utilization.
- *Bandwidth utilization for upstream and downstream*—Admission Control monitors upstream and downstream bandwidth utilization, and associated service classes, whether for data or dynamic service traffic.

Cisco IOS Release 12.3(13a)BC introduces new configuration, **debug** and **show** commands for Admission Control on the Cisco CMTS. For additional information, refer to the following document on Cisco.com:

- *Admission Control for the Cisco Cable Modem Termination System*

http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/ufg_adm.pdf

Cable ARP and Proxy ARP

The **cable arp** and **cable proxy-arp** commands control whether the Cisco uBR7200 series router allows ARP requests on the cable interfaces and whether the router serves as a proxy ARP server for cable modems, so that cable modems on the same subnet can communicate with each other, without having to send the traffic through the Cisco uBR7200 series router.

For additional information about these and other CMTS commands, refer to the *Cisco IOS CMTS Cable Command Reference Guide* on Cisco.com.

cable map-advance Command Enhancements

Cisco IOS Release 12.1(10)EC updates the **cable map-advance** command with a new option, *max-delay*. The new command syntax is the following:

cable map-advance [**dynamic** [*safety*] | **static**] [*max-delay*]

The *max-delay* option specifies the maximum round trip delay between the cable plant and furthest cable modem in microseconds. The valid range is 100 to 2000 microseconds. The typical delay for a mile of coaxial cable is approximately seven microseconds. The typical delay for a mile of fiber cable is approximately eight microseconds.

A cable modem will not be allowed to exceed the maximum timing offset given by the max-delay value (in static mode) or given by the combination of the max-delay and safety values (in dynamic mode). If a cable modem reports a timing offset beyond the maximum value, the CMTS will reset its offset to the maximum value and put an exclamation point (!) next to its offset value in the show cable modem display.

In dynamic MAP operation, Cisco IOS 12.1(10)EC also implements a regular polling of the furthest cable modem, to determine if that cable modem is now offline. If the furthest cable modem has gone offline, the CMTS scans the currently online CMs to determine which is now the furthest offline and updates the dynamic MAP advance algorithm with the new value.

Tip The **show cable modem** command displays the cable modem timing offset in DOCSIS ticks. Use the following method to convert microseconds to DOCSIS ticks: ticks = microseconds*64/6.25.

cable monitor Command

The Cisco IOS command-line interface (CLI) **cable monitor** command allows an external LAN packet analyzer on the cable interface to monitor inbound and outbound data packets for specific types of traffic between the Cisco Cable Modem Termination System (CMTS) and the CMs attached to the radio frequency (RF) line card. This feature enables the CMTS administrator to analyze traffic problems with customer data exchanges.

The **cable monitor** command specifies the set of filter criteria the CMTS uses to monitor and forward copies of data packets from a cable modem, identified by its MAC address (or access list representing a group of MAC addresses). Data packets matching the filter criteria are forwarded out of a specified Ethernet or Fast Ethernet port on the CMTS to a LAN packet analyzer. The LAN packet analyzer (sometimes called "sniffer") receives the data packets, displays the data, and stores it for analysis.

For cable monitor configuration information, refer to the following document on Cisco.com:

- "Cable Monitor and Intercept Features for the Cisco CMTS" chapter in the*Cisco Cable Modem Termination System Feature Guide*

  http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/ufg_cmon.html

Cisco IOS Internationalization

Your Cisco IOS platform automatically displays 8-bit and multibyte character sets and prints the ESC character as a single character instead of as the caret and bracket symbols (^[) when the Cisco Web browser interface is enabled with the **ip http server** command.

Use the **international** command in line configuration mode to display 8-bit and multibyte international character sets and print the ESC character as a single character instead of "^[" when using Telnet to access a Cisco IOS platform.

Use the **terminal international** command in privileged EXEC mode to display 8-bit and multibyte international character sets and print the ESC character as a single character instead of "^[" when using Telnet to access a Cisco IOS platform for the current session.

For information about specifying international character sets, refer to the chapter titled"Configuring Operating Characteristics for Terminals" in the http://www.cisco.com/en/US/docs/ios/12_2/configfun/configuration/guide/ffun_c.html. To customize the user interface on a Web browser, refer to the chapter titled"Using the Cisco Web Browser User Interface" in the same guide.

DOCSIS 2.0 SAMIS ECR Data Set

The Usage-Based Billing feature for the Cisco Cable Modem Termination System (CMTS) provides subscriber account and billing information in the Subscriber Account Management Interface Specification (SAMIS) format. The SAMIS format is specified by the Data-over-Cable Service Interface Specifications (DOCSIS) Operations Support System Interface (OSSI) specification.

Release 12.3(17a)BC provides enhancements to the OSSI specifications, and billing reports (billing record format), added support to the CISCO-CABLE-METERING-MIB, which contains objects that provide subscriber account and billing information in the Subscriber Account Management Interface Specification (SAMIS) format, added support for DCC and DCC for Load balancing and Downstream LLQ.

For additional information, refer to the following document on Cisco.com:

- *Usage-Based Billing for the Cisco CMTS*

  http://www.cisco.com/en/US/docs/cable/cmts/feature/ubrsamis.html

Downstream Load Balancing Distribution with Upstream Load Balancing

Cisco IOS Release 12.3(17b)BC4 introduces further enhancements to downstream load balancing, resulting in equalized upstream load balancing group members. This enhancement synchronizes the pending statistic between different cable interface line cards in the load balancing group.

This enhancement performs downstream load balancing that accounts for loads on upstream channels in the same upstream load balancing group, rather than on the basis of the entire downstream channel load. Prior Cisco IOS releases may not have distributed cable modems evenly over individual upstream channels, nor in a way that accounted for downstream and upstream segment loads that account for one another.

This enhancement applies when downstream load balancing occurs on a headend system with separate upstream load balancing segments; the upstream segments are spread over multiple downstreams segments. This enhancement provides an alternative downstream load balancing scheme that accounts and makes use of per-upstream loads rather than total downstream loads.

For additional information about Load Balancing on the Cisco CMTS, refer to the following documents on Cisco.com:

- *Load Balancing and Dynamic Channel Change on the Cisco CMTS*

  http://www.cisco.com/en/US/docs/cable/cmts/troubleshooting_batch9/cmtslbg.html
- *Cisco IOS CMTS Cable Command Reference Guide*

  http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html

Dynamic Channel Change (DCC) for Loadbalancing

Cisco IOS Release 12.3(17a)BC introduces Dynamic Channel Change (DCC) and DCC for Load Balancing on the Cisco CMTS.

DCC in DOCSIS 1.1 dynamically changes cable modem upstream or downstream channels without forcing a cable modem to go offline, and without re-registration after the change. DCC supports four different initializations, instead of one, as in earlier DOCSIS support.

DCC and DCC for load balancing is supported on the Cisco uBR7246VXR router and the Cisco uBR10012 router with distributed cable interface line cards, including the Cisco MC28U and the Cisco MC5X20S/U/H.

- Load Balancing techniques allow for moving cable modems with DCC by using configurable initialization techniques.
- DCC allows line card channel changes across separate downstream channels in the same cable interface line card, with the DCC initialization techniques ranging from 0 to 4.
- DCC transfers cable modem state information from the originating downstream channel to the target downstream channel, and maintains synchronization of the cable modem information between the cable interface line card and the Network Processing Engine (NPE) or Route Processor (RP).
- When the target channel is in ATDMA mode, only DOCSIS 2.0-capable modems can be successfully load balanced. (Only DOCSIS 2.0-capable modems can operate on an ATDMA-only upstream channel.) Cisco recommends identical channel configurations in a load balancing group.

Dynamic Channel Change for Load Balancing entails the following new or enhanced commands in Cisco IOS Release 12.3(17a)BC, and later releases:

Global Configuration Commands

- **cable load-balance group** *group-num* **dcc-init-technique <0-4>**
- **cable load-balance group** *group-num* **policy { pcmm | ugs }**

- **cable load-balance group** *group-num* **threshold** {**load** | **pcmm** | **stability** | **ugs**} **<1-100>**
- **cable load-balance group** *group-num* **threshold load <1-100>** {**minimum**}
- **cable load-balance group** *group-num* **threshold load <1-100>** {**enforce**}

Testing Command

- **test cable dcc** *mac-addr* {*slot/port* | *slot/subslot/port*} *target-us-channel-id ranging-technique*

For configuration, command reference, testing, and examples for DCC on the Cisco CMTS, refer to the following documents on Cisco.com:

- *Load Balancing and Dynamic Channel Change (DCC) on the Cisco CMTS*

  http://www.cisco.com/en/US/docs/cable/cmts/troubleshooting_batch9/cmtslbg.html
- *Cisco IOS CMTS Cable Command Reference Guide*

  http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html

Dynamic Ranging Support

The functionality of the **clear cable modem <***mac-address***> reset** command is extended to send a "Ranging Abort" message instead of just removing the SID.

A new modem state—Reset (display: resetting)— has been introduced into the modem state list. A modem is deprovisioned when moving into this state as if going offline. Move the modem to the Continue Ranging list. If a ranging request is received from the modem, send a "Ranging Abort" message. Continue until an "Initial Ranging" message is received or until normal timeout (16 attempts). If the modem does not go back to initial ranging, set it to offline.

The Reset modem state may show as follows in the output of the **show cable modem** command:

```
Cable4/0/U1 80 resetting 3575 0.25 3 0 10.30.160.26 0050.7318.e965
```

This is an intermediate state. A modem will not be in this state for more than a few seconds. If the modem does not respond, it may remain in this state for up to 30 seconds. The subsequent modem state is offline.

For additional command information about the **show cable modem** command, refer to the *Cisco IOS CMTS Cable Command Reference Guide*.

Enhanced Modem Status Display

The Cisco uBR7200 series universal broadband router supports polling of the CMs to obtain parameter and status information on an ongoing basis. Two new Cisco IOS commands are added to support this feature.

- The **cable modem remote** command configures the router for the polling interval; the **no** version of this command disables the status polling.

- The **show cable modem remote-query** command displays the collected information:
  - Downstream receive power level
  - Downstream signal/noise ratio (SNR)
  - Upstream power level
  - Transmit timing offset
  - Micro reflection (in dB)

For additional information about the enhanced modem status display, refer to *Modem Status Enhancements for the Cisco uBR7200 Series Cable Router* on Cisco.com.

Entity MIB, Phase 1

For a complete list of MIBs supported by the Cisco uBR7200 series platform, refer to the *Cisco uBR7200 Series Software Release Notes* on Cisco.com:

http://www.cisco.com/en/US/docs/cable/cmts/ubr7200/release/notes/12_3bc/123BCu72.html

For descriptions of supported MIBs and how to use MIBs, refer to the *Cisco MIBs* web page on Cisco.com.

Load Balancing for the Cisco CMTS

The Load Balancing on the Cisco CMTS feature allows service providers to optimally use both downstream and upstream bandwidth, enabling the deployment of new, high-speed services such as voice and video services. This feature also can help reduce network congestion due to the uneven distribution of cable modems across the cable network and due to different usage patterns of individual customers.

By default, the Cisco CMTS platforms use a form of load balancing that attempts to equally distribute the cable modems to different upstreams when the cable modems register. You can refine this form of load balancing by imposing a limit on the number of cable modems that can register on any particular upstream, using the cable upstream admission-control command.

However, this default form of load balancing affects the cable modems only when they initially register with the Cisco CMTS. It does not dynamically rebalance the cable modems at later times, such as when they might change upstream channels in response to RF noise problems, or when bandwidth conditions change rapidly because of real-time traffic such as Voice over IP (VoIP) and video services. It also does not affect how the cable modems are distributed among downstream channels.

For more information about the Load Balancing feature, refer to the following document on Cisco.com:

- *Configuring Load Balancing on the Cisco CMTS*

  http://www.cisco.com/en/US/docs/cable/cmts/troubleshooting_batch9/cmtslbg.html

Management Information Base (MIB) Changes and Enhancements

MIB enhancements in Cisco IOS Release 12.3(17a)BC provide enhanced management features that enable the Cisco uBR 7200 Series router and the Cisco uBR10012 router to be managed through the Simple Network Management Protocol (SNMP). These enhanced management features allow you to:

- Use SNMP set and get requests to access information in Cisco CMTS universal broadband routers.
- Reduce the amount of time and system resources required to perform functions like inventory management.
- A standards-based technology (SNMP) for monitoring faults and performance on the router.

- Support for SNMP versions (SNMPv1, SNMPv2c, and SNMPv3).
- Notification of faults, alarms, and conditions that can affect services.

Additional Information

To access the *Cisco CMTS Universal Broadband Router MIB Specifications Guide*, go to:

http://www.cisco.com/en/US/docs/cable/cmts/mib/reference/guide/ubrmibv5.html

MAX-CPE Override for Cable Modems

The following cable-specific configuration command provides a way to override the MAX-CPE parameter in the cable modem's DOCSIS configuration file:

[**no**] **cable modem max-cpe** [<*n*> | **unlimited**]

When set to unlimited or if *n* is larger than the MAX-CPE value in the configuration file of a cable modem, it overrides the configuration file value.

Note The **cable max-hosts** and **cable modem max-hosts** commands can also be used to set this value for all cable modems on a particular cable interface or for a particular cable modem.

For additional command information, refer to these documents on Cisco.com:

- *Cisco IOS CMTS Cable Command Reference Guide*

  http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html
- "Maximum CPE or Host Parameters for the Cisco Cable Modem Termination System" chapter in the *Cisco Cable Modem Termination System Feature Guide*

  http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/ufg_Max.html
- *Using the max-cpe Command in the DOCSIS and CMTS*, TAC Document ID: 22177

  http://www.cisco.com/en/US/tech/tk86/tk168/technologies_tech_note09186a00800a7609.shtml

Per-Modem Error Counter Enhancements

The Cisco uBR7200 Series supports display of per-modem error counters with the following new command:

show cable modem [<*ip-addr*> | <*mac-addr*>] **error**

Below is an example display from the **show cable modem error** command:

```
Router# show cable modem error

MAC Address    SID   I/F          CRC        HCS
00d0.ba26.eee7 1     Cable4/0/U0  0          0
```

Note Both the Cyclic Redundancy Check (CRC) and Header Check Sum (HCS) are on a per- cable modem basis.

For additional command information about the **show cable modem** command, refer to the *Cisco IOS CMTS Cable Command Reference Guide* on Cisco.com.

Pre-equalization Control for Cable Modems

Cisco IOS Release 12.3(17a)BC introduces pre-equalization control for cable modems on a per-modem basis. This feature enhances support for pre-equalization control on an interface basis with the Organizational Unique Identifier (OUI), which is also supported.

When pre-equalization is enabled on an upstream interface, this feature allows you to disable pre-equalization adjustment selectively, for a specific cable modem or a group of cable modems. This feature prevents cable modems from flapping when processing pre-equalization requests sent from the Cisco CMTS.

Restrictions

This feature observes the following restrictions in Cisco IOS Release 12.3(17a)BC:

- For pre-equalization to be supported on a per-modem basis, the cable modem must send verification of pre-equalization after it registers with the Cisco CMTS.
- The option of excluding the OUI is a global configuration. For the cable modem on which OUI is excluded, the excluded OUI is disabled for all interfaces. This method uses a list of OUI values, recording which modems are sent and not sent pre-equalization.
- To remove this exclusion, use the **no cable pre-equa exclude** {**modem**|**oui**} form.

cable pre-equalization exclude

To exclude a cable modem from pre-equalization during registration with the Cisco CMTS, use the **cable pre-equalization exclude** command in global configuration mode. Exclusion is supported for a specified cable modem, or for a specified OUI value for the entire interface. To remove exclusion for the specified cable modem or interface, use the **no** form of this command. Removing this configuration returns the cable modem or interface to normal pre-equalization processes during cable modem registration.

cable pre-equalization exclude {**oui** | **modem**} *mac-addr*

no cable pre-equalization exclude {**oui** | **modem**} *mac-addr*

Syntax Description

oui	Organizational Unique identifier for the interface specified. Using this keyword excludes the specified OUI during cable modem registration for the associated interface.
modem	Cable Modem identifier for the cable modem specified. Using this keyword excludes the cable modem.
mac-addr	Identifier for the OUI or cable modem to be excluded.

Command Default

Pre-equalization is enabled by default on the Cisco router, and for cable modems that have a valid and operational DOCSIS configuration file. When enabled, pre-equalization sends ranging messages for the respective cable modems. When disabled with the new **exclude** command, pre-equalization is excluded for the respective cable modems.

Command Modes

Global configuration mode

Command History

Release	Modification
12.3(17a)BC	This command was introduced to the Cisco uBR10012 router and the Cisco uBR7246VXR router.

Usage Guidelines

The pre-equalization exclusion feature should be configured for the running configuration of the Network Processing Engine (NPE), the Performance Routing Engine (PRE), and the line card console.

Examples

The following example configures pre-equalization to be excluded for the specified cable modem. Pre-equalization data is not sent for the corresponding cable modem:

```
Router(config)# cable pre-equalization exclude modem mac-addr
```

The following example configures pre-equalization to be excluded for the specified OUI value of the entire interface. Pre-equalization data is not sent for the corresponding OUI value of the entire interface:

```
Router(config)# cable pre-equalization exclude oui mac-addr
```

The following series of commands configures pre-equalization on the Cisco uBR7246VXR router with MC5X20U BPEs. On the PRE Console, configure the following commands.

```
Router# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# cable pre-equalization exclude oui 00.09.04
Router(config)# end
Router# show run
Router# show running-config | inc oui
cable pre-equalization exclude oui 00.09.04
Router#
```

On the line card console for the same Cisco uBR7246VXR router, verify the configuration with the following command:

```
clc_7_1# show running-config | inc oui
cable pre-equalization exclude oui 00.09.04
clc_7_1#
```

The following series of commands configures pre-equalization on the Cisco uBR7246VXR router with MC28U cable interface line cards. On the Network Processing Engine (NPE) console, configure and verify with the following commands.

```
npeg1-test# conf t
Enter configuration commands, one per line. End with CNTL/Z.
npeg1-test(config)# cable pre-equalization exclude oui 00.09.24
npeg1-test(config)# end
npeg1-test#show ru
02:58:10: %SYS-5-CONFIG_I: Configured from console by consolen
npeg1-test# show running-config | inc oui
cable pre-equalization exclude oui 00.09.24
npeg1-test#
```

On the line card console for the same Cisco uBR7246VXR router, verify the configuration with the following command:

```
clc_4_0# show running-config | inc oui
cable pre-equalization exclude oui 00.09.24
clc_4_0#
```

After either of these exclusion methods for pre-equalization are configured, you can verify that all ranging messages do not include pre-equalization data. Use the following debug commands in global configuration mode:

- **debug cable range**
- **debug cable interface** cx/x/x mac-addr

Verify the ranging message for the non-excluded cable modems include pre-equalization data, and for the excluded cable modems, the ranging messages do not include such data.

The following example removes pre-equalization exclusion for the specified OUI and interface. This results in the cable modem or OUI to return to normal pre-equalization functions. Ranging messages resume sending pre-equalization data.

```
Router(config)# no cable pre-equalization exclude { oui | modem } mac-addr
```

Removal of this feature can be verified with the following **debug** command:

- **debug cable interface** cx/x/x mac-ad—Verifies the ranging message for all non-excl modems include pre-eq data, and for the excluded modems ranging messages do not include pre-eq data.

For additional information about this feature, refer to the following documents on Cisco.com:

- *DOCSIS 1.1 for the Cisco CMTS*

  http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/ufg_docs.html
- *Cisco Broadband Cable Command Reference Guide*

  http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html

Subscriber Traffic Management (STM) Version 1.1

Cisco IOS Release 12.3(9a)BC introduces support for Subscriber Traffic Management (STM) Version 1.1 with the Cisco Broadband Troubleshooter (CBT) Version 3.2 on the Cisco uBR7246VXR universal broadband router.

STM 1.1 extends earlier STM functions to monitor a subscriber's traffic on DOCSIS 1.1 primary service flows and supports these additional features:

- Cisco Broadband Troubleshooter (CBT) 3.2 supports STM 1.1.
- DOCSIS 1.0-compliant and DOCSIS 1.1-compliant cable modem are supported.
- Monitoring and application of traffic management policies are applied on a service-flow basis.
- Monitoring window duration increased from seven to 30 days.

For additional information about STM 1.1 and Cisco CBT 3.2, refer to the following document on Cisco.com:

- *Subscriber Traffic Management for the Cisco CMTS*

  https://www.cisco.com/en/US/docs/cable/cmts/feature/ubsubmon.html
- *Release Notes for Cisco Broadband Troubleshooter Release 3.2*

  http://www.cisco.com/en/US/products/sw/netmgtsw/ps530/prod_release_notes_list.html

Usage Based Billing (SAMIS)

Cisco IOS Release 12.3(9a)BC introduces the Usage-Based Billing feature on the Cisco uBR7246VXR universal broadband router, supporting DOCSIS 1.0- and DOCSIS 1.1-compliant cable modems. This feature provides subscriber account and billing information in the Subscriber Account Management Interface Specification (SAMIS) format. SAMIS is specified by the Data-over-Cable Service Interface Specifications (DOCSIS) Operations Support System Interface (OSSI) specification.

For additional information about configuring and monitoring Usage-Based Billing (SAMIS) on the Cisco uBR7246VXR CMTS, refer to the following document on Cisco.com:

- *Usage Based Billing for the Cisco CMTS*

  http://www.cisco.com/en/US/docs/cable/cmts/feature/ubrsamis.html

Multicast Features

The Cisco uBR7200 Series supports the following multicast options:

- Bidirectional PIM, page 1-96
- DOCSIS Set-top Gateway (DSG) 1.0, page 1-97
- Advanced-mode DOCSIS Set-Top Gateway Issue 1.1, page 1-97
- Advanced-mode DOCSIS Set-Top Gateway Issue 1.2, page 1-99
- IGMP Version 3, page 1-99
- IP Multicast Load Splitting across Equal-Cost Paths, page 1-99
- IP Multicast over ATM Point-to-Multipoint Virtual Circuits, page 1-100
- IP Multicast over Token Ring LANs, page 1-100
- Source Specific Multicast, page 1-101
- Stub IP Multicast Routing, page 1-101

Bidirectional PIM

Cisco IOS Releases—Supported in the Cisco IOS 12.2 BC and 12.1 EC release trains.

Bidirectional Protocol Independent Multicast (bidir-PIM) is a variant of the Protocol Independent Multicast (PIM) suite of routing protocols for IP multicast. In PIM, packet traffic for a multicast group is routed according to the rules of the mode configured for that multicast group. The Cisco IOS implementation of PIM supports three modes for a multicast group:

- Bidirectional mode
- Dense mode
- Sparse mode

A router can simultaneously support all three modes or any combination of them for different multicast groups. In bidirectional mode, traffic is only routed along a bidirectional shared tree that is rooted at the rendezvous point (RP) for the group. In bidir-PIM, the IP address of the RP acts as the key to having all routers establish a loop-free spanning tree topology rooted in that IP address. This IP address does not need to be a router, but can be any unassigned IP address on a network that is reachable throughout the PIM domain. Using this technique is the preferred configuration for establishing a redundant RP configuration for bidir-PIM.

For additional information about bidir-PIM and its configuration, refer to *Configuring Bidirectional PIM* in the *Cisco IOS IP Configuration Guide*, Release 12.2 on Cisco.com.

DOCSIS Set-top Gateway (DSG) 1.0

The following DSG 1.0 features were added for multiple Cisco CMTS platforms in Cisco IOS release 12.3(9a)BC:

- Vendor names are supported to 20 characters per SNMP requirements (all platforms).
- SNMP MIB support introduced for the DSG-IF-MIB.
- Multicast MAC addresses are supported for DSG tunnels. DSG tunnel MAC addresses are no longer limited only to unicast addresses.
- DSG 1.0 prevents the configuration of any reserved or otherwise inappropriate IP multicast addresses.

For additional information about configuring and using DSG 1.0 on the Cisco uBR7246VXR router, refer to the following document on Cisco.com:

- *DOCSIS Set-Top Gateway for the Cisco CMTS*

  http://www.cisco.com/en/US/products/hw/cable/ps2217/products_feature_guides_list.html

Advanced-mode DOCSIS Set-Top Gateway Issue 1.1

Cisco IOS Release 12.3(13a)BC introduces support for DOCSIS Set-Top Gateway (DSG) Issue 1.1 on the Cisco uBR10012 router. DOCSIS Set-Top Gateway (DSG) 1.1 introduces Advanced mode DSG functionality based on Cablelabs specification CM-SP-DSG-I03-041124 on the Cisco uBR7246VXR and uBR10012 platforms.

DSG 1.1 introduces support for several DOCSIS 1.1 networks and their multiple service operators (MSOs):

- Supports advanced mode capabilities such as DCD, Regionalization, Fragmentation, and Quality of Service (QoS).
- Retains the essential nature of out of band (OOB) messaging, but moves it to a modern technology base, offering enhanced security for Multicast delivery of OOB messages dynamically to Set-top boxes.
- Replaces single-vendor, low-density, special-purpose equipment on the network, with significantly increased subscriber bandwidth and traffic.
- Consolidates cable modem and STB data traffic on a shared DOCSIS channel.
- Increases high-speed data (HSD) services to cable TV subscribers over the DOCSIS 1.1 infrastructure,
- Extends support for DOCSIS 1.1 digital video broadcast traffic.
- Enables shared or dedicated support for either HSD or video traffic.
- Supports one- or two-way operations, and advanced, two-way interactive applications such as streaming video, Web browsing, email, real-time chat applications, and targeted advertising services.

These powerful advantages maximize the performance and return of hybrid fiber-coaxial (HFC) plant investments.

Changes from Cisco DSG 1.0

DSG Issue 1.0 is oriented to the DOCSIS DSG-I01 specifications, while DSG Issue 1.1 is oriented towards DOCSIS DSG-I02 specifications, to include the new Advanced Mode DSG (A-DSG).

The following DSG 1.1 features are supported in 12.3(13a)BC while continuing support for Basic Mode DSG:

- DSG 1.1 enables the learning of dynamic tunnel definitions. DSG 1.0 only had static tunnel definitions (programmed into the set-top box).
- DSG 1.1 features new Cisco IOS command-line interface (CLI) configuration and **show** commands for A-DSG configuration and network information.

Unlike earlier issues of DSG, Advanced-mode DSG (A-DSG) uses a DOCSIS MAC Management Message called the Downstream Channel Descriptor (DCD) message, and this DCD message manages the DSG Tunnel traffic. The DCD message is sent once per second on each downstream and is used by the DSG Client to determine which tunnel and classifier to use.

The DCD has a DSG address table located in the DOCSIS MAC management message. The primary difference between DSG 1.0 (and earlier issues) and A-DSG 1.1 is that advanced mode uses DCD messages to manage the DSG tunnels.

The DCD message contains a group of DSG Rules and DSG Classifiers, including the following:

- DSG rules and rule priority
- DSG classifiers
- DSG channel list type/length value (TLV)
- DSG client identifier (whether broadcast, CA System, application, or MAC-level)
- DSG timer list
- DSG upstream channel ID (UCID) list
- Vendor-specific information field

Prerequisites for DSG 1.1

- Cisco IOS release 12.3(13a)BC or a later 12.3 BC release are required.
- Cisco DSG 1.1 is supported on the Cisco uBR10012 router with PRE2 performance routing engine modules.
- Cisco DSG 1.1 is supported on the Cisco uBR10012 router with the following cable interface line cards and broadband processing engines (BPEs):
  - Cisco uBR10-LCP2-MC16C/MC16E/MC16S Cable Interface Line Card
  - Cisco uBR10-LCP2-MC28C Cable Interface Line Card
  - Cisco uBR10-MC5X20S/U Broadband Processing Engine

Restrictions and Caveats for DSG 1.1

Cisco DSG 1.1 has the following restrictions:

- Cisco DSG 1.1 does not support the PRE1 module on the Cisco uBR10012 router.
- Cisco DSG 1.1 does not support Service Flow Quality of Service (QoS), which is available at Layer 3.
- Cisco DSG 1.1 does not support tunnel security, but strictly access control lists (ACLs).
- Cisco DSG 1.1 does not support subinterfaces.
- Cisco DSG 1.1 does not support HCCP N+1 interoperability.
- Cisco DSG 1.1 does not support SNMP MIBS for A-DSG.

Additional Information about DSG 1.1

- *Advanced-mode DOCSIS Set-Top Gateway Issue 1.1 for the Cisco CMTS*

  http://www.cisco.com/en/US/products/hw/cable/ps2217/products_feature_guides_list.html
- *DOCSIS Set-Top Gateway (DSG) for the Cisco CMTS*

  http://www.cisco.com/en/US/products/hw/cable/ps2217/products_feature_guides_list.html
- *Cisco DOCSIS Set-top Gateway* White Paper

  http://www.cisco.com/en/US/products/hw/cable/ps2217/products_white_paper09186a00801b3f0f.shtml#wp1002158
- CableLabs *DOCSIS Set-top Gateway (DSG) Interface Specification SP-DSG-I03-041124*

  http://www.cablelabs.com/specifications/CM-SP-DSG-I03-041124.pdf

Advanced-mode DOCSIS Set-Top Gateway Issue 1.2

Cisco IOS Release 12.3(17a)BC2 introduces support for advanced-mode DOCSIS Set-Top Gateway (DSG) Issue 1.2. DSG Issue 1.2 introduces support for the latest DOCSIS Set-Top specification from CableLabs™:

- *DOCSIS Set-top Gateway (DSG) Interface Specification*, CM-SP-DSG-I05-050812

  http://www.cablelabs.com/specifications/CM-SP-DSG-I05-050812.pdf

Advanced-mode DSG 1.2 is a powerful tool in support of latest industry innovations. Advanced-mode DSG 1.2 offers substantial support for enhanced DOCSIS implementation in the Broadband Cable environment. The set-top box dynamically learns the overall environment from the Cisco Cable Modem Termination System (CMTS), to include MAC address, traffic management rules, and classifiers. For additional information, refer to the following document on Cisco.com:

- *Advanced-mode DOCSIS Set-Top Gateway 1.2 for the Cisco CMTS*

  http://www.cisco.com/en/US/products/hw/cable/ps2217/products_feature_guides_list.html

IGMP Version 3

Internet Group Management Protocol (IGMP) is a protocol used by IPv4 systems to report IP multicast group memberships to neighboring multicast routers. On networks with hosts directly attached, IGMP Version 3 (IGMPv3) adds support for “source filtering”, which enables a multicast receiver to signal to a router which groups it wants to receive multicast traffic from, and from which source(s) this traffic is expected. Based on this membership information, Cisco IOS software only forwards traffic that is requested by the host or by other routers via Protocol Independent Multicast [PIM]) to that network. In addition to restricting traffic on the network of the receiver host, IGMPv3 membership information can also be propagated to multicast routing protocols to enable the forwarding of traffic from permitted sources or to restrict traffic from denied sources along the entire multicast data delivery path.

In the Source Specific Multicast (SSM) feature, introduced in Cisco IOS Release 12.1(3)T, hosts must explicitly include sources when joining a multicast group (this is known as “channel subscription”). IGMPv3 is the industry-designated standard protocol for hosts to signal channel subscriptions in SSM. In deployment cases where IGMPv3 cannot be used (for example, if it is not supported by the receiver host or its applications), there are two other mechanisms to enable SSM: URL Rendezvous Directory (URD) and IGMP Version 3 lite (IGMP v3lite). Both of these features were introduced with SSM in Cisco IOS Release 12.1(3)T.

IP Multicast Load Splitting across Equal-Cost Paths

You can now configure load splitting of IP multicast traffic across equal-cost paths. Prior to this feature, when there were equal-cost paths between routers, IP multicast packets traversed only one path. If a

tunnel was configured, the same next hop was always used, and no load splitting occurred. IP multicast load splitting is accomplished indirectly by consolidating the available bandwidth of all the physical links into a single tunnel interface. The underlying physical connections then use existing unicast load-splitting mechanisms for the tunnel (multicast) traffic.

Note This feature is load splitting the traffic, not load balancing the traffic.

By configuring load splitting among equal-cost paths, you can use your links between routers more efficiently when sending IP multicast traffic. For configuration information, refer to the following document on Cisco.com:

- *"Configuring IP Multicast Routing"* chapter in the*Cisco IOS IP Configuration Guide*, Release 12.2 guide on Cisco.com:

  http://www.cisco.com/en/US/docs/ios/12_2/ip/configuration/guide/fipr_c.html

IP Multicast over ATM Point-to-Multipoint Virtual Circuits

IP multicast over ATM point-to-multipoint virtual circuits is a feature that dynamically creates ATM point-to-multipoint SVCs to handle IP multicast traffic more efficiently.

The feature can enhance router performance and link utilization because packets are not replicated and sent multiple times over the ATM interface.

For configuration information, refer to the following document on Cisco.com:

- *"Configuring IP Multicast Routing"* chapter in the*Cisco IOS IP Configuration Guide*, Release 12.2 guide on Cisco.com:

  http://www.cisco.com/en/US/docs/ios/12_2/ip/configuration/guide/fipr_c.html

IP Multicast over Token Ring LANs

By default, IP multicast datagrams on Token Ring LAN segments use the MAC-level broadcast address 0xFFFF.FFFF.FFFF. That default places an unnecessary burden on all devices that do not participate in IP multicast. The IP multicast over Token Ring LANs feature defines a way to map IP multicast addresses to a single Token Ring MAC address.

This feature defines the Token Ring functional address (0xc000.0004.0000) that should be used over Token Ring. A functional address is a severely restricted form of multicast addressing implemented on Token Ring interfaces. Only 31 functional addresses are available. A bit in the destination MAC address designates it as a functional address.

The implementation used by Cisco complies with RFC 1469, *IP Multicast over Token-Ring Local Area Networks*.

If you configure this feature, IP multicast transmissions over Token Ring interfaces are more efficient than they formerly were. This feature reduces the load on other machines that do not participate in IP multicast because they do not process these packets.

For configuration information, refer to the following document on Cisco.com:

- *"Configuring IP Multicast Routing"* chapter in the*Cisco IOS IP Configuration Guide*, Release 12.2 guide on Cisco.com:

  http://www.cisco.com/en/US/docs/ios/12_2/ip/configuration/guide/fipr_c.html

Source Specific Multicast

The Source Specific Multicast (SSM) feature is an extension of IP multicast, where datagram traffic is forwarded to receivers from only those multicast sources that the receivers have explicitly joined. When SSM is used, only source-specific multicast distribution trees (no shared trees) are created.

SSM is a datagram delivery model that best supports one-to-many applications, also known as broadcast applications. SSM is the core networking technology for the Cisco implementation of the IP Multicast lite suite of solutions targeted for audio and video broadcast application environments.

This feature module introduces the following Cisco IOS components that support SSM:

- PIM-SS (PIM source specific)
- Internet Group Management Protocol Version 3 lite (IGMP v3lite)
- URL Rendezvous Directory (URD)

The Cisco implementation of SSM will soon be deployed with Internet Group Management Protocol Version 3 (IGMPv3) support. Cisco developed IGMP v3lite and URD to support the deployment of applications using SSM services before the introduction of IGMPv3.

Stub IP Multicast Routing

When you use PIM in a large network, there are often stub regions over which the administrator has limited control. To reduce the configuration and administration burden, you can configure a subset of PIM functionality that provides the stub region with connectivity, but does not allow it to participate in or potentially complicate any routing decisions.

Stub IP multicast routing allows simple multicast connectivity and configuration at stub networks. It eliminates periodic flood-and-prune behavior across slow-speed links (ISDN and below) using dense mode. It eliminates that behavior by using forwarded IGMP reports as a type of Join message and using selective PIM message filtering.

Stub IP multicast routing allows stub sites to be configured quickly and easily for basic multicast connectivity, without the flooding of multicast packets and subsequent group pruning that occurs in dense mode, and without excessive administrative burden at the central site.

For configuration information, refer to the following document on Cisco.com:

- *"Configuring IP Multicast Routing"* chapter in the *Cisco IOS IP Configuration Guide*, Release 12.2 guide on Cisco.com:

  http://www.cisco.com/en/US/docs/ios/12_2/ip/configuration/guide/fipr_c.html

PacketCable and Voice Support Features

The Cisco uBR7200 Series supports the following PacketCable and PacketCable MultiMedia feature:

- PacketCable 1.0 With CALEA, page 1-102

PacketCable 1.0 With CALEA

Cisco IOS Release 12.3(9a)BC introduces DOCSIS 1.1 support for PacketCable 1.0 with Communications Assistance for Law Enforcement Act (CALEA) on the Cisco uBR10012 universal broadband router with the Cisco uBR10-MC5X20S/U Broadband Processing Engine (BPE).

PacketCable is a program initiative from Cablelabs and its associated vendors to establish a standard way of providing packet-based, real-time video and other multimedia traffic over hybrid fiber-coaxial (HFC) cable networks. The PacketCable specification is built upon the Data-over-Cable System Interface Specifications (DOCSIS) 1.1, but it extends the DOCSIS protocol with several other protocols for use over non-cable networks, such as the Internet and the public switched telephone network (PSTN).

This allows PacketCable to be an end-to-end solution for traffic that originates or terminates on a cable network, simplifying the task of providing multimedia services over an infrastructure composed of disparate networks and media types. It also provides an integrated approach to end-to-end call signaling, provisioning, quality of service (QoS), security, billing, and network management.

Cisco IOS Release 12.2(11)BC1 and later releases in the Cisco IOS 12.3 release train support the PacketCable 1.0 specifications and the CALEA intercept capabilities of the PacketCable 1.1 specifications.

For additional information about configuring PacketCable on the Cisco CMTS, refer to the following document on Cisco.com:

- *Configuring PacketCable on the Cisco CMTS*

  http://www.cisco.com/en/US/docs/cable/cmts/feature/pcktcbl.html

Security Features

The Cisco uBR7200 Series supports multiple security features:

- Vendor-Proprietary RADIUS Attributes, page 1-109

For additional BPI information and configuration steps, refer to the *DOCSIS 1.1 for the Cisco uBR7200 Series Universal Broadband Routers* feature module on Cisco.com, and to additional documents cited below:

http://www.cisco.com/en/US/docs/cable/cmts/feature/DOCSIS11.html

Access Control Lists

Access control lists (ACLs) are supported on the Cisco uBR7200 Series in Cisco IOS Release 12.2(4)XF1 and later XF and BC releases, and in 12.2(10)EC and later EC releases.

The Cisco uBR7200 Series provides basic traffic filtering capabilities with access control lists (ACLs — also referred to as access lists). Access lists can be configured for all routed network protocols (IP, AppleTalk, and so on) to filter the packets of those protocols as the packets pass through a router.

You can configure access lists at your router to control access to a network: access lists can prevent certain traffic from entering or exiting a network.

For complete information about access lists, see the *Traffic Filtering and Firewall* volume in the *Cisco IOS Release 12.1 Security Configuration Guide*, available on Cisco.com:

http://www.cisco.com/en/US/docs/ios/12_1/security/configuration/guide/scdfirwl.html

The Cisco uBR7200 Series also supports SNMP access lists and Turbo Access Control Lists, and these are described elsewhere in this chapter.

Automated Double Authentication

The automated double authentication feature enhances the existing double authentication feature. Previously, with the existing double authentication feature, a second level of user authentication is achieved when the user accesses the network access server or router through Telnet and enters a user name and password. Now, with automated double authentication, the user does not have to Telnet anywhere but instead responds to a dialog box that requests a user name and password or PIN.

For information about the existing double authentication feature, refer to the following document on Cisco.com:

- Configuring Authentication" chapter of the *Cisco IOS Security Configuration Guide*, Release 12.2

  http://www.cisco.com/en/US/docs/ios/12_2/security/configuration/guide/fsecur_c.html

Cable Modem and Multicast Authentication Using RADIUS

As an enhancement to Baseline Privacy, the Cisco uBR7200 series universal broadband routers can be configured for cable modem and multicast authentication using the Remote Authentication Dial-In User Server (RADIUS) protocol, an access server authentication, authorization, and accounting protocol originally developed by Livingston, Inc. This release also supports additional vendor-proprietary RADIUS attributes.

When a cable modem comes online or when a JOIN request is sent through a multicast data stream, the Cisco uBR7200 series universal broadband routers send relevant information to RADIUS servers for cable modem/host authentication. This feature can be configured on a per-interface basis.

An Internet Engineering Task Force (IETF) draft standard, RFC 2138, defines the RADIUS protocol. RFC 2139 defines the corresponding RADIUS accounting protocol. Additional RFC drafts define vendor-proprietary attributes and MIBs that can be used with an SNMP manager.

For additional information, refer to the following document on Cisco.com:

- "Security Server Protocols" chapters of the *Cisco IOS Security Configuration Guide*, Release 12.2

  http://www.cisco.com/en/US/docs/ios/12_2/security/configuration/guide/fsecur_c.html

Cable Source Verification (cable source-verify Command)

The **cable source-verify** command helps to prevent the spoofing of IP addresses by CMs or their CPE devices by verifying that the upstream packets coming from each cable modem are known to be associated with the IP address in that packet. Packets with IP addresses that do not match those associated with the cable modem are dropped.

Note The **cable source-verify** [**dhcp**] cable interface command specifies that DHCP lease-query requests are sent to verify any unknown source IP address found in upstream data packets. This feature requires a DHCP server that supports the new LEASEQUERY message type.

For additional information about the **cable source-verify** command, refer to the *Cisco IOS CMTS Cable Command Reference Guide* on Cisco.com.

Cisco IOS Firewall Feature Set

The Cisco IOS Firewall feature set interoperates in seamless fashion with Cisco IOS software, providing great value for the many benefits it delivers. The most outstanding benefits include:

- Flexibility — installed on a Cisco router, this all-in-one scalable solution performs multiprotocol routing, perimeter security, intrusion detection, VPN functionality, and per-user authentication and authorization.
- Investment protection — integrating firewall functionality into a multiprotocol router leverages an existing router investment without the cost and learning curve associated with a new platform.
- VPN support — deploying Cisco IOS Firewall with Cisco IOS encryption and QoS VPN features enables extremely secure, low-cost transmissions over public networks and ensures mission—critical application traffic receives high priority delivery.
- Scalable deployment — available for a wide variety of router platforms, the Cisco IOS Firewall scales to meet any network`s bandwidth and performance requirements.
- Easier management — with Cisco ConfigMaker software, a network administrator can configure Cisco IOS security features (including the Cisco IOS Firewall, Network Address Translation, and Cisco IPSec) from a central console over the network.

For additional Cisco IOS firewall information, refer to the document titled *Cisco IOS Firewall Feature Set* on Cisco.com.

Cisco IOS Firewall Feature Enhancements

Cisco IOS Release 12.1(1a)T1 enhances the previous Cisco IOS Secure Integrated Software feature set with the following set of features:

- Context-Based Access Control (CBAC) that intelligently filters TCP and UDP packets based on the application-layer protocol. This includes Java applets, which can be blocked completely or allowed only from known and trusted sources.
- Detection and prevention of the most common denial of service (DoS) attacks, such as ICMP and UDP echo packet flooding, synchronize/start (SYN) packet flooding, half-open or other unusual TCP connections, and deliberate misfragmentation of IP packets.
- Support for a broad range of commonly used protocols, including H.323 and NetMeeting, FTP, HTTP, MS Netshow, RPC, SMTP, SQL*Net, and TFTP.
- Authentication Proxy for authentication and authorization of web clients on a per-user basis.

- Dynamic port mapping that maps the default port numbers for well-known applications to other port numbers. This can be done on a host-by-host basis or for an entire subnet, providing a large degree of control over which users can access different applications.
- Configurable alerts and audit trail.
- Intrusion Detection System (IDS) that recognizes the signatures of 59 common attack profiles. When an intrusion is detected, IDS can either send an alarm to a syslog server or to NetRanger Director, drop the packet, or reset the TCP connection.
- User-configurable audit rules.
- Configurable real-time alerts and audit trail logs.

For general information, see the description of the Cisco IOS Firewall Feature Set in the Cisco Product Catalog. For detailed information, refer to these documents on Cisco.com:

- *Cisco IOS Firewall Feature Set* documentation
- In particular, refer to the "Security Configuration Guide, Traffic Filtering" chapter:

  http://www.cisco.com/en/US/docs/ios/11_3/security/configuration/guide/secur_c.html

Dynamic Mobile Hosts

This feature addresses a security hole that occurs when the Cisco uBR7200 series router supports mobile hosts. (Mobile host are hosts that can move from one modem to another modem.) Anyone who knows the MAC address of a mobile host can "fake" the mobile host, thereby causing denial of access for the real mobile host.

To avoid this security hole, the Dynamic Mobile Hosts feature pings the mobile host on the old service identifier (SID) to verify that the host has indeed been moved.

A DHCP server is used to verify addresses and can be configured with the **cable source-verify dhcp** command; the **no cable arp** command should be configured in the CMTS to prevent it from sending ARP requests.

For additional information, refer to the *Cisco IOS CMTS Cable Command Reference Guid*e on Cisco.com:

http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html

Dynamic Shared Secret for DOCSIS

The Dynamic Shared Secret feature provides service providers a way of providing higher levels of security for their Data-over-Cable Service Interface Specifications (DOCSIS) cable networks, by using randomized, single-use shared secrets to verify the DOCSIS configuration files that are downloaded to each cable modem. The Dynamic Shared Secret feature is enabled using the **cable dynamic-secret** interface configuration command.

The Dynamic Shared Secret feature automatically creates a unique DOCSIS shared secret on a per-modem basis, creating a one-time use DOCSIS configuration file that is valid only for the current session. This ensures that a DOCSIS configuration file that has been downloaded for one cable modem can never be used by any other modem, nor can the same modem reuse this configuration file at a later time.

This patent-pending feature is designed to guarantee that all registered modems are using only the quality of service (QoS) parameters that have been specified by the DOCSIS provisioning system for that particular modem at the time of its registration.

For additional information, refer to the following document on Cisco.com:

- *Configuring a Dynamic Shared Secret for the Cisco CMTS* document:

  http://www.cisco.com/en/US/docs/cable/cmts/feature/ubrdmic.html

Note The Dynamic Shared Secret feature does not affect the use of the original shared secret or secondary shared secrets that are configured using the **cable shared-secondary-secret** and **cable shared-secret** commands. If these shared secrets are configured, the Cisco CMTS continues to use them to validate the original DOCSIS configuration file that is downloaded from the TFTP server. If the DOCSIS configuration file fails to pass the original or secondary shared secret verification checks, the cable modem is not allowed to register, and the Dynamic Shared Secret feature is not invoked for that particular cable modem.

Tip Verify that a cable modem is able to register with the Cisco CMTS before enabling the Dynamic Shared Secret feature.

Dynamic Shared Secret (DMIC) with OUI Exclusion for DOCSIS

Cisco IOS Release 12.3(9a)BC introduces the option of *excluding* the Organizational Unique Identifiers (OUIs) from being subjected to the DMIC check. The new **cable dynamic-secret exclude** command allow specific cable modems to be excluded from the Dynamic Shared Secret feature on the following Cisco CMTS platforms:

- Cisco uBR7246VXR universal broadband router
- Cisco uBR10012 universal broadband router

The Dynamic Shared Secret feature automatically creates a unique DOCSIS shared secret on a per-modem basis, creating a one-time use DOCSIS configuration file that is valid only for the current session. This ensures that a DOCSIS configuration file that has been downloaded for one cable modem can never be used by any other modem, nor can the same modem reuse this configuration file at a later time.

This patent-pending feature is designed to guarantee that all registered modems are using only the quality of service (QoS) parameters that have been specified by the DOCSIS provisioning system for that particular modem at the time of its registration.

For additional command information, refer to the following document on Cisco.com:

- *Configuring a Dynamic Shared Secret for the Cisco CMTS*

  http://www.cisco.com/en/US/docs/cable/cmts/feature/ubrdmic.html

- *Cisco IOS CMTS Cable Command Reference Guide*

  http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html

HTTP Security

Cisco IOS Release 12.2(4)BC1 includes the HTTP security solution introduced for earlier Cisco IOS releases and router platforms. For additional information, refer to the document titled *Cisco IOS HTTP Server Query Vulnerability*, Revision 1.3 on Cisco.com:

http://www.cisco.com/warp/public/707/cisco-sa-20001025-ios-http-server-query.shtml

Named Method Lists for AAA Authorization & Accounting

Named method lists for Authentication, Authorization, and Accounting (AAA) allow you to define different methods for authorization and accounting and apply those methods on a per-interface or per-line basis. For additional information, refer to the following document on Cisco.com:

- *Configuring Authorization*

  http://www.cisco.com/en/US/docs/ios/12_2/security/configuration/guide/scfathor.html

Per-Modem Filters (Per-Modem and Per-Host Access Lists)

Per-modem filters provide you with the ability to filter incoming packets from individual hosts or cable interfaces based on the source Media Access Controller (MAC) or Internet Protocol (IP) address. This allows access lists to be specified on a per-interface and per-direction basis. The packets received from cable interfaces and/or individual hosts are filtered based on the cable interface or the host from which the packets are received.

For additional information, refer to these documents on Cisco.com:

- "Configuring Per-Modem Filters" section on page 5-8
- *Cisco IOS CMTS Cable Command Reference Guide*

  http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html

Per-User Configuration

Per-user configuration provides a flexible, scalable, easily maintained solution for customers with a large number of dial-in users. This solution can tie together the following dial-in features:

Virtual template interfaces, generic interface configuration and router-specific configuration information stored in the form of a virtual template interface that can be applied (cloned) to a virtual access interface each time any user dials in. This is described in the following document on Cisco.com:

- "Virtual Templates, Profiles, and Networks" chapter in the *Cisco IOS Dial Technologies Configuration Guide*, Release 12.2

  http://www.cisco.com/en/US/docs/ios/12_2/dial/configuration/guide/fdial_c.html

AAA per-user security and interface configuration information stored on a separate AAA server and sent by the AAA server to the access server or router in response to authorization requests during the PPP authentication phase. The per-user configuration information can add to or override the generic configuration on a virtual interface.

Virtual profiles, which can use either or both of the two sources of information above for virtual interface configuration. When a user dials in, virtual profiles can apply the generic interface configuration and then apply the per-user configuration to create a unique virtual access interface for that user.

A virtual access interface created dynamically for any user dial-in session is deleted when the session ends. The resources used during the session are returned for other dial-in uses.

This set of features is supported on all platforms that support Multilink PPP.

Redirect-Number Support for RADIUS and TACACS+ Servers

The telco-return RADIUS server has been enhanced to provide additional authentication information, allowing an administrator to determine whether a subscriber dialed a number that requires special billing arrangements (such as a toll-free number). If a telco return customer is being authenticated by a TACACS+ or RADIUS server, and if the number dialed by the cable modem is being redirected to another number for authentication, the system can include the original number in the information sent to the authentication server. The original number can be sent as a Cisco vendor-specific attribute (VSA) for TACACS+ servers and as RADIUS Attribute 93 (Ascend-Redirect-Number) for RADIUS servers.

For additional information, refer to the following document on Cisco.com:

- "Telco Return for the Cisco Cable Modem Termination System" chapter in the *Cisco Cable Modem Termination System Feature Guide*

  http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/cmtsfg.html

Reflexive Access Lists

Reflexive access lists allow IP packets to be filtered based on upper-layer session information. You can use reflexive access lists to permit IP traffic for sessions originating from within your network but to deny IP traffic for sessions originating from outside your network. This is accomplished by reflexive filtering, a kind of session filtering.

Reflexive access lists can be defined with extended named IP access lists only. You cannot define reflexive access lists with numbered or standard named IP access lists or with other protocol access lists.You can use reflexive access lists in conjunction with other standard access lists and static extended access lists.

Reflexive access lists are an important part of securing your network against network hackers, and can be included in a firewall defense. Reflexive access lists provide a level of security against spoofing and certain denial-of-service attacks. Reflexive access lists are simple to use, and, compared to basic access lists, provide greater control over which packets enter your network.

For additional information, refer to the following document on Cisco.com:

- *Configuring IP Session Filtering (Reflexive Access Lists)*

  http://www.cisco.com/en/US/docs/ios/12_2/security/configuration/guide/scfreflx.html

Secure Shell (SSH) Supported in "k1" Images for Cisco uBR7200

In Cisco IOS Release 12.1 T, the definition of "k1" images for Cisco uBR924 cable access routers was changed from support for BPI only, to also include support for Secure Shell (SSH). This change caused an inconsistency with Cisco uBR7200 series images, since the definition of "k1" for the Cisco uBR7200 was not changed and did not include SSH.

Cisco uBR7200 series universal broadband routers support the Cisco IOS Firewall feature. This feature set offers Network Address Translation (NAT) and is designed to prevent unauthorized, external access to your internal network, blocking attacks on your network, while still allowing authorized users to access network resources. This feature is described in detail in the *Cisco IOS Firewall* web page on Cisco.com.

Turbo Access Control Lists

The Turbo Access Control List (ACL) feature processes access lists more expediently, providing faster functionality for routers equipped with the feature. ACLs are normally searched sequentially to find a matching rule, and ACLs are ordered specifically to take this factor into account. Because of the increasing needs and requirements for security filtering and packet classification, ACLs can expand to the point that searching the ACL adds a significant amount of time and memory when packets are being forwarded. Moreover, the time taken by the router to search the list is not always consistent, adding a variable latency to the packet forwarding. A high CPU load is necessary for searching an ACL with several entries.

The Turbo ACL feature compiles the ACLs into a set of lookup tables, while maintaining the first match requirements. Packet headers are used to access these tables in a small, fixed number of lookups, independently of the existing number of ACL entries. The benefits of this feature include:

- For ACLs larger than 3 entries, the CPU load required to match the packet to the pre-determined packet-matching rule is lessened. The CPU load is fixed, regardless of the size of the ACL, allowing for larger ACLs without incurring any CPU overhead penalties. The larger the ACL, the greater the benefit.

- The time taken to match the packet is fixed, so that latency of the packets are smaller (significantly in the case of large ACLs) and more importantly, consistent, allowing better network stability and more accurate transit times.

For additional feature and configuration information, refer to the following document on Cisco.com:

- "Enabling Turbo Access Control Lists" topic of the "IP Addressing and Services" section of the *Cisco IOS IP Configuration Guide*, Release 12.2

  http://www.cisco.com/en/US/docs/ios/12_2/ip/configuration/guide/1cfip.html

Vendor-Proprietary RADIUS Attributes

Remote Authentication Dial-In User Service (RADIUS) attributes are used to define specific authentication, authorization, and accounting elements in a user profile, which is stored on the RADIUS daemon. Cisco supports a variety of vendor-proprietary RADIUS attributes. For additional information, refer to the appendix "Radius Attributes" in the *Cisco IOS Security Configuration Guide*, Release 12.2 on Cisco.com:

http://www.cisco.com/en/US/docs/ios/12_2/security/configuration/guide/fsecur_c.html

SNMP Features and Enhancements

Multiple Cisco IOS releases that support the Cisco uBR7200 Series include enhanced Simple Network Management Protocol (SNMP) features:

Individual SNMP Trap Support

The Individual SNMP Trap Support feature adds the ability to enable or disable SNMP system management notifications (traps) individually. SNMP traps that can be specified are "authentication", "linkup", "linkdown", and "coldstart." This feature expands the functionality of the **snmp-server enable traps** command.

Note When the **snmp-server enable traps** command is given without any options, it enables all traps, which can generate a significant number of traps at key events, such as system power-up. If the SNMP queue is not large enough to handle all of the traps, new traps will be dropped without notification until the existing traps are sent and slots become available in the queue.

You can do two things to avoid dropping traps in this situation:

- Increase the SNMP trap queue size. The default queue size is 10, which is insufficient to handle all traps. Use the snmp-server queue-length length global configuration command to increase the queue size. The length parameter can range from 10 to 1000. Increase the queue size until traps are no longer dropped.
- Disable unneeded SNMP traps. For example, if you do not need SYSLOG traps (which are sent for every message displayed on the console), disable those traps as follows:

```
Router(config)# snmp-server enable traps
Router(config)# no snmp-server enable traps syslog
```

For additional feature information, refer to the following document on Cisco.com:

- *Individual SNMP Trap Support*

  http://www.cisco.com/en/US/docs/ios/12_1t/12_1t3/feature/guide/dtitraps.html

LinkUp/Down Traps Support (RFC 2233)

The objects in the varbind list, based on the Internet Engineering Task Force (IETF) standard, are defined in IF-MIB. Since IF-MIB supports subinterfaces, all objects in this varbind list are also supported for subinterfaces. The feature allows you to base the Link Up/Down trap varbind list on a Cisco-specific or IETF standard with a new CLI configuration command.

To enable linkUp/linkDown Simple Network Management Protocol (SNMP) traps which are compliant with RFC2233, use the **snmp-server trap link** command in global configuration mode. To disable IETF compliant functionality and revert to the default Cisco implementation of linkUp/linkDown traps, use the **no** form of this command.

snmp-server link-trap [cisco | ietf]

no snmp-server link-trap [cisco | ietf]

Syntax Description

cisco	The default is a Cisco-specific link trap (**snmp-server link-trap cisco**). The user can switch between Cisco and IETF standard.
ietf	This keyword links functionality of SNMP linkUp/linkDown traps to the Internet Engineering Task Force (IETF) standard (as opposed to the previous Cisco implementation).

SNMPv2C

SNMPv2 defines several new macros. The following macros identify a MIB as an SNMPv2 MIB:

- MODULE-IDENTITY
- MODULE-COMPLIANCE
- OBJECT-GROUP
- NOTIFICATION-TYPE TEXTUAL-CONVENTION

For additional information about SNMPv2C, refer to the document titled *http://www.cisco.com/cisco/web/psa/default.html?mode=prod* on Cisco.com.

SNMPv3

SNMPv3 is an interoperable standards-based protocol for network management. SNMPv3 provides secure access to devices by a combination of authenticating and encrypting packets over the network. The security features provided in SNMPv3 are:

- Message integrity—Ensures that a packet has not been tampered with in-transit.
- Authentication—Determines the message is from a valid source.
- Encryption—Scrambling the contents of a packet prevents it from being seen by an unauthorized source.

SNMPv3 provides for both security models and security levels. A security model is an authentication strategy that is set up for a user and the group in which the user resides. A security level is the permitted level of security within a security model. A combination of a security model and a security level will determine which security mechanism is employed when handling an SNMP packet.

For additional information about SNMPv3, refer to the document titled *SNMPv3* feature summary on Cisco.com.

SNMP Cable Modem Remote Query

Configuring Remote Modem Monitoring

To specify how often SNMP polls the modem, and to configure access, use the **cable modem remote-query** command in global configuration mode. To disable the gathering of cable modem statistics, use the **no** form of this command.

cable modem remote-query *polling-interval community-string*

no cable modem remote-query

Syntax Description

polling-interval	Specifies how often the CMTS polls for cable modem statistics. Valid range is from 1 to 86,400 seconds.
community-string	Defines the Simple Network Management Protocol (SNMP) community string.

Verifying Remote Query Information

To display information from a queried modem, enter the **show cable modem remote-query** command in global configuration mode.

Troubleshooting Tips

To display debugging information, use the **debug cable remote-query** command in global configuration mode.

For additional configuration and feature information, refer to *Modem Status Enhancements for the Cisco uBR7200 Series Cable Router* on Cisco.com.

SNMP Management Information Base (MIB) Enhancements

Obtaining Current Management Information Bases

To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, refer to the *Cisco MIB* web page on Cisco.com. For additional information, refer to the *Cisco uBR7200 Series Software Release Notes* on Cisco.com:

http://www.cisco.com/en/US/docs/ios/12_1/12_1ec/release/notes/72_121ec.html

Categories of Supported Management Information Bases

The Cisco uBR7200 series universal broadband routers support the following categories of MIBs:

- SNMP standard MIBs—These MIBs are required by any agent supporting SNMPv1 or SNMPv2 network management.
- Cisco's platform and network-layer enterprise MIBs—Common across most of Cisco's router platforms. If your network management applications are already configured to support other Cisco routers, such as the 2600 series or 7200 series, no further configuration is needed unless the version of Cisco IOS software being used has updated these MIBs.
- Cable-specific MIBs—Provide information about the cable interfaces and related information on the uBR7200 series routers. They include both DOCSIS-specific MIBs and Cisco-specific enterprise MIBs. If your network management applications have not already been configured for the uBR7200 series routers, these MIBs must be loaded.
- Deprecated MIBs—Supported in earlier releases of Cisco IOS software but have been replaced by more standardized, scalable MIBs. Network Management applications and scripts should convert to the replacement MIBs as soon as possible.

The cable-specific MIBs are described in the following section. For information on the SNMP standard MIBs and Cisco's platform and network-layer enterprise MIBs, see the *Cisco MIB* web page on Cisco.com.

SNMP and Cable-Specific MIBs

Table 1-14 shows the SNMP and cable-specific MIBs that are supported on the Cisco uBR7200 series universal broadband routers. The table provides a brief description of each MIB's contents and the Cisco IOS software release in which the MIB was initially functional—earlier releases might have had unsupported prototype versions of the MIB; later releases might have added new attributes and functionality. Because of interdependencies, the MIBs must be loaded in the order shown in the table.

Note The names given in Table 1-14 are the filenames for the MIBs as they exist on Cisco's FTP site (http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml). Most MIBs are available in both SNMPv1 and SNMPv2 versions; the SNMPv1 versions have *V1SMI* as part of their filenames.

Note MIB files from the Cisco IOS 12.0 SC release train that are no longer supported in the subsequent 12.1 EC, 12.2 XF, or 12.2 BC release trains are not listed in the table below.

Table 1-14 SNMP and Cable-Specific MIBs Supported on Cisco uBR7200 Series Routers

MIB Filename	Description	Introduced in Releases
SNMPv2-SMI.my	This module specifies the Structure of Management Information (SMI) for SNMPv2, as defined in RFC 1902.	12.0(6)SC 12.1(2)EC 12.2(4)XF1 (12.2 BC[1])
SNMPv2-TC.my	This module defines the textual conventions as specified in RFC 1903.	12.0(6)SC 12.1(2)EC 12.2(4)XF1 (12.2 BC)
SNMPv2-MIB.my	The management protocol, SNMPv2, provides for the exchange of messages that convey management information between the agents and the management stations, as defined in RFC 1907.	12.0(6)SC 12.1(2)EC 12.2(4)XF1 12.2 BC

Table 1-14 SNMP and Cable-Specific MIBs Supported on Cisco uBR7200 Series Routers

MIB Filename	Description	Introduced in Releases
CISCO-SMI.my CISCO-SMI-V1SMI.my	This module specifies the SMI for Cisco's enterprise MIBs.	12.0(6)SC 12.1(2)EC 12.2(4)XF1 (12.2 BC)
CISCO-TC.my CISCO-TC-V1SMI.my	This module defines the textual conventions used in Cisco's enterprise MIBs.	12.0(6)SC 12.1(2)EC 12.2(4)XF1 (12.2 BC)
IF-MIB.my IF-MIB-V1SMI.my	This module describes generic objects for the Layer 3 network interface sublayers. This MIB is an updated version of MIB-II's *if* table and incorporates the extensions defined in RFC 2233.	12.1(2)EC 12.2(4)XF1 (12.2 BC)
DOCS-IF-MIB.my DOCS-IF-MIB-V1SMI.my	This module describes the DOCSIS-compliant Radio Frequency (RF) interfaces in cable modems (CMs) and the CMTS, as defined in RFC 2670.	12.1(2)EC 12.2(4)XF1 (12.2 BC)
DOCS-BPI-MIB.my	This module—available in an SNMPv2 version only—describes the attributes for the DOCSIS-specified Baseline Privacy Interface (BPI) on CMs and the CMTS.	12.1(2)EC 12.2(4)XF1 (12.2 BC)
CISCO-DOCS-EXT-MIB.my CISCO-DOCS-EXT-MIB-V1SMI.my	This module extends the DOCSIS standard RFI MIB (DOCS-IF-MIB) with Cisco-specific extensions, such as QoS attributes and connection status and other information regarding the CMs and CPE devices supported by the CMTS.	12.1(2)EC 12.2(4)XF1 (12.2 BC)
CISCO-DOCS-REMOTE-QUERY-MIB.my	This module facilitates SNMP polling of remote CMs on a CMTS.	12.1(2)EC 12.2(4)XF1 (12.2 BC)
CISCO-CABLE-SPECTRUM-MIB.my CISCO-CABLE-SPECTRUM-MIB-V1SMI.my	This module describes the spectrum management flap list attributes.	12.1(2)EC 12.2(4)XF1 (12.2 BC)

1. The Cisco IOS 12.2 BC release train continues the MIBs and most features introduced in the Cisco IOS 12.2 XF release train.

Circuit Interface Identification MIB

The Circuit Interface Identification MIB feature adds support for a new Cisco enterprise MIB, used to assist in SNMP monitoring of circuit-based interfaces. The Circuit Interface MIB (CISCO-CIRCUIT-INTERFACE-MIB) provides a MIB object that can be used to identify individual circuit-based interfaces (for example, interfaces using ATM or Frame Relay). This user-specified identification will then be returned when linkup and linkdown SNMP traps are generated for the interface.

The Circuit Interface MIB consists of a single table, with each row being a sequence of two objects: Circuit Interface Description (cciDescr) and Circuit Interface Status (cciStatus). The "cciDescr" object is used to identify circuits using a textual description of up to 255 characters specified by the user (note that MIB objects are modified using network management system [NMS] applications, and can not be configured using the Cisco IOS command-line interface).

When the row is created by a user, a value is set for the cciDescr object. The table is indexed by "ifIndex" from the IF-MIB. The "cciStatus" is the "RowStatus" object for the rows in the table. The "cciStatus" object can be set to only two values by the user: "createAndGo(4)", which creates a new row, and "destroy(6)", which removes an existing row. If the row is created successfully, the "cciStatus" will be active(1). When creating a new row, the user should set the "cciDescr" object along with the "cciStatus" in a single **snmp set pdu** command. If the row is already active, only the "cciDescr" object can be modified.

The other option is to delete the row first by setting the "cciStatus" to "destroy(6)" and then recreate the row with a new value for "cciDescr". When creating a new row, the "ifIndex" is validated first. If the "ifIndex" value is not valid, the row is not created and an error code is returned. Similarly, when an interface is deleted and there was a corresponding row in this table, that row will be deleted automatically.

After an identifying description is created for an interface by a user, the description (the "cciDescr" object) will be sent along with the other varbinds as part of linkup and linkdown trap notifications.

For further details, see the CISCO-CIRCUIT-INTERFACE-MIB.my file, available at ftp://ftp.cisco.com/pub/mibs/v2/CISCO-CIRCUIT-INTERFACE-MIB.my.

cdxCmtsCmOnOffTrapEnable SNMP Object

The following new CLI commands are supported for the "cdxCmtsCmOnOffTrapEnable" object:

[**no**] **cable enable-trap cmonoff-notification**

[**no**] **cable enable-trap cmonoff-interval** <*time 0 to 86400*>

These commands have the following default settings:

no cable enable-trap cmonoff-notification

no cable enable-trap cmonoff-interval

After the default setting has been changed and the new configuration has been saved, the new configuration will remain active after the CMTS reloads.

Examples

cable enable-trap cmonoff-notification	This command enables "cdxCmtsCmOnOffNotification" in the RF MAC interface. Alternatively, you can set the SNMP object "cdxCmtsCmOnOffTrapEnable" to true (1).
no cable enable-trap cmonoff-notification	This command disables "cdxCmtsCmOnOffNotification" in the RF MAC interface. Alternatively, you can set the SNMP object "cdxCmtsCmOnOffTrapEnable" to false (2).
cable enable-trap cmonoff-interval <*time 0 to 86400*>	This command sets the interval for "cdxCmtsCmOnOffNotification" sent by the CMTS for one online/offline cable modem state change when "cdxCmtsCmOnOffTrapEnable" is set to true (1). Alternatively, you can set the SNMP object "cdxCmtsCmOnOffTrapInterval" to the same time value.
no cable enable-trap cmonoff-interval	This command sets the interval "cdxCmtsCmOnOffNotification" to 0 so that "cdxCmtsCmOnOffNotification" will be sent for every online/offline cable modem state change when "cdxCmtsCmOnOffTrapEnable" is set to true (1). Alternatively, you can set the SNMP object "cdxCmtsCmOnOffTrapInterval" to 0.

Note The default for "cdxCmtsCmOnOffTrapInterval" is 0.

DOCSIS Ethernet MIB Objects Support (RFC 2665)

For a complete list of MIBs supported by the Cisco uBR7200 Series, refer to the *Cisco uBR7200 Series Software Release Notes* on Cisco.com:

http://www.cisco.com/en/US/docs/ios/12_1/12_1ec/release/notes/72_121ec.html

For descriptions of supported MIBs and how to use MIBs, refer to the *Cisco MIBs* web page on Cisco.com.

DOCSIS OSSI Objects Support (RFC 2233)

Cisco uBR7200 series routers now support the required objects in RFC 2233 for DOCSIS Operations Support System Interface (OSSI) compliance.

- IF-MIB.my is updated to match RFC 2233.
- The following new object is now supported:
  - ifCounterDiscontinuityTime

For a complete list of MIBs supported by the Cisco uBR7200 Series, refer to the *Cisco uBR7200 Series Software Release Notes* on Cisco.com:

http://www.cisco.com/en/US/docs/ios/12_1/12_1ec/release/notes/72_121ec.html

For descriptions of supported MIBs and how to use MIBs, refer to the *Cisco MIBs* web page on Cisco.com.

Expression MIB Support of Delta, Wildcarding, and Aggregation

This feature adds support of the Delta, Wildcarding, Delta Wildcarding, and Aggregation features in the Distributed Management Expression MIB (EXPRESSION-MIB) to Cisco IOS software for use by SNMP.

The Delta function enables the Expression MIB to use Delta values of an object instead of absolute values when evaluating an expression. Delta is obtained by taking the difference between the current value of an object and its previous value.

The Wildcarding function of the Expression MIB allows evaluation of multiple instances of an object. This is useful in cases where an expression needs to be applied to all instances of an object. The user need not individually specify all instances of an object in the Expression but only has to set the "expWildcardedObject" in "expObjectTable" to TRUE for the respective object.

Aggregation is performed using the sum function in the Expression MIB. The operand to the sum function has to be a wildcard object. The result of the sum function is the sum of values of all instances of the wildcard object.

For a complete description of Expression MIB functionality, see the *Distributed Management Expression MIB,* Internet-Draft, available through the ITEF at http://www.ietf.org/ids.by.wg/disman.html.

Cisco Call History MIB Command Line Interface

For a complete list of MIBs supported by the Cisco uBR7200 Series, refer to the *Cisco uBR7200 Series Software Release Notes* on Cisco.com:

http://www.cisco.com/en/US/docs/ios/12_2/12_2b/12_2bc/release/notes/u7208bc1.html

For further descriptions of supported MIBs and how to use MIBs, refer to the *Cisco MIBs* web page.

RF Interface MIB

For a complete list of MIBs supported by the Cisco uBR7200 Series, refer to the refer to the *Cisco uBR7200 Series Software Release Notes* on Cisco.com:

http://www.cisco.com/en/US/docs/ios/12_2/12_2b/12_2bc/release/notes/u7208bc1.html

For descriptions of supported MIBs and how to use MIBs, refer to the *Cisco MIBs* web page on Cisco.com.

Multicast Source Discovery Protocol (SDP) MIB

The Multicast Source Discovery Protocol (MSDP) MIB feature adds support in Cisco IOS software for the MSDP MIB. This MIB describes objects used for managing MSDP operations using Simple Network Management Protocol (SNMP). Documentation for this MIB exists in the form of an Internet Draft titled "Multicast Source Discovery Protocol MIB" (draft-ietf-msdp-mib-03.txt) and is available through the Internet Engineering Task Force (IETF) at http://www.ietf.org. For additional information, refer to the *MSDP MIB* feature module on Cisco.com.

Network Time Protocol (NTP) MIB

The Network Time Protocol (NTP) is used to synchronize timekeeping among a set of distributed time servers and clients. The Cisco NTP MIB enables users to remotely monitor an NTP server using the Simple Network Management Protocol (SNMP), provided the MIB itself is implemented on that server. Use of the NTP MIB to monitor the NTP status of routing devices is accomplished using software on a network management system (NMS). There are no new or modified Cisco IOS software commands associated with this feature.

The Cisco implementation of the NTP MIB is based on NTP version 3 (RFC-1305). The MIB objects are all read-only. SNMP requests are processed by reading the corresponding variables from the NTP subsystem and returning them in the response. The NTP MIB defines a set of NTP server system objects, including an NTP server peers table and an NTP server filter register table.

For complete details on the Cisco implementation of the NTP MIB, refer to the MIB file itself at ftp://ftp.cisco.com/pub/mibs/v2/CISCO-NTP-MIB.my.

SNMP Enhancements to CISCO-DOCS-EXT-MIB

Commencing with Cisco IOS Release 12.2(4)BC1, the following attributes have been added to CISCO-DOCS-EXT-MIB to provide information about the Unsolicited Grant Service (UGS) allocation on the upstream interfaces:

- "cdxIfUpChannelNumActiveUGS" returns the number of active UGS flows currently allocated on the upstream.
- "cdxIfUpChannelMaxUGSInLastOneHour" returns the maximum number of UGS flows allocated on the upstream in the last hour.
- "cdxIfUpChannelMinUGSInLastOneHour" returns the minimum number of UGS flows allocated on the upstream in the last hour.
- "cdxIfUpChannelAvgUGSInLastOneHour" returns the average number of UGS flows allocated on the upstream in the last hour.
- "cdxIfUpChannelMaxUGSInLastFiveMins" returns the maximum number of UGS flows allocated on the upstream in the last five minutes.
- "cdxIfUpChannelMinUGSInLastFiveMins" returns the minimum number of UGS flows allocated on the upstream in the last five minutes.
- "cdxIfUpChannelAvgUGSInLastFiveMins" returns the average number of UGS flows allocated on the upstream in the last five minutes.

For a complete list of MIBs supported by the Cisco uBR7200 Series, refer to the *Cisco uBR7200 Series Software Release Notes* on Cisco.com:

http://www.cisco.com/en/US/docs/ios/12_2/12_2b/12_2bc/release/notes/u7208bc1.html

For descriptions of supported MIBs and how to use MIBs, refer to the *Cisco MIBs* web page on Cisco.com.

SNMP Objects for Clear Host, Clear Cable Modem, and Show Current CPEs

Host or cable modems can be cleared using the "cdxCmCpeResetNow" MIB object. The number of current CPEs can be displayed using the "cdxCmtsCmCurrCpeNumber" MIB object.

SNMP MIBs Changes and Updates in Cisco IOS Release 12.3(9a)BC

Cisco IOS Release 12.3(9a)BC adds the following new MIB support for the Cisco uBR7246VXR router.

- CISCO-CABLE-QOS-MONITOR MIB
- CISCO-CABLE-SPECTRUM-MIB
- CISCO-PROCESS-MIB
- DOCS-IF-MIB
- DOCS-QOS-MIB
- DSG-IF-MIB

For additional information about MIBs for the Cisco CMTS, refer to the following resources on Cisco.com:

- *Cisco CMTS Universal Broadband Router MIB Specifications Guide*
  http://www.cisco.com/en/US/docs/cable/cmts/mib/reference/guide/ubrmibv5.html
- *SNMP Object Navigator*
  http://www.cisco.com/pcgi-bin/Support/Mibbrowser/unity.pl

CISCO-CABLE-QOS-MONITOR MIB

Cisco IOS Release 12.3(9a)BC introduces additional features for the CISCO-CABLE-QOS-MONITOR MIB, including the following:

- Clarified the descriptions of a number of objects.
- Added a number of objects in the ccqmCmtsEnforceRuleTable to support DOCSIS 1.1 and DOCSIS 2.0 cable modems and to support peak and off-peak monitoring.
- Added the ccqmCmtsIfBwUtilTable to provide thresholds for downstream/upstream bandwidth utilization.
- Deprecated and removed ccqmCmtsEnfRuleByteCount.

CISCO-CABLE-SPECTRUM-MIB

Cisco IOS Release 12.3(9) introduces support for the CISCO-CABLE-SPECTRUM-MIB on the Cisco uBR7246VXR universal broadband router, with these additional MIB object enhancements:

- ccsFlapListMaxSize and ccsFlapListCurrentSize SNMP objects provide additional description for cable flap lists.
- Added the ccsCmFlapTable to replace the ccsFlapTable. The new object uses `downstream`, `upstream` and `Mac` as indices to replace the ccsFlapTable object.
- The enhanced ccsSNRRequestTable object provides a table of SNR requests with modified description.
- Added the ccsUpSpecMgmtUpperBoundFreq object to assist with spectrum management on the Cisco CMTS.
- Added the ccsCompliance5 object object.

- Added ccsCmFlapResetNow to reset the flap list for a particular cable modem.
- Updated the descriptions for ccsFlapListMaxSize, ccsFlapListCurrentSize, and ccsSNRRequestTable.

The following objects are also now deprecated:

- ccsFlapPowerAdjustThreshold
- ccsFlapMissThreshold
- ccsFlapResetAll
- ccsFlapClearAll
- ccsFlapLastClearTime

The maximum number of entries in the flap-list was changed from a maximum of 8191 for the entire router, to the following:

- 8191 entries for each Broadband Processing Engine (BPE) cable interface, such as the Cisco uBR-MC16U/X, Cisco uBR-MC28U/X, and Cisco uBR-MC5X20S/U.
- 8191 maximum flap-list entries for all non-BPE cable interfaces, such as the Cisco uBR-MC16C, Cisco uBR-MC16S, and Cisco uBR-MC28C.

Two objects are now used to track the flap list size:

- ccsFlapListMaxSize—Reflects the flap list size, as configured by the **cable flap-list size** command.
- ccsFlapListCurrentSize—Reflects the current size of the flap list for each MAC domain (downstream).

CISCO-PROCESS-MIB

The CISCO-PROCESS-MIB enables you to monitor CPU and memory utilization for RF cards, cable interface line cards and broadband processing engines on the Cisco CMTS. This information is collected via SNMP.

DOCS-IF-MIB

The DOCS-IF-MIB (released as RFC 2670) has been updated to conform to the version 5 of the DOCSIS 2.0 RF MIB Specification (draft-ietf-ipcdn-docs-rfmibv2-05.txt).

DOCS-QOS-MIB

Cisco IOS Release 12.3(9) introduces additional MIB object enhancements for the DOCS-QOS-MIB on the Cisco uBR7246VXR and Cisco uBR10012 universal broadband routers:

- Updated with the DOCSIS operations support system interface (OSSI) v2.0-N-04.0139-2.
- The default values of docsQosPktClassIpSourceMask and docsQosPktClassIpDestMask objects are set to 0xFFFFFFFF.

DSG-IF-MIB

The DSG-IF-MIB defines objects that are used to configure, control, and monitor the operation of the DOCSIS Set-top Gateway (DSG) 1.0 feature on Cisco uBR7200 Series and Cisco uBR10012 routers.

Note The MODULE-IDENTITY for the DSG-IF-MIB is dsgIfMib, and its top-level OID is 1.3.6.1.4.1.9.9.999 (iso.org.dod.internet.private.enterprises.cisco.ciscoMgmt.dsgIfMib). Because this is an experimental MIB, its top-level OID is expected to change when the DSG specifications are finalized.

MIB Constraints

The DSG-IF-MIB has the following constraints:

- This is an experimental MIB that can be obsoleted and replaced without prior notice, when the DSG specification is finalized.
- This MIB is supported only in Cisco IOS Release 12.3(9a)BC and later releases. It is not supported for the version of DSG that was implemented in Cisco IOS Release 12.2(15)BC1.
- This MIB is not supported in Cisco IOS Release 12.1 EC.
- This MIB is not supported on Cisco uBR7100 routers.

SNMP Warm Start Trap

When two Cisco uBR7200 series routers are configured for failover and the active unit fails, the standby unit takes over and becomes the active unit. Whenever this occurs, a Failover Switchover SNMP trap is generated and appears to the SNMP server as a "Warm Start" trap.

Note When a Cisco uBR7200 series router is powered up, an SNMP trap is generated and appears to the SNMP server as a "Cold Start" trap. This functionality is already supported in all Cisco IOS 12.1 EC releases.

Spectrum Management and Advanced Spectrum Management Features

Spectrum management features, including dynamic upstream modulation were introduced in Cisco IOS Release 12.2(4)XF1, and these continue in the Cisco 12.2 BC release train. These and other features relating to spectrum management are described below:

The Cisco uBR7200 Series line cards support varying options that allow service providers to specify different rules the system uses when encountering noise on the cable plant. The primary problem with the upstream system is the ingress of noise, both long-term interference from RF sources such as CB and commercial services, and degradation of the HFC plant. There is also short term sources of noise such as electric appliances or switches that appear a finite number of times for a typical duration of 1 microsecond in length and then go away. These various noise sources affect the Bit Error Rate of the upstream data, and can impact the reliability of two-way services on the plant.

Advanced Spectrum Management

In addition to other features, Cisco offers advanced spectrum management features for optimal selection of the hop-to frequency (optimal frequency hopping) with the advent of the Cisco uBR-MC16S spectrum management card. The Cisco uBR-MC16S features advanced spectrum management capability that records signal-to-noise (SNR) information from 5-to-42 MHz for each upstream port for the purpose of determining noise level, and to identify potential clear spectrum in the event of the need to initiate a frequency hop. When the number of missed station management messages exceeds a configured threshold, an upstream channel frequency reassignment is initiated. The Cisco uBR-MC16S scans the upstream spectrum and locates a clean, available upstream channel within the defined spectrum group.

Note Clean band is defined as > 29 db SNR for 16 Quadrature Amplitude Modulation (QAM), and > 19 db SNR for Quadrature Phase Shift Keying (QPSK). The SNR calculation is based on the signal power level, noise power level over the desired bandwidth.

If you choose to bypass the existing Cisco uBR-MC16S optimal frequency hopping capability designed to optimize the look-ahead capability of the Digital Signal Processors (DSPs), it is possible enforce guided hopping as used on the Cisco uBR-MCxC and Cisco uBR-MC16E line cards. Cisco does not recommend that you disable the optimal frequency hopping feature of the Cisco uBR-MC16S for normal operations.

In addition to optimal frequency hopping, the Cisco uBR-MC16S can dynamically vary upstream channel widths. By entering an optional second channel width value per upstream port, you can instruct the Cisco uBR-MC16S to hierarchically search for clean upstream channels of 3.2 MHz, 1.6 MHz, 800 kHz, 400 kHz, and 200 kHz width.

For additional information about spectrum management features and their configuration, refer to the chapter titled "Spectrum Management for the Cisco Cable Modem Termination System" in the *Cisco Cable Modem Termination System Feature Guide* on Cisco.com.

Cable Modulation Profile Default Templates

The cable modulation-profile global configuration command has been enhanced with three new options that provide the ability to quickly create basic modulation profiles using the default values for each burst type. The syntax for the new options is:

cable modulation-profile *profile* [**mix** | **qam-16** | **qpsk**]

Syntax Description

profile	Specifies the modulation profile number (1-8).
mix	Creates a default QPSK/16-QAM mix modulation profile where short and long grant bursts are sent using 16-QAM, while request, request data, initial ranging, and station maintenance bursts are sent using QPSK). The burst parameters are set to their default values for each burst type.
qam-16	Creates a default 16-QAM modulation profile, where all bursts are sent using 16-QAM. The burst parameters are set to their default values for each burst type.
qpsk	Creates a default QPSK modulation profile, where all bursts are sent using QPSK. The burst parameters are set to their default values for each burst type.

Downstream Traffic Shaping

Downstream traffic shaping (to include Type-of-Service) allows traffic shaping from the CMTS on a DOCSIS downstream channel. Downstream traffic shaping limits surges on output interfaces to reduce downstream congestion or to conform to traffic contract parameters such as PCR.

For additional information about downstream traffic shaping, refer to the following resources:

- "Setting Downstream Traffic Shaping" section on page 3-10
- The "Spectrum Management for the Cisco Cable Modem Termination System" chapter in the *Cisco Cable Modem Termination System Feature Guide* on Cisco.com:

  http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/cmtsfg.html

Dynamic Upstream Modulation

The Dynamic Upstream Modulation feature reduces the risks associated with making transition to Quadrature Amplitude Modulation (QAM)-16 in the return path, and provides assurance that subscribers remain online and connected during periods of return-path impairments.

This feature actively monitors the signal-to-noise-ratio (SNR) and forward error correction (FEC) counters in the active return path of each upstream port. The software tracks whether the current upstream channel signal quality can adequately support the higher modulation scheme configured, and adjusts in proactive fashion to the more robust quadrature phase-shift keying (QPSK) modulation scheme when necessary. When return-path spectrum conditions improve, the software returns the upstream channel to the higher-modulation QAM scheme. This is done through modulation profiles supported in Cisco IOS, which can be configured in a variety of ways to support the unique environment at each user's facility.

You can configure Dynamic Upstream Modulation on interfaces with fixed upstream frequencies or on interfaces with spectrum groups assigned. Cisco IOS provides one preconfigured modulation profile resident in memory, which defines a typical profile for QPSK modulation. In order to use the Dynamic Upstream Modulation feature, a second profile must be created that is unique from the first profile and typically provides a higher modulation scheme. The upstream port must be assigned this second modulation profile.

Use the **cable upstream modulation-profile** command in cable interface configuration mode to configure Dynamic Upstream Modulation:

```
Router(config)# cable modulation-profile 2 mix
```

Use the **cable upstream modulation-profile** command in cable interface configuration mode to assign the modulation profile to an upstream port:

cable upstream *n* **modulation-profile** <*primary profile-number*> <*secondary profile-number*>

For more information, refer to the *Cisco uBR7200 Dynamic Upstream Modulation* feature module on Cisco.com.

Guided and Scheduled Spectrum Management

Cisco's initial response to combat upstream ingress was to add frequency agility through software support on the Cisco uBR-MCxxC DOCSIS line cards. Operators configured spectrum groups to select the new upstream frequency based on scheduled frequency hopping or based on guided frequency hopping. Using time scheduled spectrum management, the upstream channel frequency reassignment process is initiated at a configured time of day or week. Using guided frequency hopping, the number of missed station management messages from the cable modems or set top boxes on that upstream exceeding a configured threshold initiates an upstream channel frequency reassignment. All cable modems on the upstream port migrate to the next frequency, using a round robin scheme to select the next available frequency band, with an assigned input power level defined in the spectrum management group. The frequency change occurs rapidly without data loss and minimal latency.

Input Power Levels

The input power level, power-level-dBmV, is an option in the **cable spectrum-group** command. The option allows you to specify the expected U.S. input power levels on the upstream receivers on the CMTS when the cable modems are hopping from one fixed frequency to another or from one band to another. Each upstream frequency has an associated upstream input power level in dBmV. The power level is the modem transmit power that each spectrum group can use when an upstream frequency change is necessary. The input power level may be set at the time of the frequency hop.

Specifying an input power level is done so that the cable modems do not have to increase or decrease their transmit power with every hop. The cable operator can perform minor power equalizations as a function of frequency. The valid range is -10 to +10dBmV. The power level value should be changed only if you want to change the power level as part of spectrum management. Some cable plants may want to change only the input power level and not the frequency on a daily time schedule.

For information on how to configure input power levels, see the "Setting Input Power Level" section in the *Cisco Cable Modem Termination System Feature Guide* on Cisco.com.

Spectrum Management Enhancements in Cisco IOS Release 12.3(9a)BC

Cisco IOS Release 12.3(9a)BC introduces enhancements to spectrum management for the Cisco uBR7246VXR router:

- Supports the Cisco Broadband Troubleshooter (CBT) 3.2, page 1-123 (with caveats)
- Supports Subscriber Traffic Management (STM) Version 1.1, page 1-95 (with caveats)

For additional information about CBT 3.2, spectrum management and STM 1.1, refer to the following documents on Cisco.com:

- *Release Notes for Cisco Broadband Troubleshooter Release 3.2*

  http://www.cisco.com/en/US/products/sw/netmgtsw/ps530/prod_release_notes_list.html
- *Spectrum Management for the Cisco CMTS*

  http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/ufg_spec.html
- *Subscriber Traffic Management for the Cisco CMTS*

  https://www.cisco.com/en/US/docs/cable/cmts/feature/ubsubmon.html

Upstream Traffic Shaping

This feature allows the cable modem termination system (CMTS) to perform upstream rate shaping on the DOCSIS (Data-Over-Cable Service Interface Specifications) upstream channel.

With traffic shaping, the CMTS can buffer the grants for rate exceeded modems. This grant buffering at the CMTS avoids TCP-related timeouts and retransmits resulting in an improved TCP throughput performance for the rate-exceeded modems. Thus, shaping enables the CMTS to enforce the peak upstream rate for the modem without degrading overall TCP performance for the modem.

When users do not enable the shaping option for upstream rate limiting, the CMTS upstream-rate-policing code drops bandwidth requests from CMs that are found to have exceeded their configured-peak-upstream rate (using different local drop policies). The effect of bandwidth requests (eventually upstream packets) being dropped causes degraded throughput performance of window-based protocols (like TCP) for these rate-exceeded modems because of the timeouts and retransmits that follow.

For additional information about upstream traffic shaping, refer to the "Setting Upstream Traffic Shaping" section on page 3-26 and to *Spectrum Management for the Cisco Cable Modem Termination System* on Cisco.com.

Testing, Troubleshooting and Diagnostic Features

The Cisco uBR7200 Series supports several troubleshooting and diagnostic features:

Cable Downstream Frequency Override

Support for the **cable downstream override** command was introduced for the Cisco uBR7200 series routers in the Cisco IOS 12.0 SC, 12.1 EC, and 12.1T release trains.

This command is never needed for normal operations, because downstream frequency override is enabled by default for DOCSIS operations. However, this command can be used to disable the frequency override feature for test and lab use. This override forces the cable modems on that interface to use a particular downstream frequency, regardless of the signal quality.

Additional information about this command and usage guidelines are available in the *Cisco IOS CMTS Cable Command Reference Guide* on Cisco.com:

http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html

Cable Flap List

The flap list is a patented tool that is incorporated in the Cisco IOS software for the Cisco Cable Modem Termination System (CMTS) universal broadband routers for troubleshooting cable modem connectivity problems. The flap list tracks “flapping” cable modems—cable modems that have intermittent connectivity problems—that could indicate a problem with the cable modem or with the upstream or downstream portion of the cable plant.

The flap-list feature does not require any special polling or data transmissions but instead monitors the registration and station maintenance activity that is already performed over any network that conforms to Data-over-Cable Service Interface Specifications (DOCSIS). The CMTS, therefore, collects its flap-list data without creating additional packet overhead and without impacting network throughput and performance. It also supports any cable modem or set-top box (STB) that meets the DOCSIS standard.

Note Although this is a Cisco proprietary CMTS feature, it is compatible with all DOCSIS-compliant cable modems. Unlike other monitoring methods that use the Simple Network Management Protocol (SNMP), the flap list uses zero bandwidth.

For additional flap list information, refer to the chapter titled “Flap List Troubleshooting for the Cisco Cable Modem Termination System” in the *Cisco Cable Modem Termination System Feature Guide* on Cisco.com.

Cisco Broadband Troubleshooter (CBT) 3.2

Multiple Service Operators (MSOs) provide a variety of services such as TV, video on demand, data, and voice telephony to subscribers. Cable companies provide a variety of services such as TV, video on demand, data, and voice telephony to subscribers. Network Administrators and radio frequency (RF)

technicians need specialized tools to resolve RF problems in the cable plant. Cisco Broadband Troubleshooter 3.2 (CBT 3.2) is a simple, easy-to-use tool designed to accurately recognize and resolve such issues.

Cisco IOS Release 12.3(9a)BC enhances support for the Cisco Broadband Troubleshooter (CBT) Version 3.2 on the Cisco uBR7246VXR universal broadband, with newly supported interoperability for the additional software features.

CBT 3.2 offers the following enhancements on the Cisco uBR7246VXR router:

- CBT 3.2 resolves the former caveat CSCee03388. This enable users to compare an upstream and cable modem on the same trace window.

  Formerly, trace windows could support the selection of up to three upstream or cable modems, but the upstream(s) and cable modems could not be mixed. CBT 3.2 now supports three upstreams or cable modems to be selected and mixed in the trace window.

For additional information about CBT 3.2, spectrum management and STM 1.1, refer to the following documents on Cisco.com:

- *Release Notes for Cisco Broadband Troubleshooter Release 3.2*

  http://www.cisco.com/en/US/products/sw/netmgtsw/ps530/prod_release_notes_list.html

- *Spectrum Management for the Cisco CMTS*

  http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/ufg_spec.html

- *Subscriber Traffic Management for the Cisco CMTS*

  https://www.cisco.com/en/US/docs/cable/cmts/feature/ubsubmon.html

Cisco CMTS Static CPE Override

The **cable submgmt default** command enables Multiple Service Operators (MSOs) to override network DHCP settings on CPE devices when performing troubleshooting with a laptop computer and console connection to the Cisco universal broadband router.

For additional information about using the **cable submgmt default** command, refer to these documents on Cisco.com:

- *Cisco CMTS Static CPE Override*

  http://www.cisco.com/en/US/docs/cable/cmts/feature/stat_cpe.html

- *Cisco IOS CMTS Cable Command Reference Guide*

  http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html

Fast Fault Detection

Cisco IOS Release 12.2(15)BC1 introduces support for Fast Fault Detection (FFD) on the Cisco uBR7246VXR router. This feature improves performance and convergence times when performing N+1 redundancy switchovers by having the failing line card proactively notify the HCCP control system about its failure. This results in a switchover occurring immediately upon a software fault, reducing the downtime of the card and minimizing any interruptions in the traffic that is flowing across the card.

FFD is automatically used on the Cisco uBR7246VXR router when N+1 redundancy operations are configured. For information on configuring and using N+1 redundancy, see the "N+1 Redundancy for the Cisco CMTS" chapter in the *Cisco CMTS Feature Guide*, at the following URL:

http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/uFGnpls1.html

Virtual Interfaces

The Cisco uBR7200 Series supports the following virtual interface feature, primarily in the Cisco IOS 12.3 BC release train:

Virtual Interface Bundling on the Cisco uBR-MC28/U BPE

Cisco IOS Release 12.3(13a)BC introduces support for virtual interface bundling on the Cisco uBR72046VXR universal broadband router and the Cisco uBR-MC28/U Broadband Processing Engine (BPE).

In prior Cisco IOS releases, cable interface bundling was limited to physical interfaces as master or slave interfaces, and **show** commands did not supply bundle information.

Virtual interface bundling removes the prior concepts of master and slave interfaces, and introduces these additional changes:

- Virtual interface bundling uses *bundle interface* and *bundle members* instead of master and slave interfaces.
- The virtual bundle interface is virtually defined, as with IP loopback addresses, for example.
- Virtual interface bundling supports bundle information in multiple **show ip interface** commands.

Virtual interface bundling prevents loss of connectivity on physical interfaces should there be a failure, problematic online insertion and removal (OIR) of one line card in the bundle, or erroneous removal of configuration on the master interface.

Virtual interface bundling supports and governs the following Layer 3 settings for the bundle member interfaces:

- IP address
- IP helper-address
- source-verify and lease-timer functions
- cable dhcp-giaddr (The giaddr field is set to the IP address of the DHCP client.)
- Protocol Independent Multicast (PIM)
- Access control lists (ACLs)
- Sub-interfaces

Note This virtual interface for the bundle should always remain on (enabled with **no shutdown**), but the Cisco CMTS provides warning messages prior to execution of the **shutdown** command.

For configuration, examples, and general guidelines for virtual interface bundling on the Cisco CMTS, refer to the following documents on Cisco.com:

- *Cable Interface Bundling and Virtual Interface Bundling for the Cisco CMTS*

  http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/ufg_bund.html
- *Virtual Interfaces and Frequency Stacking Configuration on MC5x20S and MC28U Line Cards*

  http://www.cisco.com/en/US/tech/tk86/tk804/technologies_white_paper09186a0080232b49.shtml

VLAN Features

The Cisco uBR7200 Series support the following VLAN feature:

- HSRP over ISL in Virtual LAN Configurations, page 1-126

HSRP over ISL in Virtual LAN Configurations

Inter-Switch Link protocol (ISL) is a Cisco protocol for interconnecting multiple switches and maintaining VLAN information as traffic goes between switches. ISL provides VLAN capabilities while maintaining full wire speed performance on Fast Ethernet links in full- or half-duplex mode. ISL operates in a point-to-point environment and will support up to 1000 VLANs. You can define virtually as many logical networks as are necessary for your environment.

For configuration information for Hot Standby Router Protocol (HSRP) over Inter-Switch Link (ISL) protocol, refer to these documents on Cisco.com:

- "*Configuring Routing Between VLANs with Inter-Switch Link Encapsulation*" chapter in the *Cisco IOS Switching Services Configuration Guide*, Release 12.2

  http://www.cisco.com/en/US/docs/ios/12_1/switch/configuration/guide/xcdvlisl.html

VPN and Layer 2 Tunneling Features

The Cisco uBR7200 Series supports multiple features and functions for virtual private networks (VPNs), to include the following:

- Dynamic SID/VRF Mapping Support, page 1-126
- IP Type-of-Service and Precedence for GRE Tunnels, page 1-127
- IPv6 over L2VPN, page 1-127
- Mapping Service Flows to MPLS-VPN, page 1-128
- MPLS VPN Support for Subinterfaces and Cable Interface Bundles, page 1-128
- Overlapping Subinterface IP Addresses, page 1-129
- Transparent LAN Services (TLS) and L2 Tunneling ATM/SIDs, page 1-130
- Transparent LAN Services (TLS) and L2 Virtual Private Networks, page 1-130

Dynamic SID/VRF Mapping Support

Cisco IOS release 12.3(13a)BC introduces support for dynamic service ID (SID) and VRF mapping on the Cisco CMTS, to support VoIP with MPLS. Formerly, the MPLS SID mapping feature only applied to provisioned service flows. This feature enables the mapping of all PacketCable DQoS service flows to one particular VRF.

For additional information about dynamic SID to VRF mapping, refer to the following:

- *Mapping Service Flows to MPLS VPN on the Cisco CMTS*

http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/ufg_serv.html

IP Type-of-Service and Precedence for GRE Tunnels

Prior to this feature, at generic route encapsulation-based tunnel endpoints, the Type-of-Service (TOS) bits (including precedence bits) were not copied to the tunnel or GRE IP header that encapsulates the inner packet. Instead, those bits were set to zero. This was not a problem unless the intermediate routers between two tunnel endpoints honored TOS or precedence bits, in which case those settings were ignored.

With the advent of virtual private network (VPN) and QoS applications, it is desirable to copy the TOS bits when the router encapsulates the packets using GRE. Thus, intermediate routers between tunnel endpoints can take advantage of the QoS features such as weighted fair queuing (WFQ) and weighted random early detection (WRED).

This feature provides the following benefits:

- Routers between GRE tunnel endpoints will adhere to precedence bits and other TOS bits, thereby possibly improving the routing of important packets. Cisco IOS Quality-of-Service technology, such as policy routing, Committed Access Rate, WFQ, and WRED can operate on intermediate routers between GRE tunnel endpoints.
- Additional security is possible when Cisco IOS network layer encryption is used with precedence for GRE tunnels to provide data confidentiality between VPN tunnel endpoints.
- QoS policy granularity is available per network, per user, and per application.
- The deployment of a GRE tunnel is flexible; it can be applied at the Enterprise CPE or at the Service Provider ingress point.

For configuration information, refer to the following document on CIsco.com:

- *IP Precedence for GRE Tunnels*

http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/113t/113t_4/greqos.htm

IPv6 over L2VPN

Beginning with Cisco IOS Release 12.3(17a)BC, the Cisco uBR7246VXR router now supports IPv6 using Layer 2 VPNs based on SID to 802.1q mapping. The Cisco uBR7246VXR router already supported Transparent LAN service with Layer 2 VPNs in Cisco IOS Release 12.3(13a)BC and later releases. As more Internet users switch to IPv6, the Cisco IPv6 protocol support helps enable the transition. IPv6 fixes a number of limitations in IPv4, such as limited numbers of available IPv4 addresses in addition to improved routing and network autoconfiguration. This feature allows customers to introduce IPv6 into their network with minimal operational impact.

For additional information about this feature, refer to the following documents on Cisco.com:

- IPv6 Documentation: overview, technology, design and configuration information

  http://www.cisco.com/en/US/tech/tk872/tsd_technology_support_protocol_home.html

Mapping Service Flows to MPLS-VPN

The Cisco uBR7200 series routers have been providing Managed Access using multiprotocol label switching-virtual private networks (MPLS-VPNs) configured over cable subinterfaces, with each subinterface configured for a specific ISP. Thus, service providers have a manageable way to offer users access to multiple Internet Service Providers (ISPs) over the same physical hybrid fiber-coaxial (HFC) cable network.

This system works very well when all customer premises equipment (CPE) devices behind a cable modem are using the same ISP. However, users are increasingly requesting more complex networks that would allow multiple CPE devices to access different ISPs through the same cable modem.

For example, different users in one household might want to use different PCs to access different ISPs. Another increasingly common situation is that one user requires a secure VPN connection for telecommuting through one ISP, while other users in the household use other computers to access the public Internet through a separate ISP.

The Mapping Service Flows to MPLS-VPN feature enhances this existing MPLS-VPNs support to provide more flexible Managed Access for different ISPs through the same cable modem.

The Mapping Service Flows to MPLS-VPN feature uses DOCSIS 1.1 upstream packet classifiers and service flow IDs (SFIDs) to map individual CPE devices to separate MPLS-VPN interfaces.

In summary, the service provider creates a DOCSIS configuration file for each cable modem that contains:

- Multiple secondary upstream service flows that specify QoS profiles for each CPE device.
- A Vendor Specific QoS Parameter that identifies the MPLS-VPN route to be used for packets using a particular service flow.
- Multiple secondary upstream packet classifiers that specify the MAC address for each CPE device as the Source MAC Address parameter.

The cable modem then downloads the DOCSIS configuration file during its registration process and configures itself for the proper service flows and packet classifiers.

When the cable modem comes online, it begins receiving packets from its CPE devices. The cable modem uses the packet's source MAC address to match the packet to the proper packet classifier, which then identifies the correct SFID to use. The cable modem then transmits the packet to the Cisco uBR7200 series router using this upstream SFID.

The Cisco uBR7200 series router examines the packet to determine its SFID, and then uses the Vendor-Specific QoS Parameter associated with that service flow to route the packet to the appropriate MPLS-VPN interface.

For additional information on the Mapping Service Flows to MPLS-VPN feature, refer to the following document on Cisco.com:

- *Mapping Service Flows to MPLS-VPN on the Cisco uBR7200 Series Router*

  http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/ufg_serv.html

MPLS VPN Support for Subinterfaces and Cable Interface Bundles

The Cisco uBR7200 routers offer MPLS VPN support for subinterfaces and cable interface bundles. Using MPLS VPN technology, service providers can create scalable and efficient private networks using a shared hybrid fiber coaxial (HFC) network and Internet protocol (IP) infrastructure.

Using MPLS VPN technology, service providers can create scalable and efficient private networks using a shared hybrid fiber-coaxial (HFC) network and IP infrastructure. The cable MPLS VPN network consists of this infrastructure:

- The multiple service operator (MSO) or cable company that owns the physical infrastructure and builds VPNs for the Internet service providers (ISPs) to move traffic over the cable and IP backbone.
- ISPs that use the HFC network and IP infrastructure to supply Internet service to cable customers.

Each ISP moves traffic to and from a subscriber's PC, through the MSO's physical network infrastructure, to the ISP's network. MPLS VPNs, created in Layer 3, provide privacy and security by constraining the distribution of a VPN's routes to only the routers that belong to its network. Thus, each ISP's VPN is insulated from other ISPs that use the same MSO infrastructure.

An MPLS VPN assigns a unique VPN Routing/Forwarding (VRF) instance to each VPN. A VRF instance consists of an IP routing table, a derived forwarding table, a set of interfaces that use the forwarding table, and a set of rules and routing protocols that determine the contents of the forwarding table. Each PE router maintains one or more VRF tables. It looks up a packet's IP destination address in the appropriate VRF table, only if the packet arrived directly through an interface associated with that table. MPLS VPNs use a combination of Border Gateway Protocol (BGP) and IP address resolution to ensure security.

Refer to the chapter "Configuring Multiprotocol Label Switching" in the *Cisco IOS Switching Services Configuration Guide*, Release 12.2 on Cisco.com.

Overlapping Subinterface IP Addresses

Multiprotocol Label Switching (MPLS)-based Virtual Private Networks (VPNs) are created in Layer 3, and provide privacy and security by constraining the distribution of a VPN's routes to those routers that are members of the VPN only, and by using MPLS forwarding. Each ISP's VPN is insulated from all others sharing the HFC and IP-over-cable infrastructure. MPLS VPN enforces traffic separation by assigning a unique VPN Routing/Forwarding (VRF) instance to each VPN. A VRF instance consists of an IP routing table, a derived forwarding table, a set of interfaces that use the forwarding table, and a set of rules and routing protocols that determine what is in the forwarding table.

Cisco IOS Release 12.1(2)EC1 and earlier releases assumed that IP addresses were unique, but it is possible with an MPLS VPN to configure overlapped IP addresses within a VRF. A configuration of overlapped IP addresses could have caused errors. Cisco IOS Release 12.1(3)EC supports a configuration of overlapping IP addresses for subinterfaces. The same IP subnet can now be configured for CPEs on different VRFs using a Cisco uBR7200 series router to configure an MPLS VPN.

The following CLI commands have been updated in recent Cisco IOS releases to support overlapping IP addresses on subinterfaces:

New CLI Commands

- **cable device** {*ip-address* | *mac-address*} [**no**] **access-group** {*access-list* | *access-name*} | {[**vrf** *vrf-name*] *ip-address* [**no**] **access-group** [*access-list* | *access-name*]}
- **cable host** {*ip-address* | *mac-address*} [**no**] **access-group** {*access-list* | *access-name*} | {[**vrf** *vrf-name*] *ip-address* [**no**] **access-group** [*access-list* | *access-name*]}
- **clear cable host** {*ip-address* | *mac-address*}
- **show cable device** [**vrf** *vrfname*] [*ip-address*] **access-group**
- **show cable host** [**vrf** *vrfname*] [*ip-address* | *mac-address*] **access-group**

Note For the latest command information and detailed command history, refer to the *Cisco IOS CMTS Cable Command Reference Guide* on Cisco.com.

Transparent LAN Services (TLS) and L2 Tunneling ATM/SIDs

Cisco IOS 12.3(9a)BC introduces support for the Transparent LAN Service over Cable feature on the Cisco uBR7246VXR router. This feature enhances existing Wide Area Network (WAN) support to provide more flexible Managed Access for multiple Internet service provider (ISP) support over a hybrid fiber-coaxial (HFC) cable network.

This feature allows service providers to create a Layer 2 tunnel by mapping an upstream service identifier (SID) to an ATM permanent virtual connection (PVC) or a Virtual Local Area Network (VLAN).

For additional information about configuring TLS on the Cisco uBR7246VXR router, refer to the following document on Cisco.com:

- *Transparent LAN Service over Cable*

http://www.cisco.com/en/US/docs/cable/cmts/feature/tls-cmts.html

Transparent LAN Services (TLS) and L2 Virtual Private Networks

Cisco IOS Release 12.3(13a)BC introduces the following changes or requirements for the TLS feature with Layer 2 VPNs:

- When the TLS feature is used with Layer 2 VPNs, the participating cable modems must have the Baseline Privacy Interface security feature (BPI) enabled. Otherwise, the Cisco CMTS drops such Layer 2 traffic in the upstream or downstream.
- Information about Customer Premises Equipment (CPE) does not display in the output of the **show cable modem** command.

Note Configuring ATM L2VPN or 802.1q for a particular cable modem removes any previous cable modem configuration on the Cisco uBR7246VXR router. For example, if TLS with 802.1q is configured on the router for a particular cable modem, and then you configure ATM L2VPN for the same cable modem, the Cisco uBR7246VXR router supports the latter and removes the former with no additional warning or system messages.

Refer to the following documents on Cisco.com for additional TLS information:

- *TLS for the Cisco CMTS*

  http://www.cisco.com/en/US/docs/cable/cmts/feature/tls-cmts.html

- *TLS Over Cable* - TAC Document #60027

  http://www.cisco.com/en/US/products/hw/cable/ps2217/products_configuration_example09186a008029160d.shtml

WAN Optimization and Services Features

The Cisco uBR7200 Series supports multiple WAN features:

Bandwidth Allocation Control Protocol (BACP)

The BACP provides Multilink PPP (MLP) peers with the ability to govern link utilization. Once peers have successfully negotiated BACP, they can use the Bandwidth Allocation Protocol (BAP), which is a subset of BACP, to negotiate bandwidth allocation. BAP provides a set of rules governing dynamic bandwidth allocation through call control; a defined method for adding and removing links from a multilink bundle for Multilink PPP is used.

BACP provides the following benefits:

- Allows multilink implementations to interoperate by providing call control through the use of link types, speeds, and telephone numbers.
- Controls thrashing caused by links being brought up and removed in a short period of time.
- Ensures that both ends of the link are informed when links are added or removed from a multilink bundle.

For configuration information, refer to the chapter titled "Configuring the Bandwidth Allocation Control Protocol" in the *Cisco IOS Dial Services Configuration Guide: Network Services*, Release 12.1 on Cisco.com.

Closed User Group Selection Facility Suppress Option

A closed user group (CUG) selection facility is a specific encoding element that allows a destination data terminal equipment (DTE) to identify the CUG to which the source and destination DTEs belong. The Closed User Group Selection Facility Suppress Option feature enables a user to configure an X.25 data

communications equipment (DCE) interface or X.25 profile with a DCE station type to remove the CUG selection facility from incoming call packets destined for the preferential CUG only or for all CUGs. You can also remove the selection facility from a CUG with outgoing access (CUG/OA).

Enhanced Local Management Interface (ELMI)

When used in conjunction with traffic shaping, the router can respond to changes in the network dynamically. The optional Enhanced Local Management Interface (ELMI) feature allows the router to learn QoS parameters from the Cisco switch and use them for traffic shaping, configuration, or management purposes.

ELMI also simplifies traffic shaping configuration on the router. Previously, users needed to configure traffic shaping rate enforcement values, possibly for every VC. Enabling ELMI reduces the chance of specifying inconsistent or incorrect values when configuring the router.

To enable ELMI, you must configure it on the main interface. For configuration information, refer to the chapter titled Configuring Frame Relay and Frame Relay Traffic Shaping" in the *Cisco IOS Quality of Service Solutions Configuration Guide*, Release 12.2 on Cisco.com.

Frame Relay Enhancements

Cisco IOS Releases—Cisco IOS Release 12.2(4)BC1 and the Cisco uBR7200 series support recent frame relay enhancements, such as:

- Frame Relay end-to-end keepalives
- PPP configuration over Frame Relay

For additional information about configuring frame relay, refer to one of these two documents, on Cisco.com, depending on your Cisco IOS release:

- "Configuring Frame Relay" in the *Cisco IOS Wide-Area Networking Configuration Guide*, Release 12.1
- Configuring Frame Relay and Frame Relay Traffic Shaping" in the *Cisco IOS Quality of Service Solutions Configuration Guide*, Release 12.2

Frame Relay MIB Extensions

The Cisco Frame Relay MIB adds extensions to the standard Frame Relay MIB (RFC 1315). It provides additional link-level and VC-level information and statistics that are mostly specific to Cisco Frame Relay implementation. This MIB provides SNMP network management access to most of the information covered by the **show frame-relay** commands, such as **show frame-relay lmi**, **show frame-relay pvc**, **show frame-relay map**, and **show frame-relay svc**.

For additional information, refer to "Configuring Frame Relay" in the *Cisco IOS Wide-Area Networking Configuration Guide*, Release 12.2 on Cisco.com.

For a release-specific list of MIBs supported by the Cisco uBR7200 Series, refer to the *Cisco uBR7200 Series Software Release Notes* on Cisco.com:

http://www.cisco.com/en/US/docs/ios/12_2/12_2b/12_2bc/release/notes/u7208bc1.html

For descriptions of supported MIBs and how to use MIBs, refer to the *Cisco MIBs* web page on Cisco.com.

Frame Relay Router ForeSight

ForeSight is the network traffic control software used in some Cisco switches. The Cisco Frame Relay switch can extend ForeSight messages over a User-to-Network Interface (UNI), passing the backward congestion notification for VCs. ForeSight allows Cisco Frame Relay routers to process and react to ForeSight messages and adjust VC level traffic shaping in a timely manner.

ForeSight must be configured explicitly on both the Cisco router and the Cisco switch. ForeSight is enabled on the Cisco router when Frame Relay traffic shaping is configured. However, the router's response to ForeSight is not applied to any VC until the **frame-relay adaptive-shaping foresight** command is added to the VCs map-class. When ForeSight is enabled on the switch, the switch will periodically send out a ForeSight message based on the time value configured. The time interval can range from 40 to 5000 milliseconds.

For additional information about configuring frame relay, refer to "Configuring Frame Relay" in the *Cisco IOS Wide-Area Networking Configuration Guide, Release 12.2* on Cisco.com.

ISDN Advice of Charge

ISDN Advice of Charge (AOC) allows users to obtain charging information for all calls during the call (AOC-D) or at the end of the call (AOC-E) or both. Users must have subscribed through their local ISDN network to receive the AOC information from the switch. No router configuration changes are required to retrieve this call charging information.

The ISDN AOC feature also supports, for the AOC-D service, an optional configurable short-hold mode that provides a dynamic idle timeout by measuring the call charging period, based on the frequency of the AOC-D or the AOC-E message from the network. The short-hold mode allows users to track call costs and to control and possibly reduce tariff charges. The short-hold mode idle time will do the following:

- Disconnect a call just prior to the beginning of a new charging period if the call has been idle for at least the configured minimum idle time.
- Maintain the call to the end of the current charging period past the configured idle timeout if the time left in the charging period is longer.

Incoming calls are disconnected using the static dialer idle timeout value.

For configuration information, refer to the chapter titled "Configuring ISDN Special Signalling" in the *Cisco IOS Dial Services Configuration Guide: Terminal Services*, Release 12.1 on Cisco.com.

ISDN Caller ID Callback

ISDN caller ID callback allows the initial incoming call from the client to the server to be rejected based on the caller ID message contained in the ISDN setup message, and it allows a callback to be initiated to the calling destination.

ISDN caller ID callback allows great flexibility for you to define which calls to accept, which to deny, and which calls to reject initially but for which the router should initiate callback. The feature works by using existing ISDN caller ID screening, which matches the number in the incoming call against numbers configured on the router, determining the best match for the number in the incoming call, and then, if configured, initiating callback to the number configured on the router.

When a call is received, the entire list of configured numbers is checked and the configuration of the best match number determines the action:

- If the incoming number is best matched by a number that is configured for callback, then the incoming call is rejected and callback is initiated.
- If the incoming number is best matched by another entry in the list of configured numbers, the call is accepted.
- If the incoming number does not match any entry in the configured list, the call is rejected and no callback is started.

For configuration information, refer to the chapter titled "Configuring ISDN Caller ID Callback" in the *Cisco IOS Dial Services Configuration Guide: Network Services*, Release 12.1 on Cisco.com.

ISDN Multiple Switch Types

The Cisco IOS software provides an enhanced *Multiple ISDN Switch Types* feature that allows you to apply an ISDN switch type to a specific ISDN interface and to configure more than one ISDN switch type per router. This feature allows both ISDN BRI and ISDN PRI to run simultaneously on platforms that support both interface types.

For configuration information, refer to the chapter titled Setting Up Basic ISDN Service" in the *Cisco IOS Dial Services Configuration Guide: Terminal Services*, Release 12.1 on Cisco.com.

ISDN NFAS

ISDN Non-Facility Associated Signalling (NFAS) allows a single D channel to control multiple PRI interfaces. A backup D channel can also be configured for use when the primary NFAS D channel fails.

For configuration information, refer to the chapter titled "Configuring ISDN Special Signalling" in the *Cisco IOS Dial Services Configuration Guide: Terminal Services*, Release 12.1 on Cisco.com.

Microsoft Point-to-Point Compression (MPPC)

In March of 1997, Microsoft Corporation introduced the Microsoft Point-to-Point Compression (MPPC) scheme as a means of representing arbitrary PPP packets in a compressed form. MPPC was ratified by the Internet Engineering Task Force (IETF) and is known as RFC 2118. The Windows 95 client software supports both MPPC and LZS Stacker compression, whereas the Microsoft NT server and Windows 2000 only support MPPC, which is negotiated during the Compression Control Protocol (CCP) process.

To enable MPPC compression on access servers, you need to be running Cisco IOS Software version 11.3T or later. Refer to these two documents on Cisco.com for additional information:

- *MPPC Compression on Access Servers*
- *Microsoft Point-to-Point Compression (MPPC)*

MLPPP Support

The Cisco IOS Multilink Point-to-Point Protocol (MLPPP) feature is now supported for selected line cards and port adapters on the Cisco uBR7100 series and the Cisco uBR7200 Series, which share the same MLPPP code as the Cisco 7200 series. There is no new hardware or software for MLPPP in this release.

Note MLPPP combines one or more physical interfaces into a virtual "bundle" interface. The bandwidth of the bundle interface is equal to the sum of the component links' bandwidth. This allows service providers to make the step from T1 and E1 lines to affordable T3 and E3 speeds.

MLPPP is configured not on a cable interface, but on the T1/E1 link.

Line Cards and Port Adapters Supporting MLPPP on the Cisco uBR7200 Series

Table 15 lists the line cards and port adapters on the Cisco uBR7200 Series, in conjunction with the applicable network processing engine (NPE), that are supported for MLPPP at the time Cisco IOS Release 12.3(13a)BC was released.

Table 15 Line Cards and Port Adapters Supporting MLPPP on the Cisco uBR7200 Series for Cisco IOS Release 12.3(13a)BC

Model	NPE	Line Card	Port Adapter
Cisco uBR7246VXR	NPE-400, NPE-G1	MC16C, MC16S, MC28C, MC28U	PA-4T+, PA-MC-2E1/120, PA-MC-4T1
Cisco uBR7114	N/A	N/A	PA-4E1G/120, PA-4T+, PA-MC-4T1

National ISDN Switch Types for BRI and PRI

The Cisco uBR7200 series supports many national ISDN switch types, including those that support Basic Rate Interface (BRI) and Primary Rate Interface (PRI). ISDN switch types are described further in the document titled *ISDN Switch Types, Codes, and Values* on Cisco.com.

PAD Subaddressing

In situations where the X.121 calling address is not sufficient to identify the source of the call, you can append a specified value to the calling address using the PAD subaddressing feature. PAD subaddressing allows you to create unique X.121 calling addresses by including either a physical port number or a value specified for a line as a subaddress to the X.121 calling address.

PAD subaddressing enables an X.25 host application to uniquely identify the source of an X.121 call. For example, in some bank security alarm applications, the central alarm host identifies the physical location of the alarm units from subaddressing information contained in the Call Request packet.

For additional information, refer to"Configuring the Cisco PAD Facility for X.25 Connections" in the *Cisco IOS Terminal Services Configuration Guide*, Release 12.2 on Cisco.com.

PPPoE Termination Support on Cable Interfaces

Cisco IOS Release 12.2(4)BC1 adds support for Point-to-Point Protocol over Ethernet (PPPoE) by allowing a direct connection to cable interfaces. PPPoE provides service-provider digital-subscriber line (DSL) support. The support of PPPoE on cable interfaces of the Cisco uBR7200 series routers allows customer premises equipment (CPE) behind the cable modem to use PPP as a mechanism to get their IP addresses and use it for all subsequent data traffic, just like a dial-up PPP client. In a PPP dial-up session, the PPPoE session is authenticated and the IP address is negotiated between the PPPoE client and the server, which could be either a Cisco uBR7200 series router or a Home Gateway.

Additional information about configuring PPPoE is available in the following documents:

- *Configuring Broadband Access: PPP and Routed Bridge Encapsulation* chapter of the *Cisco IOS Wide-Area Networking Configuration Guide*, Release 12.2 on Cisco.com
- Cisco *PPPoE on Ethernet* feature module on Cisco.com
- *RFC 2516*

VPDN MIB and Syslog Facility

For a complete list of MIBs supported by the Cisco uBR7200 Series, refer to the *Cisco uBR7200 Series Software Release Notes* on Cisco.com:

http://www.cisco.com/univercd/cc/td/doc/product/cable/cab_rout/ub7200rn/index.htm

For descriptions of supported MIBs and how to use MIBs, refer to the *Cisco MIBs* web page on Cisco.com.

X.25 Enhancements

X.25 packet-switched support is provided by the operating software that is bundled with the Cisco IOS software image. The operating software provides both the link- and packet-level facilities of the 4T+ port adapter.

The operating software is accessed via a VT100 terminal connected to the console port of the Input/Output controller. The settings of the terminal should be as follows:

Baud: 9600
Data bits: 8
Parity: none
Stop bits: 1

To boot the software from Flash memory, type the following command at the ">" prompt:

```
Router> b flash
```

X.25 Switching Between PVCs and SVCs

To configure PVC to SVC switching between two serial interfaces, both interfaces must already be configured for X.25. In addition, X.25 switching must be enabled using the x25 routing global configuration command. The PVC interface must be a serial interface configured with X.25 encapsulation. (The SVC interface may use X.25, XOT, or CMNS.)

Use the following command in interface configuration mode once the interfaces have been configured for X.25 switching to configure X.25 switching between PVCs and SVCs:

Command	Purpose
x25 pvc *number1* **svc** *x121-address* [*flow-control-options*] [*call-control-options*]	Configures PVC traffic to be forwarded to an SVC.

To display information about the switched PVC to SVC circuit, use the following command in privileged EXEC mode:

Command	Purpose
show x25 vc [**lcn**]	Displays information about the active SVCs and PVCs.

For additional information, refer to the chapter titled "*Configuring X.25 and LAPB*" in the *Cisco IOS Wide-Area Networking Configuration Guide*, Release 12.2 on Cisco.com.

Note Early deployment releases contain fixes to software caveats as well as support for new Cisco hardware and software features

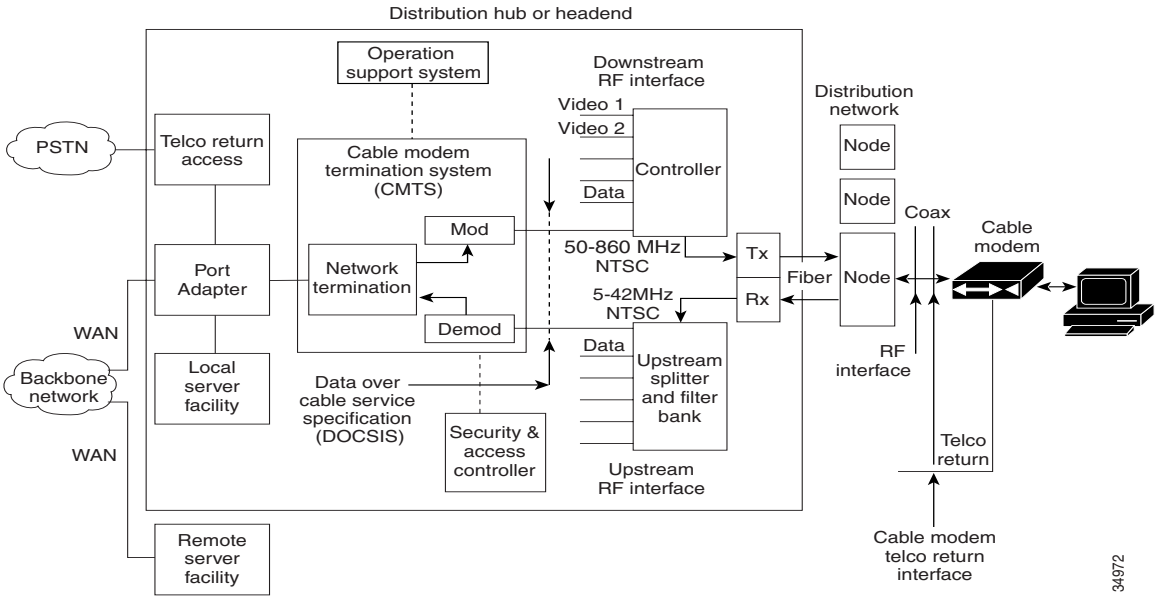
DOCSIS and CMTS Interoperability

This section contains the following topics to familiarize you with DOCSIS architectural fundamentals:

DOCSIS NTSC Cable Plants

DOCSIS-compliant cable plants that support North American channel plans use ITU J.83 Annex B RF. Figure 1-1 illustrates a DOCSIS two-way and telco-return architecture.

Figure 1-1 DOCSIS Two-Way and Telco-Return Architecture



Larger cable companies typically have high-speed fiber backbones that carry Internet data, voice, and video between the following cable company facilities:

- Regional processing centers
- Headends
- Hubs

The fiber backbone can be made up of OC-3 (155 Mbps) to OC-48 (2488 Mbps) Synchronous Optical Network (SONET) or Asynchronous Transfer Mode (ATM) rings. The backbone network can connect to other networks, including the Public Switched Telephone Network (PSTN), other cable system backbones, or to public Internet interconnect points that multiple ISPs use.

The CMTS Media Access Control (MAC) domain typically includes one or more downstream paths and one or more upstream paths. Depending on the CMTS configuration, the CMTS MAC domain can be defined to have its downstreams on one cable interface line card with its upstreams on another card, or one or more CMTS MAC domains per cable interface line card.

Cisco provides high-speed routers to route interactive traffic between the backbone and Ethernet in the headend internal network. Signaling protocols maintain the network intelligence needed to route traffic optimally, automatically building and maintaining routing tables to direct traffic and signal failures for rerouting in the network.

Border Gateway Protocol (BPG) typically operates between the cable operator's regional network and external networks, providing routing information exchange between different networks. The Open Shortest Path First (OSPF) protocol is used in regional networks usually. Cisco routers incorporate Cisco IOS software, which offers advanced software features, including quality of service (QoS), Weighted Fair Queuing (WFQ), and IP multicast.

EuroDOCSIS Cable Plants

EuroDOCSIS-based cable plants use EuroDOCSIS J.112 (Annex A) standard, similar to the DAVIC/DVB J.83 Annex A physical layer. The MC16E builds on the DOCSIS protocol, adding support at the physical layer for PAL and SECAM channel plans. The card permits full bandwidth utilization of the 8 MHz downstream channel, allowing up to 50 Mbps throughput, and greater upstream frequency selection—5 to 65 MHz, instead of 5 to 42 MHz.

Figure 1-2 illustrates a three-tier EuroDOCSIS configuration involving STB deployment. The sample architecture has four subsystems:

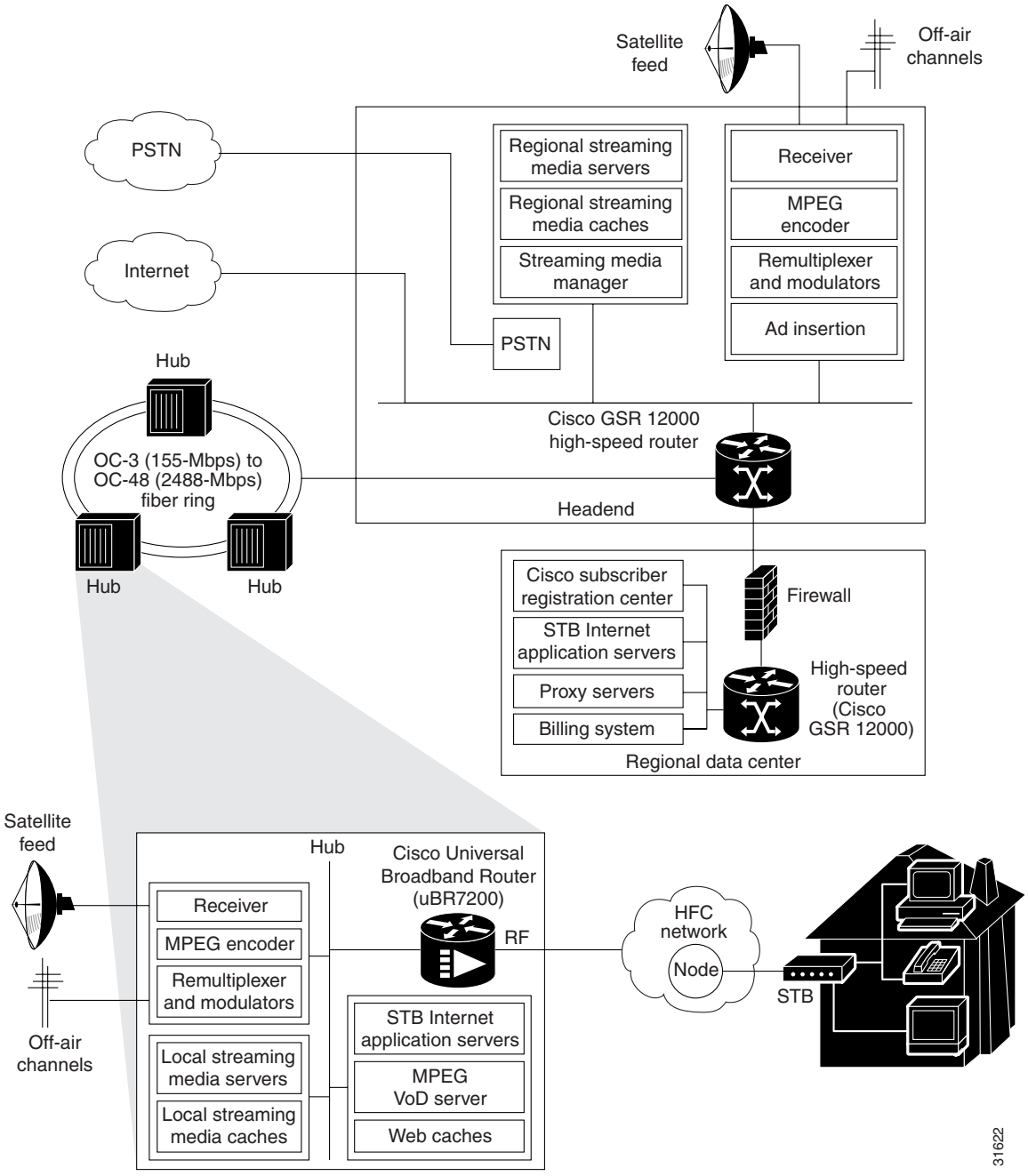
- High-speed fiber backbone—Carries Internet data, voice, and video between regional processing centers, headends, and hubs.
- Headend—Aggregates content at the national and regional level and sends it to the fiber backbone.
- Hub—Combines regional programming with local content and sends that combined content to the cable network.
- Interactive STBs with integrated EuroDOCSIS CMs—Connects subscribers to the cable network.

Video sources are Motion Picture Experts Group (MPEG) encoded and then fed into an MPEG multiplexer that packs the MPEG video streams into a single stream. This stream is uplinked to a satellite and then downlinked to multiple headends, which then distribute the MPEG stream directly onto the HFC plant.

The STB receives signals from the cable network and displays them on a television. An STB with EuroDOCSIS cable modem functionality supports two-way interactivity. Inside the EuroDOCSIS STB are two tuners:

- One handles MPEG-2 video, audio, broadcast control data, and broadcast service data.
- The other supports DOCSIS IP data. The return path is implemented with EuroDOCSIS.

Figure 1-2 EuroDOCSIS and STB Architecture



DOCSIS-Compliant Downstream Signals

Downstream signals are modulated using 64 or 256 Quadrature Amplitude Modulation (QAM-64 or QAM-256), based on the cable interface card used, your cable plant, and the significance of the data. DOCSIS defines the messages and data types for CMTS to cable modem (or cable modem in an STB)

communications. All CMs listen to all frames transmitted on the downstream channel on which they are registered and accept those where the destinations match the units themselves or the devices each supports.

The Cisco uBR7200 series supports multicast groups using standard protocols such as Protocol Independent Multicast (PIM), Distance Vector Multicast Routing Protocol (DVMRP), and Internet Group Management Protocol (IGMP) to determine if multicast streams are to be forwarded to a prescribed downstream cable modem or STB, or a multicast routing peer.

The Cisco uBR7200 series software periodically sends MAC allocation and management messages—known as MAPs—to all CMs on the network, defining the transmission availability of channels for specific periods of time. The MAP rate is fixed—every 2 msec.

Different transmission intervals are defined that associate an interval with a Service Identifier (SID). SIDs define the devices allowed to transmit and provide device identification and class of service management. Software defines what type of transmission is allowed during the interval.

The CMTS system administrator typically assigns one or more SIDs to each cable modem, corresponding to the classes of service the cable modem requires. Each MAP is associated with a particular upstream channel. The SID concept supports multiple data flows and use of protocols such as Resource Reservation Protocol (RSVP) that allows IP backbone QoS features to be extended to the CMTS. The CMTS schedules the times granted for sending and receiving packets, and if defined, manipulates the Type-of-Service (ToS) field in the IP packet header to accommodate QoS.

Note Cisco uBR7200 Series software supports extensions to DOCSIS 1.0 to operate with DOCSIS 1.0-based CMs or cable RF CPE devices (such as Cisco uBR924 cable access routers or Cisco uBR910 series cable data service units) that also support DOCSIS 1.0 extensions.

Tip DOCSIS 1.0 extensions address the problem of QoS for VoIP until DOCSIS 1.1 is solidified. Currently, only certain vendors offer products that support DOCSIS 1.0 extensions.

DOCSIS 1.0 extensions build intelligence into the MAP file the CMTS sends to voice-enabled CMs to address jitter and delay. The extensions support unsolicited grants, allowing a portion of bandwidth to be dedicated to a voice call as soon as a subscriber initiates a call until that call is terminated. Unsolicited grants are used to create a constant bit rate-like stream between the CMTS and the cable modem, in contrast to typical data applications where CMs request grants from the CMTS before they can transmit upstream. Refer to the "This section summarizes Cisco uBR7200 series router software features for all supported Cisco IOS Release trains, and directs you to additional configuration information for each feature." section on page 1-22 for feature descriptions and links to configuration information.

DOCSIS-Compliant Upstream Signals

The upstream channel is characterized by many CMs (or CMs in STBs) transmitting to the CMTS. These signals typically operate in a burst mode of transmission. Time in the upstream channel is slotted.

The CMTS provides time slots and controls the usage for each upstream interval. The CMTS sends regular mappings of minislot structure in downstream broadcast MAP messages. The CMTS allocates contention broadcast slots that all CMs can use, and also allocates upstream minislots for unicast or non-contention data from specific CMs.

The CMTS allocates two basic types of contention slots on the upstream:

- Initial ranging slots that CMs use during their initialization phase to join the network. Once the CMTS receives an initial ranging request from a cable modem using this kind of slot, it subsequently polls the cable modem, along with other operational CMs, in unicast, non-contention station maintenance slots.
- Bandwidth-request minislots that CMs use to request data grants from the CMTS to send data upstream in non-contention mode. Any cable modem can use this type of minislot to request a data grant from the CMTS.

The stream of initial ranging slots and bandwidth request minislots comprise two separate contention subchannels on the upstream. Cisco uBR7200 Series software uses a "dynamic bandwidth-request minislots-per-MAP" algorithm to dynamically control the rate of contention slots for initial ranging and bandwidth-requests. The CMTS uses a common algorithm to vary backoff parameters that CMs use within each of the two upstream contention subchannels. The CMTS uses these algorithms to dynamically determine the initial ranging slots and bandwidth-request minislots to allocate on the slotted upstream.

When power is restored after a catastrophic power failure, a large number of CMs will want to join the network simultaneously. This represents an impulse load on the initial ranging subchannel. The CMTS in this situation will increase the frequency of initial ranging slots so that CMs can quickly join the network.

During high upstream data loads, the CMTS conserves the scarce upstream channel bandwidth resource and is more frugal in introducing upstream initial ranging slots. The CMTS schedules bandwidth-request minislots at low loads to provide low access delay. At high upstream loads, the CMTS reduces the number of contention-based request minislots in favor of data grants, while maintaining a minimum number of request slots.

Note The system default is to have the automatic dynamic ranging interval algorithm enabled, automatic dynamic ranging backoff enabled, and data backoffs for each upstream on a cable interface. Commands to configure the dynamic contention algorithms include:
[**no**] **cable insertion-interval** [*automatic* [<*Imin* [*Imax*]>] *in msecs*
[**no**] **cable upstream** <*port number*> **range backoff** [*automatic*] | [<*start*> <*end*>]
[**no**] **cable upstream** <*port number*> **data-backoff** [*automatic*] | [<*start*> <*end*>]

Caution In general, Cisco discourages adjusting default settings. Only personnel who have received the necessary training should attempt to adjust values.

The Cisco uBR7200 series equipment periodically broadcasts Upstream Channel Descriptor (UCD) messages to all CMs. These messages define upstream channel characteristics that include upstream frequencies, symbol rates and modulation schemes, Forward Error Correction (FEC) parameters, and other physical layer values.

Upstream signals are demodulated using Quadrature Phase Shift Keying (QPSK) or Quadrature Amplitude Modulation (QAM). QPSK carries information in the phase of the signal carrier, whereas QAM uses both phase and amplitude to carry information.

Tip If your cable plant is susceptible to ingress or noise, QPSK is recommended based on the importance of the data. Frequencies below 20 MHz are more susceptible to noise and might require lower symbol rates. Higher frequencies might be able to support higher rates and use QAM modulation instead.

Traffic Engineering

Sending data reliably upstream is a critical issue. Designing a robust upstream architecture requires balancing system parameters, establishing subscriber data requirements, and configuring the network to support those requirements.

Upstream spectrum varies greatly between cable plants. Maintaining stable return paths also differs based on varying patterns and levels of ingress noise and interference. Common problems in cable plants include:

- Electrical and magnetic interference (EMI)
- Thermal noise
- Carrier to noise (C/N) imbalances
- Interference of leaking signals
- Ingress due to other channels appearing at the desired channel frequency
- Distortion due to non-linearities of cable equipment
- Cross modulation—carrier to frequency distortion
- Hum and low frequency distortion
- Improper RF amplifier tuning
- Non-unity gains due to incorrect usage of attenuators
- Low-quality subscriber equipment
- Out of range signal power from the CMTS to the cable modem

When configuring your system, configure downstream and upstream parameters based on the fiber nodes involved, the required services the cable modem or STB supports, the importance of the data, and desired performance capabilities.

Your cable plant determines its data performance. Design your network to maximize its performance and capacity at minimum cost, while meeting subscriber data requirements. Select or customize upstream profiles for maximum trade-offs between bandwidth efficiency and upstream channel robustness once you're familiar with the system and have characterized your network. For example, QAM-16 requires approximately 7 dB higher C/N ratio to achieve the same bit error rate (BER) as QPSK, but it transfers information at twice the rate of QPSK.

Note Older plants and plants with long amplifier cascades are more susceptible to ingress than newer plants. These plants produce more noise and signal level variances.

Tip Cisco recommends you keep input to all amplifiers at the same power level in the upstream direction and keep output of all amplifiers in the downstream direction at the same power level. This is called unity gain. Tune amplifiers and other equipment properly at desired frequencies. To characterize and improve your cable plant's stability, follow procedures in the *Cisco uBR7200 Series Universal Broadband Router Hardware Installation Guide* on Cisco.com.

A DOCSIS cable plant has the following groups of traffic to size based on current service offerings:

- Basic Internet access data, which is burst-intensive and asymmetrical; asymmetrical traffic supports a larger data rate in one direction—the downstream.

- VoIP traffic, which requires constant bandwidth, has low tolerance to latency and jitter, and is typically symmetrical—supporting the same data rate in downstream and upstream directions. VoIP generally requires phase-lock and jitter attenuation.
- VPN traffic, which requires secure transmissions; traffic is typically symmetrical since telecommuters exchange more data upstream than residential Internet access customers.
- Video, which can include digital video channels based on the services in your network; current Cisco uBR7200 Series products support EuroDOCSIS operation where data is MPEG encoded and packed into an 8 MHz RF channel spacing based on the channel plan used and equipment at the headend or distribution hub. Video flows in one direction and control information flows in the other.
- Signaling and maintenance—the DOCSIS MAC layer support includes DOCSIS encapsulation, initial maintenance, station maintenance, registration, frequency hop, and upstream channel changes.

You have a wide range of options to engineer your network. Define your network based on your cable facilities—headend or distribution hub—and your anticipated service offerings, subscription, and required service levels. Define data requirements relative to the number of subscribers to support and their usage patterns. Select upstream symbol rate, modulation format, and other parameters based on data requirements and return path characterizations.

If the service is asymmetrical, determine the ratio of downstream to upstream data rates. For basic Internet access where the majority of traffic is sent to a subscriber and the subscriber sends only a small amount of data upstream, use ratios ranging from 5:1 to 10:1.

Determine what data rate the service should support. Define the maximum and minimum data rate, answering the following questions:

- Do you want to define the minimum data rate relative to the maximum?
- Will the minimum data rate equal the maximum?
- Will it be a percentage of the maximum?
- Will the minimum data rate be zero?

Note The minimum data rate has the greatest impact on the network. The network must be sized to accommodate this level of traffic to fulfill the defined service data requirements. The amount of bandwidth available to a group of subscribers establishes where, within the defined maximum and minimum data rates, a subscriber within a group is able to operate.

For video traffic planning purposes, use a typical bit rate to calculate densities of video streams within a channel. For QoS calculations, limit the number of video streams per channel to prevent packet drops. The key traffic parameter is how many IP video streams will fit into the RF channel.

Ideally, the network is sized so that it supports all subscribers being active at the same time at the maximum data rate. This results in an expensive network, however, where full capacity, particularly for residential subscribers, is rarely used. Cisco recommends designing your network to support a given level of over-subscription.

Note Configure your network to support a percentage of all subscribers at a given data rate. At this level, the network supports the bandwidth needs of all active users. Provided the over-subscription rate is low enough, such that service definitions are met, all subscribers receive the service to which they subscribed.

Caution With over-subscription, the network is unable to support all subscribers being active at the maximum data rate. If the over-subscription is severe enough, subscribers may be denied service.

Parameters to determine the over-subscription level include:

- Peak percentage of simultaneous users—Not all subscribers access the network at the same time. Subscribers have different access patterns that vary based on profiles; working hours; family demographics; type of user—telecommuter or residential Internet access customer. Only a portion of subscribers are active at a given time. This number serves as the "peak percentage of simultaneous users parameter"— busy hour number of subscribers.
- Average data rate per subscriber—Not only are all subscribers not active at the same time, but they do not continuously operate at peak rate. Using basic Internet access as an application, data that subscribers request and send downstream and upstream is burst-intensive. A group of subscribers, therefore, has an average data rate less than the maximum rate defined by the service.

Note For some services, the average value might be the maximum rate. VoIP is such an application.

How bandwidth contention is handled depends on the mix of services defined and individual service definitions.

Percentage of homes passed subscribing to the service is another factor to consider. If this parameter is set too conservatively, the network is under-engineered and requires modification to grow the service. If set too aggressively, the network is over-engineered and costs for services are higher than they should be.

Full implementation of service levels requires additional higher layer items including scheduling, queuing priorities, bandwidth allocation. These items are addressed in DOCSIS 1.0 extensions. Refer to the "This section summarizes Cisco uBR7200 series router software features for all supported Cisco IOS Release trains, and directs you to additional configuration information for each feature." section that follows and respective chapters of this guide for additional information.